الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –

كلية التكنولوجيا

Faculté de TECHNOLOGIE

THESE

Présentée pour l'obtention du **grade** de **DOCTORAT 3ème Cycle**

En : Génie Biomédical

Spécialité : Informatique Biomédicale

Par : BELAIDI ASMA

Sujet

Contrôle d'accès et sécurité du dossier médical informatisé

Soutenue publiquement, le 12 / 06 / 2019 , devant le jury composé de :

Mr Chikh Mohammed Amine	Professeur	Univ. Tlemcen	Président
Mr Abderrahim Mohammed El Amine	MCA	Univ. Tlemcen	Directeur de thèse
Mr Benamar Abdelkrim	MCA	Univ. Tlemcen	Examinateur 1
Mr Souier Mehdi	MCA	ESM-Tlemcen	Examinateur 2

Année Universitaire : 2018/2019

Dédicaces

Du plus profond de mon cœur, je dédie ce travail à tous ceux qui me sont chers :

A mon cher père Mohammed, Tu as été et tu seras toujours un exemple pour moi, aucune dédicace ne saurait exprimer mes sentiments, mes respects, ma reconnaissance et mon profond amour, que dieu bénisse son âme.

A ma chère mère Fatma, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours.

A mon cher époux Mohammed pour son respect, son affection, sa confiance et son soutien inconditionné.

A ma chère fille Ritadj, que dieu te protège, te procure la santé et longue vie.

A mes chers parents Abd El Hafid & Nouria, je tiens à dédier ce modeste travail, en leur témoignant ma profonde gratitude pour leurs confiances, leurs encouragements et leurs amours.

A mes chères sœurs, Wissem, Meriem, Malika, Ikram, Meriem, Nesrine, Zoubida et mes chers frères, vous m'avez toujours soutenu durant toutes mes études, je vous souhaite une vie pleine de joie, de bonheur et de réussite.

A tous mes cher(e)s ami(e)s, pour leurs aides et supports.

A toute ma chère famille,

A mes professeurs,

A tous ceux que j'aime, A tous ceux qui m'aiment.

Remerciements

Je tiens à remercier d'abord le tout puissant ALLAH, d'avoir guidé mes pas vers le chemin du savoir.

je tiens à adresser mes profonds remerciements et respects à Monsieur ABDERRAHIM Mohammed El Amine, Maître de Conférence A à l'Université de Tlemcen, en sa qualité de directeur de mes travaux de thèse. Son encadrement, sa présence, ses efforts, ses qualités humaines et professionnels, ses compétences et son expérience scientifique ainsi que ses recommandations m'ont guidé et orienté sur la bonne voie, durant toutes ces années.

Que Monsieur le Doyen de la Faculté de Technologie à l'Université de Tlemcen, Prof. Chikh Mohammed Amine, accepte l'expression de ma profonde gratitude pour l'honneur qu'il me fait en présidant le jury de ma thèse. Veuillez accepter ce travail maître, en gage de mon grand respect et ma profonde reconnaissance.

Mes sincères remerciements s'adressent également à Monsieur Benamar Abdelkrim, Maître de Conférence A à l'Université de Tlemcen, de me honorer d'accepter avec grande sympathie de siéger parmi les jury de ce travail. Veuillez trouvez ici l'expression de mon grand respect et mon vifs remerciements.

Aussi, je tiens à adresser mes sincères remerciements à Monsieur Souier Mehdi, Maître de Conférence A à l'Ecole Superieur De Management De Tlemcen, d'avoir accepté de juger cette thèse. Qu'il me soit permis à travers ce travail de vous témoigner mon estime et ma redevance.

Dans l'impossibilité de citer tous les noms, mes sincères remerciements vont à tous ceux et celles, qui de près ou de loin, ont permis par leurs conseils et leurs compétences la réalisation de ce travail.

Enfin, je remercie tout le corps professoral du département de génie biomédical, particulièrement l'équipe de recherche de laboratoire CREDOM, sans oublier l'équipe de recherche de laboratoire de traitements automatiques de la langue arabe.

Résumé

Le Dossier Médical (DM) informatisé comprend toutes les informations concernant un malade, ce dossier permet de stocker, rechercher et manipuler l'information saisie lors des consultations des patients. Il permet également de partager les données du patient avec les professionnels médicaux et les établissements de santé ce qui a une conséquence la coordination et la continuité des soins. La gestion des données du patient suppose donc l'existence des outils efficaces pour le Contrôle d'Accès (CA) à ces données.

L'objectif de ce travail de recherche est centré sur le CA dans les systèmes d'information en santé et plus spécifiquement sur les modèles de CA. Il s'agit donc de proposer une modélisation rigoureuse permettant de prendre en charge tous les aspects liés à la gestion sécurisée du DM informatisé.

Dans un premier temps, nous avons proposé un modèle en *XML* pour le DM dans le contexte d'une organisation de santé algérienne. Sur la base de cette modélisation, dans un second temps, nous avons développé un modèle pour le CA à ce dossier en se basant sur le modèle *Or-BAC* avec un nombre très réduit de règles d'accès.

L'implémentation et la validation du modèle proposé à l'aide des outils comme *MotOrBAC* et *Protégé* nous ont permis un passage sûr vers une spécification valide et implémentable et en conséquence le développement d'un ensemble d'outils simples et efficaces pour la prise en charge de l'aspect CA au DM.

Mots-clés : Dossier Médical Informatisé, Sécurité, Contrôle d'Accès, Or-BAC, MotOrBAC, Protégé, Organisation de santé algérienne.

Abstract

The electronic Health Record (HR) includes all the information concerning a patient, this record makes it possible to store, search and manipulate the information entered during the consultations of the patients. It also allows the sharing of patient data with professionals and health care institutions, which has the consequence of coordination and continuity of care. The management of the patient's data therefore presupposes the existence of effective tools for Access Control (AC) to these data.

The aim of this research work focused on AC in health information systems and more specifically on AC models. It is therefore a question of proposing a rigorous modelling allowing to take care of all the aspects related to the secure management of the electronic HR.

We proposed in the first time an *XML* model to the management of the electronic HR in the context of an Algerian health organization. Based on this modeling and by using *Or-BAC* model, in a second time, we proposed a model of the AC to this record with a very small number of access rules.

The implementation and validation of the proposed model using tools such as *MotOrBAC* and *Protégé* allowed us a safe passage to a valid and implementable specification and consequently the development of a set of simple and effective tools for the management of the AC aspect of the HR.

Keywords : Health Records, Security, Access Control, Or-BAC, MotOrBAC, Protégé, Algerian health organization.

Table des matières

Liste des tableaux

Table des figures

Glossaire

- DM : Dossier Médical
- DMI : Dossier Médical Informatisé
- DMP : Dossier Médical Partagé
- CA : Contrôle d'Accès
- DAC : Discretionary Access Control
- IBAC : Identity Based Access Control
- ACL : Access Control List
- HRU : Harrison, Ruzzo, et Ullmann
- TAM : Typed Access Matrix
- ATAM : Augmented TAM
- SQL : Structured Query Language
- MAC : Mandatory Access Control
- CDI : Constrained Data Item
- UDI : Unconstrained Data Item
- IVP : Integrity Verification Procedures
- TP : Transformations Procedures
- SELinux : Security-Enhanced Linux
- AppArmor : Application Armor
- Smack : Simplified Mandatory Access Control Kernel
- RBAC : Role-Based Access Control
- TRBAC : Temporal Role-Based Access Control
- uT-RBAC : Ubiquitous Role-Based Access Control Model
- Géo-RBAC : Geographical Role-Based Access Control
- CRBAC : Context Role-Based Access Control
- PS-RBAC : Pervasive Situation-aware Role-Based Access Control
- UML : Unified Modeling Language
- PTFA : Pattern Traversal Flow Analysis
- TBAC : Task Based Access Control
- TR-BAC : Task and Role-Based Access Control
- ERP : Enterprise Resource Planning
- TMAC : Team-based Access Control
- C-TMAC : Context-based Team Access Control
- PL/SQL : Procedural Language/Structured Query Language
- TT-RBAC : Team and Task Role-Based Access Control
- ABAC : Attribute Based Access Control
- PBAC : Policy Based Access Control
- SOA : Service Oriented Architecture
- XACML : Langage eXtensible Access control MarkupLanguage

- OASIS : Organization for the Advancement of Structured Information Standards
- XML : Extensible Markup Language
- PAP : Policy Administration Point
- PDP : Policy Decision Point
- PEP : Policy Enforcement Point
- PIP : Policy Information Point
- Or-BAC : Organization Based Acces Control
- EPH : Établissement Publique Hospitalier
- EPSP : Établissement Public de la Santé de Proximité
- EHS : Établissement Hospitalier Spécialisé
- AdOr-BAC : Administration model for Organization Based Acces Control
- PRA : Permission-Role Assignment
- URA : User-Role Assignment
- UPA : User-Permission Assignment
- I-OrBAC : Integrity-OrBAC
- DI-OrBAC : Distributed Integrity-Organization Based Acces Control
- D-OrBAC : Distributed-Organization Based Acces Control
- Multi-OrBAC : MultiOrganization-Based Access Control
- O2O : Organisation 2 Organisation
- VPO : Virtual Private Organization
- RSSO : Role Single-Sign-On
- P-RBAC : Privacy Role Based Access Control
- Poly-OrBAC : Poly-Organization Based Acces Control
- Trust-RBAC : Trust-Role Based Access Control
- SBAC : Semantic-Based Access Control
- OWL : Web Ontology Language
- SWRL : Semantic Web Rule Language
- ROWLBAC : Representing Role Based Access Control in OWL
- TSBAC : Temporal Semantic-Based Access Control
- MCA : Maitre de conférences A
- MCB : Maitre de conférences B
- EEG : Electroencéphalographie
- ECG : électrocardiogramme
- EMG : électromyographie
- DTD : Document Type Definition
- OCC : Objets Connectés Classiques
- OCI : Objets Connectés Intelligents
- U : Urgence
- T : Temporel
- S : Spatial
- MotOrBAC : Moteur Or-BAC
- RDF : Resource Description Framework

Introduction générale

1. Contexte de la thèse

Le Dossier Médical (DM) regroupe l'ensemble des informations administratives, médicales et paramédicales portant sur le patient. Ce dossier est sous forme de documents (physiques ou/et informatisés) qui retrace les épisodes de la maladie, l'historique des consultations, le parcours de soin d'un patient et constamment des mises à jour, il est devenu un outil capital d'exercice pour tout professionnel de santé afin d'assurer le bon suivi de l'état d'un malade.

Le DM était une simple prise de notes et d'observations, ensuite, il a été évolué jusqu'à qu'il est devenu un DM informatisé, et même partagé. L'informatisation de ce dossier permet de stocker, rechercher et manipuler l'information saisie lors des consultations des patients, elle permet également de partager les données du patient avec les professionnels médicaux et les établissements de santé ce qui mène une coordination et une continuité des soins. La gestion des données du patient suppose donc l'existence des outils efficaces pour son Contrôle d'Accès (CA).

La structure du DM peut être composée en quatre parties :
- Les données administratives : elles regroupent en général les données concernant l'identification du patient, de ses personnes de confiance, de son garde malade et de sa rencontre avec le médecin.
- Les données concernant les différentes mesures chez le patient, elles regroupent : la taille, le poids, la température, la fréquence cardiaque, la fréquence respiratoire, etc.
- Les données concourant à la coordination, qualité, continuité des soins et prévention : elles regroupent : les données médicales générales, les données de soins et de prévention, les données de la chirurgie, etc.
- Les données concernant l'espace d'expression du titulaire : elles concernent le don d'organes (le consentement écrit par le patient).

Actuellement (2019), en Algérie, un logiciel propriétaire appelé *PATIENT* est utilisé dans les bureaux des entrées des hôpitaux publiques pour faire la gestion du DM. Ce logiciel n'est pas assez développé et son utilisation est limitée uniquement aux bureaux des entrées. Il comprend plusieurs fonctions telles que l'admission, le transfert inter-services, les archives et les éditions. Il est à noter que les agents administratifs sont le seul type d'utilisateurs du logiciel *PATIENT* et que le personnel médical et paramédical n'est pas autorisé à l'utiliser.

PROBLÉMATIQUE

La sécurisation du DM est un aspect très important qui est devenue un enjeu essentiel pour instaurer un climat de confiance qui encourage le partage des données médicales, d'où le problème de comment peut-on partager et gérer le DM tout en gardant le secret médical.

OBJECTIF

Assurer l'aspect sécurité dans la gestion et le partage du DM et de protéger également les ressources informatiques contre l'utilisation non-autorisée, le mauvais usage, et la modification, tout en garantissant l'accès pour les utilisateurs légitimes. Plusieurs modèles de CA pour le DM ont été proposés, ces modèles doivent imposer ce qui est permit, ce qui est interdit et ce qui est obligé.

Le CA est un processus qui permet de garantir les critères de confidentialité, d'intégrité et de disponibilité d'une ressource accédée par un utilisateur par l'utilisation des méthodes d'identification, d'authentification, d'autorisation et de responsabilité. Cette politique de CA peut être physique, logique ou administrative. Dans le cadre de cette thèse, nous nous intéressons particulièrement aux techniques de CA logique.

Depuis les années 1960, les recherches et les travaux dans le domaine de CA ont évolué dû à des besoins initiaux dans différents secteurs et plusieurs modèles ont été mis en place dont nous pouvons classer ces modèles en deux catégories à savoir les modèles classiques ou traditionnels et les modèles évolués qui représentent des extensions des modèles classiques.

2. Contributions

L'accessibilité aux ressources d'information dans les systèmes de santé est un aspect très important. Le travail de cette thèse porte sur la protection et la sécurité des données médicales et et s'est centré principalement sur le CA dans les systèmes d'information en santé. Il s'agit donc de proposer une modélisation rigoureuse permettant de prendre en charge tous les aspects liés à la gestion sécurisée du DM informatisé.

Dans cette thèse, nous avons proposé des solutions pour pallier les problèmes liés à la gestion de la sécurité du DM. Brièvement, nous énumérons ces contributions :

1. Dans un premier temps nous avons proposé un modèle en XML pour le DM dans le contexte d'une organisation de santé algérienne.
2. Après une étude approfondie et une comparaison des différents modèles de CA qui existent dans la littérature, nous avons choisi le modèle de CA le plus approprié à savoir Or-BAC.
3. Sur la base de la modélisation XML du DM, nous avons développé, un modèle pour le CA à ce dossier en se basant sur le modèle Or-BAC. Les différentes entités et relations du modèle proposé ont été modélisées graphiquement en utilisant des diagrammes de classes UML.
4. En se basant sur les entités trouvées de notre modèle de CA, nous avons appliqué plusieurs optimisations pour obtenir à la fin un nombre réduit de règles de contrôle.

5. L'implémentation et la validation du modèle proposé à l'aide des outils comme MotOrBAC et Protégé nous ont permis un passage sûr vers une spécification valide et implémentable et en conséquence le développement d'un ensemble d'outils simples et efficaces pour la prise en charge de l'aspect CA au DM.

3. Organisation de la thèse

Dans cette thèse, nous avons suivi le plan proposé dans la figure 1 et qui se présente comme suit :

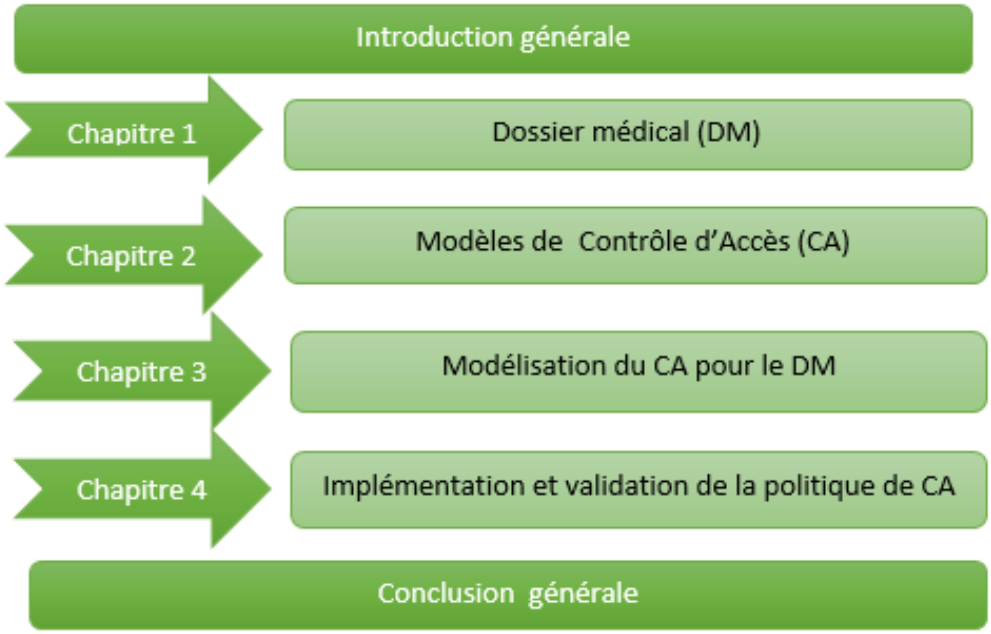


FIGURE 1 – Plan de la thèse

1. *Introduction générale :* introduit cette thèse.
2. *Chapitre 1 :* ce chapitre présente le DM pour les organisations de santé algériennes ; il comprend son historique, ses différents types, sa structure, son cycle et finalement une comparaison entre quelques logiciels de gestion de ce dossier. Sur la base des données et de la structure du DM nous avons proposé un modèle en XML pour ce DM sous la forme d'une DTD XML.
3. *Chapitre 2 :* ce chapitre présente d'abord les concepts de la politique de sécurité, ensuite, dresse un état de l'art complet sur les différents modèles de CA qui existent dans la littérature. Ils peuvent être classés selon deux catégories : modèles traditionnels et modèles évolués. Une comparaison entre les différents modèles de CA nous a permis de choisir le modèle le plus approprié dans le cadre cette thèse.
4. *Chapitre 3 :* ce chapitre présente une modélisation rigoureuse du CA pour le DM. Cette dernière est basée sur le modèle Or-BAC et compte un nombre très réduit de règles d'accès. Les différentes entités et relations du modèle proposé ont été modélisées en utilisant le langage UML.

5. *Chapitre 4 :* ce chapitre présente l'implémentation et la validation du modèle proposé à l'aide des outils MotOrBAC et Protégé qui nous ont permis un passage sûr vers une spécification valide et implémentable et en conséquence le développement d'un ensemble d'outils simples et efficaces pour la prise en charge de l'aspect CA au DM.
6. *Conclusion générale :* clôt cette thèse.

Chapitre 1

Dossier Médical (DM)

1 Introduction

Le DM regroupe l'ensemble des informations administratives, médicales et paramédicales portant sur le patient, il est devenu un outil capital d'exercice pour tout professionnels de santé afin d'assurer le bon suivi de l'état d'un malade. Ce chapitre présente le DM ; il comprend son historique, ses différents types, sa structure, son cycle et finalement une comparaison entre quelques logiciels de gestion de ce dossier.

2 Historique du DM

Un DM est un ensemble de documents (physiques ou/et informatisés) qui retrace les épisodes de la maladie, l'historique des consultations, le parcours de soin d'un patient et constamment des mises à jour. Ce dossier peut être un dossier manuel sous forme d'une enveloppe qui contient tous les documents et les informations concernant l'hospitalisation du patient, comme il peut être un dossier informatisé.

Les premières traces du DM datent du 9e siècle, époque à laquelle des médecins arabes, tels que Rhazès (865-925), Avicenne (930-1037) ou Avenzoar (1073-1162), créent la médecine clinique [8].

Avant le 14e siècle, le DM était une simple prise de notes et d'observation. Courant le 14e siècle apparait le *dossier patient* comme un support écrit, Ce support servait à la réunion et l'enregistrement des notes du médecin. Autrement dit, c'est la mémoire écrite de toutes les informations médicales concernant le patient. Également, les informations pouvaient être partagées avec d'autres médecins, équipes soignantes et/ou la famille [9].

À la fin du 18e siècle, apparaît la notion du *dossier médical personnel* pour chaque patient. Il était alors utilisé comme un cahier de notes à l'hôpital. Cependant, le contenu était simple et réduit [8] [9].

Au 19e siècle, le dossier médical inclut des données médicales, sociales et administratives, il est devenu un outil d'échange et de propagation des données entre les professionnels de santé [8].

A partir du 19e siècle, le DM inclut des données médicales (ordonnances, comptes-rendus, rapports médicaux, résultats de laboratoire, etc.), sociales et administratives il est devenu un outil primordial de communication et de transmissions des données entre les professionnels de santé [9] et ceci pour plusieurs raisons : comme l'amélioration de qualité des soins, de qualité des études dans la recherche clinique, et notamment dans le cadre de problèmes de responsabilité et de traçabilité suite à des contentieux entre patients et le corps médical [8].

Depuis le début des années 2000, Le DM Informatisé (DMI) remplace progressivement le DM papier dans les établissements [10]. Ce DMI est constitué d'informations administratives et médicales qui forment une base de données, il concerne le suivi de diagnostics, de traitements, et plus généralement tous les échanges écrits entre les professionnels de santé.

Pour les besoins de la gestion de l'assurance-maladie et à partir de 2004, le DM personnel a été proposé, il vise à ce que chaque patient dispose d'un DMI reprenant toutes ses données médicales [11].

En 2016, ce DM personnel est devenu DM Partagé (DMP) qui est un registre de santé numérique qui archive toutes les informations de santé : diagnostics, traitements, résultats d'examens, etc. Il permet de partager les informations médicales avec les professionnels de santé selon le choix du patient [12].

Actuellement (novembre 2018), en Algérie, un logiciel propriétaire appelé « PATIENT » est utilisé dans les bureaux des entrées des hôpitaux publiques pour faire la gestion du DM. Ce logiciel n'est pas assez développé et son utilisation est limitée uniquement aux bureaux des entrées.

Dans ce qui suit nous allons proposer un modèle du DM pour les organisations de la santé algérienne et ceci suite à une analyse de l'existant.

3 DM

3.1 DM physique et DM Informatisé

Le DM peut être un dossier manuel sous forme d'une enveloppe qui contient tous les documents et les informations concernant l'hospitalisation du patient, il accompagne le malade durant son séjour, une fois, il quitte l'hôpital son dossier va être destiné vers l'archive après une semaine, et il reste dans l'archive jusqu'à 5 ans. Comme il peut être un dossier informatisé. L'informatisation du DM permet de stocker, rechercher et manipuler l'information saisie lors des consultations des patients, elle sert également à partager et échanger des données médicales entre les professionnels et les établissements de santé. Le DMI assure la traçabilité de toutes les actions effectuées et le suivi du parcours hospitalier d'un patient ce qui :

- Facilite l'accès aux informations pour les professionnels de la santé.
- Aide à la décision médicale.
- Favorise la coordination et la continuité des soins.

L'informatisation du DM présente plus d'avantages par rapport au DM physique, GONNETAN Claire dans [1] a présenté une comparaison des bienfaits du DMI et du DM physique (voir tableau 1.1).

	DM physique	DMI
Stockage et communication des informations	+	+++
Intégration des données (dont données multimédias)	+	++++
Lisibilité du dossier	+	++
Prise en charge de l'ensemble des problèmes	+	++
Complétudes (domaines sélectionnés)	+	+++
Disponibilité de l'information	séquentiel, local	simultané, global
Accès à distance	0	++++
Chaînage des épisodes de soins	+	+++
Chaînage des dossiers distribués	0	++
Traitement et aide à la décision	0	++
Résumés, abstraction multiples	0	+++
Rappels, alarmes	0	+++
Suggestions diagnostiques ou thérapeutiques	0	+++
Traitement des données multimédias	0	+++
Vues différentes données	+	++
Évaluation des soins	+	+++
Recherche clinique, épidémiologique	+	+++
Contrôle de gestion, planification	0	++++
Formation et éducation	+	+
Facilité d'utilisation du dossier	+++	+
Formalisation de la démarche médicale	+	+++
Adhésion aux protocoles de soins	+	+++
Connexion à des bases de données	+	++++
Sécurité de l'information	+	++
Confidentialité	+	+

TABLE 1.1 – Les possibilités offertes par le DMI et le DM physique [1]

3.2 Structure du DM

Le DM est structuré en quatre parties (voir figure 1.1) :

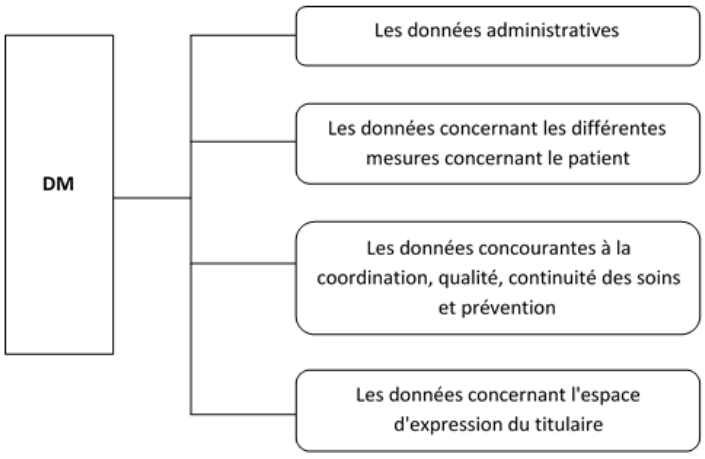


FIGURE 1.1 – Structure du DM

A. Les données administratives : elles regroupent :
   - Identification du titulaire : (identifiant, nom, prénom, date de naissance, sexe, profession, prénom père, nom mère, prénom mère, nationalité, situation familiale, nom époux, groupage, téléphone, adresse, e-mail, numéro de sécurité sociale).
   - Rencontre (nom médecin, prénom médecin, spécialité du médecin, date de rencontre, interrogatoire, lettre d'admission, motifs d'hospitalisation, décisions (le type de prise en charge prévue, prescriptions effectuées)).
   - Personnes de confiance (nom, prénom, date de naissance, lien de parenté, téléphone, adresse, e-mail).
   - Garde malade (nom, prénom, date de naissance, lien de parenté, téléphone, adresse, e-mail)

B. Les données concernant les différentes mesures concernant le patient, elles regroupent :
   - Poids, taille, sommeil, force, mouvement, mouvement fœtaux, indice de masse corporelle, potentiel hydrogène, température, fréquence cardiaque, fréquence respiratoire, pression artérielle, taux d'insuline, micro-circulation sanguine, détection de chute, l'électroencéphalographie (EEG), l'électrocardiogramme (ECG), l'électromyographie (EMG).

C. Les données concourantes à la coordination, qualité, continuité des soins et prévention : elles regroupent :
   - Les données médicales générales : antécédents (personnels, familiaux), historiques des consultations, allergies et intolérances reconnues, prothèses et appareillage.
   - Les données de soins : examens biologiques (catégories, date, résultats, comptes rendus, URL), examens d'imageries radiologiques ou d'autres imageries (catégories, date, résultats, comptes rendus, URL), pathologies en cours, traitements prescrits et administrés, soins reçus.
   - Les données de prévention : facteurs de risque individuels, traitements préventifs prescrits, calendrier des vaccinations.
   - Les données de la chirurgie : (design de la chirurgie, heure de la chirurgie, nom chirurgien, prénom chirurgien, nom anesthésiste, prénom anesthésiste, protocole de la chirurgie, compte-rendu).
   - Compte-rendu d'accouchement : (heure de l'accouchement, nom sage-femme, prénom sage-femme, nom gynécologue, prénom gynécologue, nom anesthésiste, prénom anesthésiste).
   - Résumé de sortie : (mode de sortie, certificat de sortie, ordonnances, rendez-vous).

D. Les données concernant l'espace d'expression du titulaire : elles concernent le don d'organes (le consentement écrit par le patient).

Le DM comprend des données structurées et d'autres non structurées, la modélisation des différentes parties de ce dossier en utilisant la DTD (Document Type Definition) se trouve en annexe A [13].

3.3 Cycle du DM

Le DM est créé pour un patient lors de son arrivée à un établissement hospitalier, ce patient arrive soit évacué d'un autre établissement de santé avec une fiche de transfert, soit il passe par les urgences et selon la décision du médecin généraliste il sera hospitalisé. Ce patient passe par la suite par le bureau des entrées, il présente l'accord du médecin et sa carte d'identité, l'agent administratif inscrit son entrée et lui établi un bulletin d'admission (Voir annexe B) et une fiche navette qui peut être soit pour un hôpital du jour soit pour une hospitalisation (Voir annexe C). Lors de son hospitalisation, si ce patient nécessite un garde-malade, il sera également présenté au bureau des entrées avec une carte d'identité et un document qui prouve le lien de parenté avec le malade, il sera inscrit sur son bulletin d'admission.

Par la suite, le patient sera placé dans un service et tout acte effectué pour ce patient durant son hospitalisation doit être renseigné par le personnel médical et paramédical dans sa fiche navette en précisant sa nature, la date et l'heure. Les mouvements du patient entre les services ; doivent être également renseignés dans son dossier. Lors de la sortie du patient de l'hôpital, une carte d'hospitalisation où il trouve le prochain rendez-vous renseigné, des ordonnances et une facture des frais symboliques lui seront délivrés.

La secrétaire médicale établie le résumé standard de sortie (Voir annexe D), et envoie le dossier au bureau des entrées. Dans ce bureau, un agent administratif enregistre la sortie du malade, son mode de sortie et classe le dossier du patient dans les archives où il va rester jusqu'à 5 ans avant sa destruction. La figure 1.2 présente le cycle du DM.

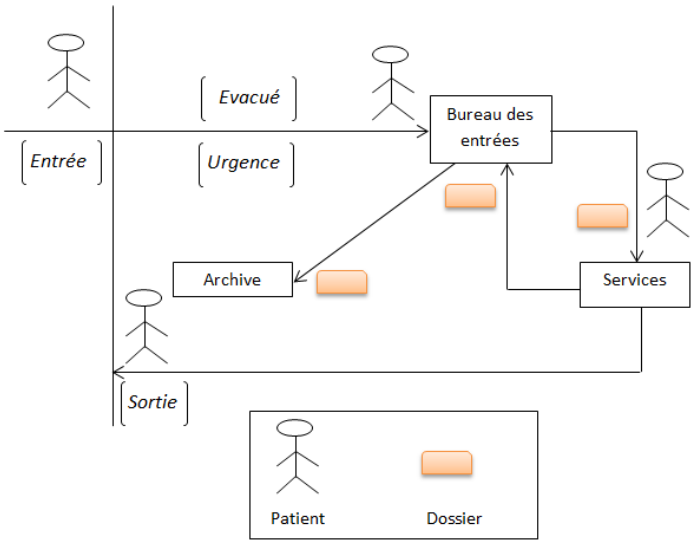


FIGURE 1.2 – Cycle du DM

3.4 Logiciels de gestion du DM

Actuellement (décembre 2018), en Algérie, il s'avère qu'il n'existe pas encore un modèle formel de DM. Par ailleurs, un logiciel propriétaire « PATIENT » est

utilisé dans les bureaux des entrées des hôpitaux publiques. Ce logiciel n'est pas assez développé et son utilisation est limitée uniquement aux bureaux des entrées. Suite à un stage effectué dans le centre hospitalo-universitaire Dr Tidjani Damerdji de Tlemcen, j'ai pu découvrir le logiciel PATIENT avec ces différentes fonctionnalités.

3.4.1 Logiciel PATIENT

Le logiciel de gestion des patients "PATIENT" (version 18 - 09.10) est réalisé par Mme ABDI (CHU Mustapha Pacha, Alger) en collaboration avec Mr BENAKACI (Ministère de la Santé, de la Population et de la Réforme Hospitalière MSPRH) en 2009, il est utilisé dans les bureaux des entrées des hôpitaux publiques, son interface utilisateur regroupe une liste des fonctions et les agents administratifs accèdent à cette interface en utilisant un code utilisateur et un mot de passe (voir figure 1.3).

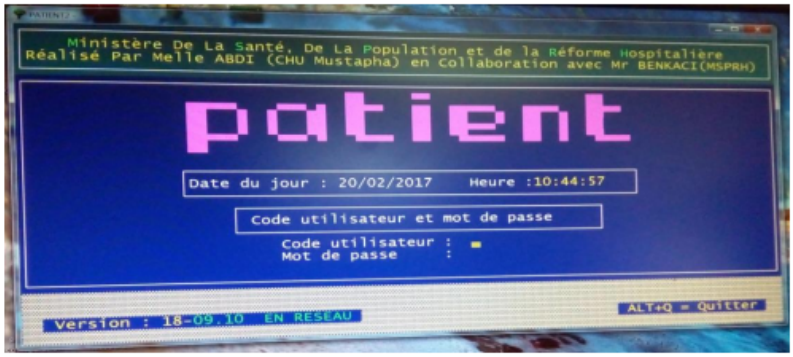


FIGURE 1.3 – Logiciel PATIENT

Le logiciel PATIENT regroupe la liste des fonctions suivantes :

1. Admission : permet de saisir le bulletin d'admission d'un patient et de son garde-malade (nom, prénom, date de naissance, mode d'admission, sexe, profession, groupage, téléphone, e-mail, etc.) (Voir annexe B).
2. Transfert inter-services : permet de saisir les informations de transfert d'un patient d'un service à un autre (service d'origine, service d'évacuation, date et heure d'évacuation, etc.) (Voir annexe E.1).
3. Renseignement : permet de rechercher un patient de l'année en cours ou à partir de l'archive (Voir annexe E.2).
4. Sortie : permet de saisir les informations de sortie d'un patient (nom, prénom, service d'origine, service de sortie, date de sortie, mode de sortie, résumé standard de sortie, etc.) (Voir annexe E.3).
5. Décomptes : permet de saisir la fiche navette d'un patient (nom, prénom, date d'entrée et de sortie, acte établissement d'hospitalisation, etc.) pour calculer la facture, néanmoins cette fonction de calcul n'est pas utilisée actuellement (Voir annexe E.4).
6. Édition : cette fonction est utilisée pour l'impression d'un ensemble de documents comme : bulletin d'admission, certificat de séjour (Voir annexe E.5), déclaration de naissance et de décès, résumé standard de sortie, etc.

7. Données nationales : cette fonction contient des paramètres de l'application qui concerne la mise à jour des wilayas, des communes, des services, des médicaments, des actes professionnels, etc (Voir annexe E.6).
8. Maintenance : pour réaliser des opérations sur la base de données comme par exemple l'indexation des bases de données ou la restauration des données à partir des archives (Voir annexe E.7).
9. La mise à jour du fichier utilisateur : dans cette partie, l'administrateur peut ajouter un utilisateur avec ses droits d'accès. Il lui donne une initiale et un mot de passe, ensuite, il lui attribue des droits d'accès selon son type. Il peut aussi supprimer ou désactiver cet utilisateur (Voir annexe E.8). Il faut noter que le seul type d'utilisateurs du logiciel PATIENT est l'agent administratif et que le personnel médical et paramédical n'a pas le droit de l'utiliser.

Il existe dans la littérature plusieurs logiciels de gestion du DM, dans ce qui suit nous allons présenter quelques logiciels librement disponibles sur le net.

3.4.2 Logiciel ClinicGate

Le logiciel de gestion du DM ClinicGate [1] présente plusieurs fonctions intéressantes (voir figure 1.4) [14] :

1. La gestion des coordonnées des patients (informations civiles, antécédents, maladies) le tout étant accompagné d'images.
2. La gestion financière avec une prise en compte des frais d'hospitalisation, des remboursements des assurances ou tout simplement de la gestion globale du budget d'un ou plusieurs services.
3. La gestion des emplois du temps.
4. La gestion des médicaments et des entrées/sorties.

FIGURE 1.4 – Logiciel ClinicGate

1. https ://goo.gl/Mx4hgS

3.4.3 Logiciel GBE

Le logiciel GBE [2](la gestion du bien-être) des cabinets médicaux présente les fonctionnalités suivantes (voir figure 1.5) [15] :

1. La gestion des patients (coordonnées du patient, sa pathologie, la liste des consultations et des différents documents, la fiche du médecin traitant).
2. La possibilité de rechercher un patient via son numéro de téléphone.
3. La gestion des agendas.
4. La gestion des messageries (la possibilité de transmettre des mails aux patients directement via le logiciel).
5. La gestion des mots de passe au lancement du logiciel.

FIGURE 1.5 – Logiciel GBE

3.4.4 ERP MEDICAL

ERP MEDICAL [3] est une application créée pour aider le personnel médical et paramédical dans la gestion des patients et des consultations prévues, c'est un outil adapté pour les cliniques et les petits bureaux médicaux. Cette application présente les différentes fonctions suivantes (voir figure 1.6) [16] :

1. Elle permet de créer une base de données avec tous les patients, de planifier des événements, de gérer les résultats de diagnostic et les traitements.
2. Elle permet de créer, modifier et supprimer des entrées.
3. Elle permet de télécharger des images radiologiques associées à un patient.

2. http ://www.gestionbienetre.com/lelogiciel.html
3. https ://goo.gl/0GLSqe

FIGURE 1.6 – Logiciel ERP MEDICAL

3.4.5 Logiciel Elixir

Elixir [4] est un logiciel de gestion de cabinet médical totalement gratuit [17], c'est le fruit d'une collaboration entre une équipe de développeurs en informatique et des médecins, il présente les fonctionnalités suivantes (voir figure 1.7) [18] :

1. La gestion des patients, des consultations (les examens cliniques, les bilans biologiques et radiologiques, les ordonnances, etc.).
2. La gestion de l'archive médicale.
3. La gestion des rendez-vous et des courriers.
4. La gestion des médicaments, des finances, etc.

FIGURE 1.7 – Logiciel ELIXIR

4. https ://dawhois.com/site/elixir-sante.com.html

3.4.6 Logiciel Consult

Consult [5] est un logiciel de gestion spécifique pour les professionnels des médecines alternatives, il offre les fonctions suivantes (voir figure 1.8) [19] [13] :

1. La gestion des patients : affiche les coordonnées du patient, les résultats aux différents tests, édition automatique de l'autorisation parentale pour les mineurs, l'attestation de suivi et une fiche du patient détaillée reprenant l'historique de ces consultations.
2. La gestion des agendas : intègre une gestion des rendez-vous (au jour, à la semaine ou au mois) avec possibilité d'adresser aux patients un rappel des rendez-vous à venir. Cet agenda est compatible avec Google Agenda et se synchronise automatiquement.
3. La gestion des consultations : mémorise le résumé de chaque consultation (le suivi du poids, l'historique des précédentes consultations, etc.).
4. La gestion des honoraires : suivi des honoraires avec édition de la note d'honoraire et la possibilité d'éditer un récapitulatif des honoraires perçus pour une période donnée.
5. La gestion des protocoles : les protocoles peuvent être conservés dans une bibliothèque intégrée.

FIGURE 1.8 – Logiciel Consult

3.4.7 Logiciel Medimust

Medimust [6] est développé pour les machines MAC, PC, ou smartphones. C'est un logiciel d'aide à la prescription qui permet de télé transmettre des feuilles de soins [20], son interface regroupe les fonctionnalités suivantes (voir figure 1.9) :

1. La gestion des patients : l'identification du patient, l'historique médical, antécédents, allergies, résumé des consultations, bilans biologiques, courriers et compte-rendus.

5. https ://goo.gl/ltzmZw
6. https ://wiki.medimust.com/index.php/Accueil

2. La gestion des consultations : la saisie et l'enregistrement des consultations.
3. La gestion des ordonnances : ce module de prescription de Medimust contrôle les interactions médicamenteuses, les allergies, intolérances et hypersensibilités, les incompatibilités avec l'état physiopathologique du patient (grossesse, allaitement, âge, etc.), les produits dopants et gère aussi les traitements chroniques des patients.
4. La gestion des images et des examens médicaux.
5. La gestion des courriers, des messageries et des télétransmissions.
6. La gestion de l'agenda et de salle d'attente.
7. La gestion du DM personnel qui est un dossier médical informatisé, accessible sur l'internet.

FIGURE 1.9 – Logiciel Medimust

3.4.8 Logiciel Medibord

T.Despoix et R.Ollivier ont développé l'application Mediboard[7] pour la gestion d'établissement de santé. Cette application présente les fonctions suivantes (voir figure 1.10) [21] :

1. La gestion des identités des patients.
2. La gestion de consultations médicales et chirurgicales.
3. La gestion des séjours.
4. La gestion des feuilles d'admissions, consentements, fiches d'information et ordonnances.
5. La gestion des antécédents et des allergies.
6. La gestion des alertes partagées entre les professionnels de santé et le personnel d'établissement.
7. La gestion des dossiers de soins infirmiers et de circuit du médicament.

7. http ://www.mediboard.org

8. La gestion des dossiers d'anesthésie.

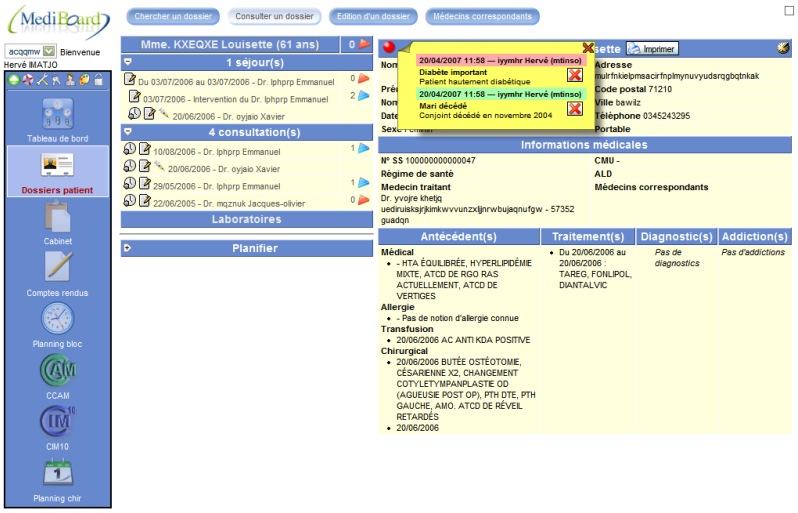


FIGURE 1.10 – Logiciel Medibord

Le tableau 1.2 présente une comparaison du logiciel « PATIENT » avec les logiciels actuellement disponibles sur le net.

	Patient	Clinic Gate	GBE	Medical ERP	Elixir	Consult	Medi must	Medi Board
Patients	+	+	+	+	+	+	+	+
Accès	+	+	+	+	+	+	+	+
Personnels	+	+	+	+	+	-	+	+
Consultations	+	+	+	+	+	-	+	+
Protocoles	+	-	+	-	+	+	-	+
Médicaments	+	+	-	+	+	-	+	+
Actes médicaux	+	+	-	-	+	-	+	+
Admission	+	+	+	+	+	+	+	+
Hospitalisation	+	+	-	-	-	-	-	+
Agendas	-	+	+	-	+	+	+	-
Rendez-vous	-	+	+	+	+	+	+	+
Messagerie	-	+	+	+	+	-	+	-
Comptabilité	+	+	+	+	+	+	+	+
Statistiques	+	-	-	+	+	-	+	+
Ordonnances	-	+	-	+	+	-	+	+
Certificats	+	-	-	-	+	-	+	+
Archive	+	-	+	-	+	+	+	+

TABLE 1.2 – Comparaison des logiciels du DM

D'après cette étude comparative (voir tableau 1.2), nous avons remarqué que par exemple la gestion et l'admission des patients sont implémentées dans tous

les logiciels tandis que la gestion du personnels, des médicaments, des protocoles, des actes médicales, etc. est implémentée dans quelques logiciels. Ces logiciels peuvent être des systèmes de gestion de cabinet médicale ou des systèmes de gestion des hospitalisations. Le logiciel Elixir regroupe toutes les fonctionnalités sauf l'hospitalisation.

4 Conclusion

Dans ce chapitre, nous avons présenté les données et la structure du DM pour les organisations de santé algériennes et ceci suite à une analyse de l'existant. Sur la base de ces données et de cette structure nous avons proposé un modèle en XML pour ce DM sous la forme d'une DTD XML. Par la suite, nous avons comparé le logiciel PATIENT avec les logiciels de gestion du DM disponibles librement et ou gratuitement sur le net.

La sécurisation du DM constitue un enjeu essentiel pour instaurer un climat de confiance qui encourage le partage des données médicales, d'où le problème de comment peut-on partager et gérer le DM tout en gardant le secret médical. Pour ce faire, plusieurs modèles de Contrôle d'Accès (CA) pour le DM ont été proposés, ces modèles doivent imposer ce qui est permit, ce qui est interdit et ce qui est obligé. Dans le chapitre suivant, nous allons décrire ces modèles pour passer ensuite au choix d'un modèle approprié supportant la structure et le contenu du DM.

Chapitre 2

Modèles de Contrôle d'Accès (CA)

1 Introduction

La sécurisation des systèmes d'informations est un aspect très important qui est devenue un enjeu majeur pour les différents systèmes ainsi que pour l'ensemble des acteurs qui l'entourent, dont l'objectif est la protection des ressources informatiques contre l'utilisation non-autorisée, le mauvais usage, la divulgation et la modification, tout en garantissant l'accès pour les utilisateurs légitimes. Pour assurer cette sécurité, plusieurs techniques ont été proposées dont nous pouvons citer : le CA, la sécurité par chiffrement de l'information (la cryptographie), la sécurité logique, la sécurité physique, la sécurité administrative, la sécurité des systèmes d'exploitation, la sécurité des communications, etc. Dans le cadre de notre travail, nous nous intéressons au CA.

Le but de ce chapitre est de dresser un état de l'art complet sur les politiques de sécurité, les principaux modèles et les architectures de CA.

2 CA

Le CA est un processus qui permet de garantir la protection des critères de confidentialité [1], d'intégrité [2] et de disponibilité [3] d'une ressource (objet) accédée par un utilisateur (sujet) par le biais des méthodes suivantes :

- L'identification : c'est un processus qui consiste à établir l'identité de l'utilisateur. Elle permet de répondre à la question : "Qui êtes-vous ?". L'utilisateur utilise un identifiant "Nom d'utilisateur" qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.
- L'authentification : c'est un processus qui cherche à certifier de l'identité d'un utilisateur. Elle intervient après la phase d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connaît.

1. Concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées.
2. Concept permettant de restreindre la modification des données aux personnes autorisées.
3. Concept permettant de rendre une donnée accessible lorsqu'un utilisateur autorisé en a besoin.

– L'autorisation : c'est un processus qui permet de lier formellement et légitimement le sujet et la ressource à travers des droits ou permissions.
– La responsabilité : c'est un processus qui permet de tracer avec des détails les étapes de permissions pour s'assurer que l'opération faite sur la ressource est conforme à la politique de CA [22].

Il existe trois types de CA : physique, logique et administratif [22] :

1. Physique : ce sont toutes les méthodes qui restreignent physiquement l'accès à une ressource : des murs d'enceinte, une porte avec verrous, etc.
2. Logique/Technique : ce sont des méthodes logicielles permettant de limiter l'accès.
3. Administratif : ce sont toutes les méthodes organisationnelles qui visent à juridiquement engager la responsabilité des personnes, qui précisent les règles à respecter, qui sensibilisent à la sécurité informatique.

Dans le cadre de cette thèse, nous nous intéressons particulièrement aux techniques de CA logique.

Un modèle de CA est défini par les éléments : Sujet, Contrôle, Action, Objet. Un sujet peut avoir une permission, une interdiction, une obligation ou une recommandation afin de réaliser une action sur un ou plusieurs objets (voir figure 2.1).

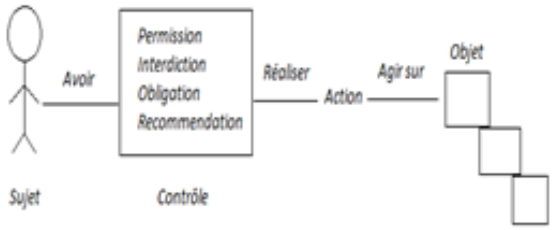


FIGURE 2.1 – Composants d'un processus de CA

– Sujet : représente l'ensemble des utilisateurs comme les médecins, les infirmiers, etc.
– Contrôle : représente les contrôles suivants :
  – Permission : action d'autoriser un sujet pour effectuer une action, par exemple : un médecin est autorisé de consulter le dossier médical de son patient.
  – Interdiction : action d'interdire un sujet pour réaliser une action, par exemple : les médecins n'ont pas le droit de supprimer les identifications des patients.
  – Obligation : action automatique et obligatoire dans un système, par exemple : une fois qu'un médecin accède à un dossier d'un patient qui n'est pas à lui, un message est automatiquement envoyé à son chef de service.
  – Recommandation : action permettant de définir des règles de sécurité utilisant une modalité de recommandation, par exemple :
    – Si le patient est mineur ou souffrant de troubles mentaux ou psychologiques, la présence du tuteur est recommandée.
– Action : les actions sont regroupées en activités qui correspondent aux divers services offerts aux utilisateurs, à titre d'exemple, nous citons :

  - Ajouter des documents au dossier patient.
  - Modifier des informations d'un patient.
- Objet : représente une donnée dans le dossier patient, par exemple : le nom du patient, la date de consultation, etc. Il faut noter que nous pouvons regrouper les objets dans des ensembles d'objets.

Il existe dans la littérature plusieurs modèles de CA, dans la section suivante, nous allons présenter l'état de l'art de ces différents modèles.

3 Modèles de CA

Depuis les années 1960, les recherches et les travaux dans le domaine de CA ont évolué dû à des besoins initiaux dans le secteur aussi bien militaires que civils. Le secteur militaire nécessite un CA dû principalement aux nombreuses données confidentielles qu'il peut contenir tandis que le secteur civil se limite au contrôle des intégrités. À partir des années 1970, beaucoup de modèles de CA ont été mis en place.

Nous pouvons classer ces modèles en deux catégories à savoir les modèles classiques ou traditionnels (DAC, MAC, RBAC, TBAC, TMAC, ABAC et Or-BAC) et les modèles évolués (IBAC, HRU, Take-Grant, TAM, Bell-LaPadula, Biba, Clark et Wilson, la muraille de Chine, TRBAC, uT-RBAC, Géo-RBAC, CRBAC, TR-BAC, C-TMAC, PBAC, Multi-OrBAC, Organisation virtuelle, O2O, Poly-OrBAC, Trust-RBAC, CA basé sur trust et risque, P-RBAC, SBAC, ROWLBAC, TSBAC, CA basé sur l'intelligence artificielle).

3.1 Modèles de CA traditionnels

En 1970, les modèles de CA et les modèles de contrôle de flux sont introduits comme les premiers modèles de sécurité. La différence entre ces modèles réside dans la représentation de l'autorité d'administration. Il existe plusieurs variantes de ces politiques de sécurité, dans la suite, nous allons dresser un état de l'art sur les différents modèles de CA.

3.1.1 Modèle de CA discrétionnaire (DAC)

La politique de CA basée sur le modèle DAC (Discretionary Access Control), accorde au propriétaire de l'information, généralement le créateur, tous les droits d'accès ainsi que la possibilité de les propager aux autres selon sa discrétion [23]. C'est-à-dire le responsable de l'information décide quels sont les sujets (utilisateurs) qui peuvent accéder aux objets (information des patients). Il existe plusieurs modèles associés au modèle DAC, dans les sous-sections suivantes, nous allons présenter ces extensions.

3.1.1.1 Modèle de CA basé sur l'identité (IBAC) Le modèle IBAC (Identity Based Access Control) a été proposé par Lampson en 1971 [24] sous la forme de matrice (voir tableau 2.1) : les lignes représentent les sujets et les colonnes représentent les objets. L'intersection d'une ligne avec une colonne constitue le droit

d'accès (lecture, écriture, exécution). Par exemple, le sujet S_1 (ligne 1) a le droit d'accéder en lecture, écriture et exécution à l'objet O_1 (colonne 1) par ailleurs, le sujet S_1 n'a pas le droit d'accès à l'objet O_N.

Sujet /Objet	O_1	...	O_N
S_1	Lecture Ecriture Exécution	...	Pas d'accès
S_2	Lecture	...	Ecriture
...	...	...	...
S_N	Pas d'accès	...	Exécution

TABLE 2.1 – Matrice de CA

Ce modèle repose sur une matrice composée d'un ensemble fini d'entités, de ressources cibles et de règles. Il conduit à l'établissement d'une liste exhaustive d'autorisations d'accès ACL (Access Control List). Cela implique que tout accès non clairement permis est interdit. Ainsi, les habilitations sont affectées directement aux comptes utilisateurs [25].

Ce modèle a été ensuite redéfini par Graham et Dening qui ont précisé des règles pour créer, supprimer des objets, transférer et donner des permissions d'accès afin de mettre à jour la matrice d'accès.

3.1.1.2 Modèle de CA HRU Ce modèle fut formalisé par Harrison, Ruzzo, et Ullmann, sous l'abréviation « HRU » en 1976 [26], où les auteurs se sont intéressés aux propriétés vérifiées par un système de CA lorsque son état change. Ce changement s'effectue par l'intermédiaire des commandes exécutant des opérations primitives sur les autorisations sous des conditions spécifiées.

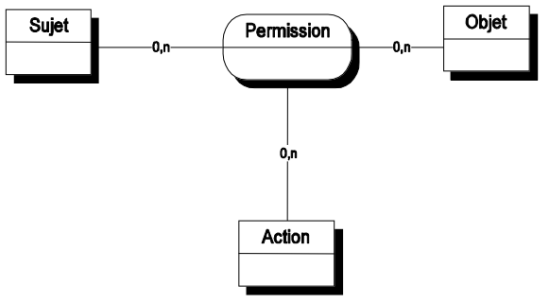


FIGURE 2.2 – Le modèle HRU [2]

Dans ce modèle, la politique de sécurité est réduite à l'expression des permissions ; ces dernières sont sous forme de relations entre les sujets, les objets et les actions. Elles sont représentées dans la matrice *A* des permissions. Si *s* est un sujet et *o* est un objet alors, *A(s, o)* définit l'ensemble des actions *A* que le sujet *s* est permis à faire sur l'objet *o* [2].

3.1.1.3 Modèle de CA Take-Grant Ce modèle a été développé par Jones et al. en 1976 [27], il est constitué d'un graphe dont les nœuds sont des sujets ou

des objets, et des règles de modification de ce graphe [28]. Le graphe est une autre représentation de la matrice d'accès. Lorsque le sujet *S* possède un droit d'accès *A* sur l'objet *O*, un arc étiqueté par le droit *A* est dessiné entre *S* et *O*. La mise à jour des droits d'accès, c'est-à-dire du graphe s'effectue à l'aide des quatre commandes suivantes [29] :

1. La commande **create** qui permet de créer un objet et d'attribuer initialement un droit d'accès à un sujet sur cet objet.
2. La commande **remove** qui permet de retirer un droit d'accès d'un sujet sur un objet.
3. La commande **take** indique qu'un sujet *S* peut prendre tous les droits qu'un sujet (ou objet) *R* possède.
4. La commande **grant** qui permet à un sujet *S* possédant un droit d'accès *A* sur un objet *O* ainsi que le droit *G* sur un autre sujet *R*, de céder à *R* le droit *A* sur *O* (que *S* possède sur *O*).

3.1.1.4 Modèle de CA TAM En 1992, Sandhu [30] a présenté un modèle appelé TAM (Typed Access Matrix) s'inspirant du modèle HRU. Dans TAM, chaque objet appartient à un certain type qui ne peut changer. Les commandes utilisent cette notion de type. Ensuite, Ammann et Sandhu ont proposé une version "augmentée" de TAM, appelée ATAM (Augmented TAM), afin de fournir un moyen simple de détecter l'absence de droits dans une matrice d'accès. Les auteurs étudient la question de savoir si le fait de tester l'absence de droits d'accès ajoute un pouvoir d'expression fondamental. Ils montrent que TAM et ATAM sont formellement équivalents par leur pouvoir expressif. Cependant, leur construction indique que, bien que les tests d'absence de droits soient théoriquement inutiles, de tels tests semblent être bénéfiques dans la pratique [31].

3.1.1.5 Avantages et inconvénients du modèle de CA DAC Le modèle de CA DAC présente les avantages suivants [32] [33] :

- Une autorité peut donner les autorisations.
- Le détenteur d'un objet peut donner aux autres utilisateurs les privilèges d'administration sur un objet.
- Il est simple à mettre en œuvre.
- C'est le plus implanté sous UNIX et SQL (Structured Query Language).
- Le modèle DAC est considéré comme satisfaisant pour ce qui concerne les besoins de gestion de sécurités d'accès dans l'industrie et les organismes gouvernementaux civils.

Le modèle de CA DAC souffre des inconvénients suivants [32] [34] [35] :

- Le problème de fuite d'information : le propriétaire de l'information, a tous les droits d'accès ainsi que la possibilité de les propager aux autres selon sa discrétion.
- Cheval de Troie : c'est un programme qui, sous couvert de réaliser une action légitime, réalise à l'insu de la personne qui l'utilise une autre action qui peut consister en une attaque contre la sécurité du système [36].

Voici un exemple qui illustre comment le Cheval de Troie peut amener à une fuite d'information vers des utilisateurs non permis : supposons dans un hôpital, X est un directeur, il va créer un fichier *état de santé du patient 1* contenant des informations très sensibles sur le patient 1. Ces informations sensibles, d'après la politique de l'hôpital, ne devraient être accessibles que par X. Supposons maintenant qu'un utilisateur malveillant Y, un codirecteur de X, veuille récupérer cette information sensible, pour cela, Y crée un fichier *observation* et donne l'autorisation à X d'écrire dans ce fichier. Y, ensuite, introduit deux opérations cachées dans l'application utilisée par X. Ces opérations sont *lire* dans le fichier *état de santé du patient 1* et *écrire* dans le fichier *observation*. Une fois que X exécute l'application, les opérations *lire* et *écrire* vont être permises. Puisque l'utilisateur malveillant Y est le propriétaire du fichier *observation* il pourra accéder à ce fichier et récupérer les informations désirées [34].

- Peut ne pas être utilisable pour l'implémentation de certains principes de sécurité, comme la confidentialité des données.
- Les modèles DAC sont assez statiques car si la matrice d'accès avec une taille grande est mise en place, sa modification peut être complexe.

Quelques domaines d'application de la politique de sécurité basée sur le modèle DAC [37] :

- Les modèles de CA DAC furent les premiers modèles implantés dans les systèmes informatiques notamment le système de fichiers d'UNIX.
- Malgré certaines limites que nous avons présenté, Ils restent, cependant, utilisés dans de nombreuses applications modernes. Le modèle de sécurité de Facebook, par exemple, est typiquement un modèle de sécurité discrétionnaire où les utilisateurs définissent les autorisations relatives aux données qu'ils publient.

3.1.2 Modèle de CA obligatoire (MAC)

Pour résoudre les problèmes des modèles DAC, les politiques de CA obligatoire MAC (Mandatory Access Control) ajoutent des règles incontournables. L'une des manières de faire est d'affecter, aux objets et aux sujets, des attributs qui ne sont pas modifiables par les usagers, ce qui limite leur pouvoir de gérer les accès aux informations qu'ils possèdent [36]. Ces politiques sont généralement des politiques multi-niveaux qui supposent que les utilisateurs et les objets aient été étiquetés par niveaux comme par exemple : Top secret, Secret, Confidentiel, Unclassified. Les règles qui régissent les autorisations d'accès sont basées sur une comparaison de l'habilitation de l'utilisateur et de la classification de l'objet.

La figure 2.3 représente un modèle de CA qui permet la lecture en bas et l'écriture en haut. En effet, un sujet peut lire des informations si son habilitation est supérieure à la classification de ces informations et peut écrire dans des objets si son habilitation est inférieure à la classification de ces objets [3].

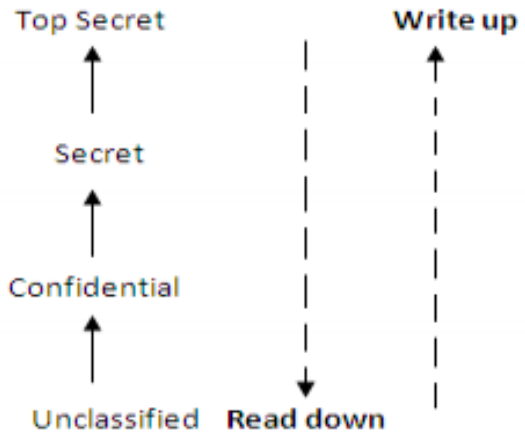


FIGURE 2.3 – Sécurité multi-niveaux [3]

Il existe plusieurs extensions du modèle MAC dont nous allons les citer dans les sous-sections suivantes.

3.1.2.1 Modèle de CA Bell-LaPadula Ce modèle a été proposé pour la première fois par David Bell et Leonard Lapadula en 1976 [38] dans le cadre de la réalisation d'un système informatique de sécurité pour les forces aériennes américaines du département de défense [23], il vise à préserver la confidentialité des données, c'est-à-dire :

- Interdire toute fuite d'information d'un objet possédant une certaine classification vers un objet possédant un niveau de classification inférieur [28].
- Interdire à tout sujet possédant une certaine habilitation d'obtenir des informations d'un objet d'un niveau de classification supérieur à cette habilitation [28].

Pour maintenir la confidentialité, des restrictions sont imposées sur les opérations de lecture et d'écriture, qui permettent de transférer des informations. Ces restrictions se traduisent par les deux principes suivants :

- *No read up* : Un sujet ne peut lire un objet que si la classe d'accès du sujet domine celle de l'objet [34](un sujet ne doit pas apprendre des informations qui ne lui sont pas autorisées.).
- *No write down* : Un sujet ne peut écrire dans un objet que si la classe d'accès de l'objet domine celle du sujet [34] (un sujet ne doit pas révéler des secrets.).

3.1.2.2 Modèle de CA Biba Ce modèle a été proposé pour la première fois par Ken Biba en 1977 [39], il vise à préserver l'intégrité des données, c'est-à-dire :

- Interdire toute propagation d'information d'un objet situé à un certain niveau d'intégrité vers un objet situé à un niveau d'intégrité supérieur [28].
- Interdire à tout sujet situé à un certain niveau d'intégrité de modifier un objet possédant un niveau d'intégrité supérieur [28].

Pour maintenir l'intégrité, des restrictions sont imposées sur les opérations de lecture et d'écriture, qui permettent de transférer des informations. Ces restrictions se traduisent par les deux principes suivants :

– *No read down* : un sujet peut lire un objet si la classe d'accès de l'objet domine celle du sujet [23].
– *No write up* : un sujet peut écrire dans un objet si la classe d'accès du sujet domine celle de l'objet [23].

3.1.2.3 Modèle de CA Clark et Wilson En 1987, Clark et Wilson ont proposé ce modèle [40], qui permet de garantir la protection de l'intégrité des données dans un système commercial. Il vise à assurer les besoins suivants :

– Une cohérence des données faisant partie de l'état interne du système. Ce type de cohérence peut être imposé par le système de calcul [28].
– Une cohérence entre l'état interne du système informatique et le monde réel qu'il représente [28].

La politique de Clark et Wilson repose sur deux anciens principes bien connus :

– Les transactions bien formées : les utilisateurs doivent utiliser des procédures de transformation spécifiques qui préservent l'intégrité pour pouvoir manipuler les données [28].
– La séparation des pouvoirs : fondé sur la répartition des pouvoirs entre plusieurs parties, et l'attribution des droits différents, mais complémentaires, à différentes catégories de personnes [28].

Dans ce modèle, les concepts importants à définir sont [41] :

– Les données contraintes CDI (Constrained Data Item) : représentent les items des données qui visent à préserver l'intégrité.
– Les données non contraintes UDI (Unconstrained Data Item) : représentent les items dont l'intégrité n'est pas garantie et qui peuvent être manipulés de façon aléatoire.
– Procédures pour la vérification de l'intégrité IVP (Integrity Verification Procedures) : servent à confirmer que tous les CDI dans le système sont conformes aux spécifications de l'intégrité au moment où les IVP sont exécutés.
– Procédures de transformation TP (Transformations Procedures) : correspondent au concept de transactions bien formées. Le but est de changer les CDI d'un état valide à un autre état valide.

3.1.2.4 Modèle de CA de la muraille de Chine Ce modèle a été développé par Brewer et Nash en 1989 [42], afin de fournir un CA à l'information qui peut évoluer dynamiquement, il a été développé pour réduire les conflits d'intérêts [4] dans des organisations commerciales et pour assurer également la propriété de confidentialité [3].

L'objectif de ce modèle de CA est de garantir qu'aucun utilisateur n'accède simultanément à des données appartenant à des ensembles en conflit d'intérêts. En effet, si un organisme financier est amené à traiter des opérations pour le compte de deux clients en concurrence directe, le personnel de cet organisme doit pouvoir accéder qu'aux informations concernant l'un de ces deux clients.

4. Un conflit d'intérêts survient lorsqu'un sujet a accès aux informations confidentielles de deux organisations en compétition permettant ainsi un flot d'informations d'une organisation vers une autre.

Au départ, l'utilisateur a le libre choix, mais une fois que les informations d'un client connues, tout accès aux informations concernant l'autre doit être interdit. Sa décision dresse donc devant lui une barrière qu'il ne peut plus franchir, d'où le nom de muraille [28].

3.1.2.5 Avantages et inconvénients du modèle de CA MAC Le modèle de CA MAC offre les bienfaits suivants [34] [32] [33] [35] :

- Résolve le problème de fuite d'information des modèles DAC et limite la diffusion de l'information.
- Limite les risques dus à des attaques de type Cheval de Troie.
- Sépare la gestion des droits d'accès, de l'accès lui-même,
- Bien adapté aux applications où la protection du secret et de l'intégrité est primordiale.

La politique de sécurité obligatoire souffre des inconvénients suivants [34] [32] [33] [35] :

- Modèle sévère qui impose des contraintes fortes.
- 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 accéder, pour des raisons exceptionnelles, à la donnée de niveau de sécurité top secret.
- Les informations circulent de façon unidirectionnelle dans un treillis où il n'y a de canaux cachés [5]où l'information serait susceptible d'être détournée. En effet, même si ces canaux cachés peuvent être identifiés, ils sont très coûteux à supprimer.

Voici quelques applications du modèle de CA MAC [43] :

La politique de sécurité obligatoire est une politique dédiée à Linux tel que SELinux (Security-Enhanced Linux), AppArmor (Application Armor), Tomoyo et Smack (Simplified Mandatory Access Control Kernel) :

- SELinux : il permet de définir une politique de CA obligatoire aux éléments d'un système issu de Linux, il fournit les mécanismes nécessaires pour assurer la confidentialité et l'intégrité des différents objets du système.
- AppArmor : c'est un logiciel de sécurité qui permet à l'administrateur système d'associer à chaque programme un profil de sécurité qui restreint ses accès au système d'exploitation. Il complète le traditionnel modèle d'UNIX du CA DAC en permettant d'utiliser le CA MAC.
- Tomoyo : c'est un module de sécurité du noyau Linux qui implémente le CA obligatoire, il est utilisé pour augmenter la sécurité d'un système, tout en étant utile en tant qu'outil d'analyse de système.
- Smack : c'est un module de sécurité du noyau Linux, permettant d'implémenter une politique de sécurité obligatoire basée sur des labels.

5. Un canal caché est un canal de transmission entre deux ordinateurs qui utilise la bande passante d'un autre canal dans le but est de transférer des informations sans l'autorisation ou la connaissance du propriétaire de l'information ou de l'administrateur du réseau

3.1.3 Modèle de CA à base de rôle (RBAC)

La politique de sécurité basée sur les rôles RBAC (Role-Based Access Control) a été proposée pour la première fois dans les années 90 [44] [45], son principe est que les permissions sont associées aux utilisateurs à travers des rôles. Un rôle représente une fonction définie dans l'organisation (par exemple, médecin, infirmier, etc.) [28], c'est une entité intermédiaire entre utilisateurs et droits d'accès. On associe à chaque rôle un ensemble de permissions.

La figure 2.4 présente le modèle de CA RBAC ou un rôle peut avoir différentes permissions et une permission peut être attribuée à plusieurs rôles. Tous les sujets ayant reçu l'autorisation de jouer un rôle héritant alors des permissions associées à ce rôle [46]. Par exemple, si le médecin *Mohamed* est à la fois médecin spécialiste et chef service, il aura le droit d'accès aux dossiers médicaux, en tant que médecin spécialiste, alors qu'en tant que chef service, il pourra accéder aux dossiers administratifs.

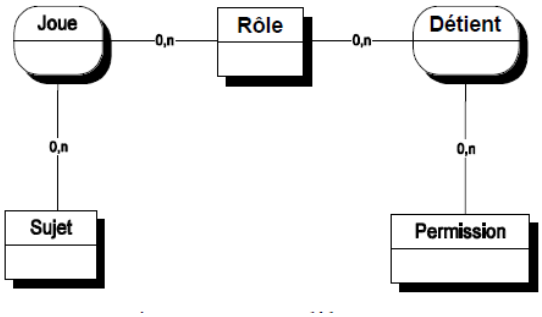


FIGURE 2.4 – Le modèle de CA RBAC [2]

Des différentes variantes du modèle de CA RBAC ont été proposées, selon R.Thion et S.Coulondre [47] nous pouvons citer les variantes suivantes :

- $RBAC_0$: représente le modèle de base qui contient les éléments minimaux d'un modèle de CA à base de rôle (utilisateurs, rôles, permissions, sessions).
- $RBAC_1$: représente le modèle $RBAC_0$ +hiérarchie des rôles, par exemple, un médecin peut hériter de toutes les permissions attribuées à un infirmier.
- $RBAC_2$: représente le modèle $RBAC_0$ +contraintes, par exemple un utilisateur ayant deux rôles ne peut pas les activer en même temps. D'autres contraintes peuvent être considérées comme les contraintes temporelles et spatiales [34].
- $RBAC_3$: représente $RBAC_1$+$RBAC_2$.

La figure 2.5 illustre les variantes du modèle RBAC.

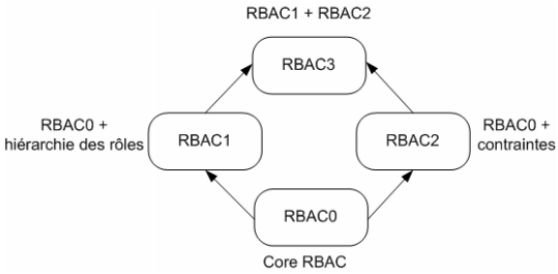


FIGURE 2.5 – Les variantes du modèle RBAC [4]

Dans la suite, nous allons présenter les différentes extensions de la politique de sécurité RBAC.

3.1.3.1 Modèle de CA TRBAC En 2001, Les travaux de Bertino et al. [48] ont étendu le modèle RBAC vers le modèle TRBAC (Temporal RBAC) dont l'axe temporel est considéré comme une contrainte qui peut déterminer l'activation et la désactivation d'un rôle. L'intégration de l'aspect temporel a donné plus de flexibilité pour créer des exceptions pour les individus et pour spécifier des dépendances temporelles entre les actions réalisées par un utilisateur [49].

3.1.3.2 Modèle de CA uT-RBAC En 2006, Chae et al. ont proposé le modèle uT-RBAC (Ubiquitous Role-Based Access Control Model) pour la prise en compte du contexte [50], et qui considère le temps et la localisation de l'utilisateur comme des éléments importants pour l'activation et désactivation d'un rôle [49].

3.1.3.3 Modèle de CA Géo-RBAC En 2007, Bertino et al. ont proposé une nouvelle extension du modèle RBAC, c'est le modèle Geo-RBAC (Geographical RBAC) [51] qui permet de définir la localisation d'un utilisateur soit par son positionnement physique exact (à l'aide d'un GPS) ou à travers son positionnement logique calculé implicitement (à travers la région dans laquelle il se déplace, cette région peut être définie à différentes granularités, par exemples : route, ville, région) [49].

Ce modèle défini de nouveaux concepts spatiaux pour représenter la position des utilisateurs et celles des objets. Ces nouveaux concepts sont utilisés pour limiter géographiquement l'utilisation des rôles. Il est très précis pour répondre à la nécessité de prendre en compte la localisation géographique, dans la construction d'une règle de politique de sécurité [52].

3.1.3.4 Modèle de CA Context RBAC adapté aux besoins des systèmes pervasifs En 2006, Park et al. ont proposé le modèle CRBAC (Context RBAC) [53] pour faire face aux exigences des applications des systèmes pervasifs, avec la prise en compte de la localisation de l'utilisateur, son état et les horaires d'utilisation [54]. Ensuite en 2008, Kulkarni et al. ont proposé une autre extension du

modèle RBAC adaptée également aux besoins des systèmes pervasifs [55] et qui sépare la gestion du contexte du CA pour faciliter la prise de décision dans le cas où une autorisation est liée à plusieurs contraintes contextuelles. Dans ce modèle un droit d'accès à une ressource est autorisé à partir d'un ensemble de contraintes contextuelles [49].

3.1.3.5 Avantages et inconvénients du modèle de CA RBAC Le modèle de CA RBAC offre les avantages suivants [36] [46] [28] [56] :

- Facilite la compréhension de la structure de l'organisation.
- Réduit la complexité de gestion des droits d'accès.
- Les différents rôles sont tirés directement de la structure de l'organisation considérée.
- Plus facile à administrer, en effet, l'intégration de nouveaux utilisateurs, la gestion des permissions ou même la définition de nouveaux objectifs dans la politique de sécurité en sont grandement facilités.
- Fournit un bon compromis entre MAC et DAC.
- Les différentes extensions ont rendus le modèle RBAC plus adapté aux contraintes du temps réel des systèmes pervasifs.

Par conséquent, ce modèle souffre de quelques inconvénients comme [46] [56] [2] :

- Le fait que tous les utilisateurs ayant le même rôle ont les mêmes privilèges, et par conséquent, il y a la difficulté de préserver la confidentialité, en effet, n'importe quel utilisateur jouant le rôle médecin peut accéder aux dossiers de tous les patients, y compris ceux qu'il ne les traite pas.
- Il n'est pas possible dans le modèle RBAC d'exprimer d'autres permissions contextuelles comme l'urgence, le médecin traitant, etc. Plus précisément, si une certaine permission est accordée à un rôle, alors tous les utilisateurs qui jouent ce rôle héritent de cette permission. Par conséquent, il n'y a aucun moyen de spécifier qu'un médecin n'a la permission d'accéder au dossier médical d'un patient que si ce dernier est son patient.

D'après la littérature, il existe des travaux qui ont utilisé le modèle de CA RBAC dont nous citons :

- En 2005, R.Thion, S.Coulondre ont proposé une approche qui permet de prendre en compte le contexte spatio-temporel dans le CA mobile aux systèmes d'informations. Pour cela, les auteurs ont utilisé la logique du premier ordre pour exprimer de façon homogène les contextes spatio-temporels combinés afin de former des contextes complexes et des rôles traditionnels (fonctionnels, hiérarchiques). Ensuite, ils ont présenté le langage générique LORAAM qui permet de développer des applications à CA mobiles, dans lesquelles le critère de confidentialité est pris en compte dès la conception du modèle logique de données. À partir de ce langage générique, ils ont montré comment l'implanter, de deux manières différentes, l'une appelée approche framework, l'autre par le biais d'un modèle objet à rôles [57].
- En 2009, DA. Kukhun et F. Sèdes ont proposé le modèle PS-RBAC (Pervasive Situation-aware RBAC) qui est une extension du modèle RBAC. L'objectif derrière ce modèle est de permettre la construction d'autorisations

flexibles qui s'adaptent au changement de droits d'accès causé par la mobilité de l'utilisateur. Leur contribution prend en compte les attributs contextuels de l'utilisateur et la situation dans laquelle il consulte le système afin de lui fournir des propositions d'accès à des ressources alternatives [49].

– En 2011, K. Eddine a proposé une démarche qui permet de réduire l'écart qui existe entre les modèles d'application et les modèles de sécurité, pour cela, il a intégré le modèle RBAC dans les diagrammes cas d'utilisation et de séquence, cette intégration se traduit par un diagramme de classe qui définit les éléments du modèle RBAC et le diagramme UML (Unified Modeling Language). L'auteur a utilisé la théorie des graphes comme un moyen formel pour détecter les incohérences qui existe entre la politique de CA et le modèle d'application modélisé en UML. Ensuite, il a proposé un simulateur qui offre à l'utilisateur la possibilité de créer des sessions et d'activer des rôles. Finalement, il a ajouté un générateur de code en XML qui permet de générer le code de la partie sécurisée [58].
– En 2018, A. Aaron et al. ont proposé un nouveau paradigme "ORGODEX" pour le CA basé sur les rôles ,c'est un nouveau modèle et une méthodologie concrète pour l'ingénierie des systèmes évolutifs à base de rôles RBAC dans les grandes organisations ou les employés ont besoin d'accès à l'information sur le principe du besoin de savoir. Ils ont d'abord motivé la nécessité de nouvelles relations structurelles RBAC, en distinguant les rôles et les responsabilités ou un rôle comme chef de service d'un hôpital est identifié et attribué des responsabilités. Ensuite, ils ont présenté leur nouveau modèle pour décrire et raisonner les implémentations RBAC, ils ont produit une nouvelle méthodologie itérative pour l'ingénierie des systèmes de CA évolutifs. Enfin, les auteurs ont validé leur travail avec une étude de cas selon laquelle le modèle et la méthodologie ORGODEX sont utilisés pour déployer l'autorisation en tant que service dans le contexte du cloud computing [59].
  En 2018, L. Papineau et M.André ont travaillé avec les applications Web qui sont très courantes, et qui ont des besoins de sécurité, l'un d'eux est le CA. Ces applications utilisent régulièrement le modèle de CA RBAC qui permet aux développeurs de définir des rôles et d'assigner des utilisateurs à ces rôles. De plus, l'assignation des privilèges d'accès se fait au niveau des rôles. Les applications Web évoluent durant leur maintenance et des changements du code source peuvent affecter leur sécurité de manière inattendue, pour s'attaquer à cette problématique, les auteurs ont proposé des analyses statiques de programmes autour de la protection garantie des privilèges [60].

3.1.4 Modèle de CA à base des tâches (TBAC)

Ce modèle a été proposé pour la première fois en 1993 par Thomas et Sandhu [61], TBAC (Task Based Access Control) fut le premier modèle à introduire le concept de tâche [6], il a été développé afin d'activer une autorisation par rapport

6. Une tâche se décompose en plusieurs actions élémentaires, au sein d'une organisation, elle permet de surveiller les activités réalisées par les utilisateurs d'un système d'information.

aux tâches effectuées par l'utilisateur. Son principe consiste à ajouter la notion de tâche dans des règles de permissions [52]. Les politiques de sécurité TBAC propose de structurer droits d'accès selon les tâches que les utilisateurs du système d'information doivent réaliser, mais sans concept de rôle.

Exemples de tâches

- La tâche admission du malade se décompose de l'identification de patient, rencontre du patient avec le médecin, les informations concernant le garde malade et la personne de confiance.
- La tâche suivie des différentes mesures de patient se décompose de suivi de température, de pression artérielle, de taux d'insuline, etc.
- La tâche diagnostic du patient se décompose de suivi des données médicales générale, suivi des données de soins, suivi des données de prévention, etc.

Il existe une extension du modèle de CA TBAC, c'est le modèle TR-BAC présenté dans la sous-section suivante.

3.1.4.1 Modèle de CA TR-BAC En 2001, Bertino et al. ont défini le modèle de CA TR-BAC (Task and Rôle BAC) [62] afin d'intégrer la notion de rôle [52]. Dans ce modèle, les droits d'accès sont activés en fonction d'un rôle et portent sur la réalisation des tâches. Par exemple l'utilisateur *Mohamed* joue le rôle médecin et effectue la tâche diagnostiquer un patient.

3.1.4.2 Avantages et inconvénients du modèle de CA TBAC La politique de CA à base de tâches présente les avantages suivants [35] [63] :

- Bien adapté pour les activités de traitement de l'information avec de multiples points d'accès.
- Les autorisations sont constamment surveillées.
- Les droits d'accès sont activés et désactivés en conformité avec des contextes accordés à des tâches.

Cette politique de sécurité ne prend pas en compte des contraintes sur les horaires ou les périodes d'accès pendant lesquels les utilisateurs sont en charge de réalisation de leurs activités et ceci présente un inconvénient pour cette politique [52].

Il existe dans la littérature certains travaux qui ont utilisé le modèle de CA TBAC et TR-BAC dont nous citons :

- En 1998, G.Coulouris et al. ont développé un schéma de CA basé sur les rôles et les tâches pour être utilisé dans une classe d'activités impliquant une coopération entre les principaux utilisateurs dans une entreprise virtuelle qui est un environnement largement distribué, ils ont choisi ce modèle pour répondre à l'exigence d'un schéma de CA générique indépendant du code de l'application. Le modèle a été mis en œuvre pour une plateforme logicielle offrant un accès partagé à des grappes d'objets distribués répliqués [64].
- En 2003, S.Oh et al. ont proposé un modèle de CA amélioré pour les environnements d'entreprise, ils ont examiné les caractéristiques du CA dans un environnement d'entreprise et ils ont introduit un modèle de CA TR-BAC

basé sur le concept de classification des tâches. Le modèle proposé traite chaque tâche différemment selon sa classe et prend en charge la hiérarchie des rôles de CA et de supervision au niveau tâche [65].
- En 2003, Deng et al. ont introduit le modèle de CA TBAC, qui modélise les tâches dans le flux de travail et gère les autorisations de manière dynamique à travers les tâches et l'état de tâches. Ce modèle convient parfaitement à l'informatique distribuée, aux activités de traitement de l'information avec de multiples points d'accès, à la prise de décision dans le flux de travail et aux systèmes de gestion de transactions distribués. Les auteurs ont introduit les concepts de base de TBAC [66].
- En 2010, F.Jian-Biao et al. ont présenté une combinaison de modèles de CA basés sur des rôles et des tâches, ils ont décrit en détail la relation d'affectation entre l'utilisateur, les rôles, les autorisations, et d'autres éléments, ainsi que les règles de contrainte dynamique et statique du modèle, afin de garantir l'efficacité de cette méthode de CA hybride. Les auteurs ont introduit le modèle de CA TR-BAC dans le système de gestion des périphériques dans les ERP (Enterprise Resource Planning) pour garantir la faisabilité de l'accès aux informations dans le processus [67].

3.1.5 Modèle de CA par équipes (TMAC)

En 1997, Thomas a défini une politique de CA par équipe TMAC (Team-based Access Control) [68] dont le l'objectif était de fournir un CA pour les systèmes d'information ayant des activités qui imposent la collaboration et la coopération de différents utilisateurs. L'entité de base de ce modèle est l'équipe qui est une abstraction qui regroupe un ensemble d'utilisateurs, ayant des rôles différents et qui coopèrent afin d'accomplir une tâche ou un objectif commun [28] par exemple dans le domaine médical une équipe de soins qui se compose d'un professeur, médecins, infirmiers, aides-soignants collaborent dans le but de diagnostiquer un patient. Le contexte de collaboration d'une équipe donnée, doit tenir compte de ces deux principes :
- Contexte utilisateur : les utilisateurs qui forment l'équipe à un moment donné,
- Contexte objet : les instances des objets que l'équipe utilise pour accomplir sa tâche [36].

Ce modèle de CA a été étendu pour tenir compte de la notion de contexte, ce nouveau modèle est présenté dans la sous-section suivante.

3.1.5.1 Modèle de CA C-TMAC En 2001, une extension appelée C-TMAC (Context-based Team Access Control) à TMAC a été proposée par Georgiadis et al. [69], pour l'intégration de la notion de contexte[7]. Ce modèle utilise un mélange des notions RBAC et TMAC, il est constitué de cinq entités : utilisateurs, rôles, privilèges, équipes et contextes.

Une équipe peut avoir plusieurs contextes et le même contexte peut être attribué à plusieurs équipes. De la même manière, un utilisateur peut être membre de

7. Contexte : spécifie des règles de sécurité spécifiques à certain conditions réelle qui entourent un fait.

plusieurs équipes et une équipe peut avoir plusieurs utilisateurs. Des contraintes existent lors de l'attribution des utilisateurs aux équipes. Par exemple, un utilisateur qui a été affecté aux rôles médecin et directeur ne peut pas participer dans une équipe de soins comme directeur [34].

3.1.5.2 Avantages et inconvénients du modèle TMAC La politique de sécurité basée sur le modèle TMAC offre un moyen de CA dans un cadre de travail collaboratif et elle est facilement mis à jour [34] [36]. Mais elle souffre d'un inconvénient majeur concernant la gestion des droits d'accès. Cela est lié, plus précisément, à l'ensemble des permissions offertes à l'équipe qui peut violer le principe du moindre privilège. D'après cette politique un utilisateur rejoignant une équipe renforce les permissions de cette équipe en ajoutant les siens. Néanmoins, dans le secteur médical, bien que les professionnels de santé appartiennent à la même équipe dans le même hôpital, ils n'ont pas forcément les mêmes droits d'accès sur les parties du DM du patient. Logiquement, il est évident que les permissions finales du médecin doivent être différentes de celle de l'infirmière même s'ils appartiennent à la même équipe [34].

Quelques travaux qui utilisent le modèle de CA TMAC et C-TMAC ont été proposé dans la littérature dont nous citons :

- En 1999, W. Wang a examiné dans son travail comment intégrer le modèle RBAC dans un contexte d'organisation en équipe et comment appliquer ce CA aux structures hypermédia. Sur la base de l'analyse de ces problèmes, l'auteur a proposé une politique de sécurité basée sur les équipes et les rôles, qui décrit divers aspects du CA basé sur les rôles dans des environnements hypermédia coopératif. Le modèle a été implémenté dans un système coopératif de support de processus basé sur l'hypermédia. Les exemples d'application montrent que ses autorisations de gestion de contexte d'organisation et d'autorisation d'accès conservent la simplicité de RBAC. Les extensions proposées fournissent un CA efficace et flexible pour la gestion de divers types d'espaces de travail partagés, en particulier des espaces de processus partagés, où le CA est utilisé non seulement pour gérer la sécurité, mais également pour prendre en charge la coordination [70].
- En 2002, Georgiadis et al. ont implémenté expérimentalement le modèle C-TMAC pour répondre aux exigences de sécurité spécifiques aux applications de santé. Ils ont présenté l'architecture opérationnelle du système utilisée pour implémenter les composants de sécurité C-TMAC dans un intranet de soins de santé. Les auteurs ont utilisé la plate-forme technologique d'un système de gestion de bases de données Oracle et un serveur d'applications pour coder la logique de l'application avec des procédures PL/SQL (Procedural Language/Structured Query Language) stocké, qui incluent des routines SQL dynamiques. Le système de sécurité actif qui en résulte s'adapte aux besoins actuels des utilisateurs lors de l'exécution et fournit une granularité détaillée des autorisations. Outre les certificats d'identité pour l'authentification, il utilise des certificats d'attribut pour la communication de méta-données de sécurité critiques, telles que l'appartenance à un rôle et la participation à une équipe d'utilisateurs [71].

– En 2006, A.Abou El Kalam et Y.Deswarte ont présenté un modèle de CA qui se base sur une utilisation croisée des rôles et des groupes d'objets comme étant deux moyens de structuration assez flexible qui se complètent pour supporter la richesse des systèmes d'information et de communication en santé. De la même manière que le rôle lie les utilisateurs aux privilèges, les groupes d'objets permettent d'établir une relation entre les opérations et les objets à protéger. Les auteurs ont également introduit la notion de contexte afin de permettre un CA respectant le principe du moindre privilège tout en garantissant une flexibilité favorisant le profit des patients [56].
– En 2007, Zhou et al. ont introduit un nouveau paradigme pour le CA et la gestion des autorisations, c'est le modèle TT-RBAC (Team and Task Role-Based Access Control). Ce modèle étend le modèle RBAC en ajoutant des ensembles de deux éléments de données de base appelés équipes et tâches. Ce modèle dans son ensemble est fondamentalement défini en termes d'utilisateurs individuels attribués à des rôles et à des équipes, de rôles et de tâches attribués à des équipes et d'autorisations attribuées à des rôles et à des tâches. En vertu de l'appartenance à une équipe, les utilisateurs ont accès aux ressources de l'équipe spécifiées par les tâches attribuées. Cependant, pour chaque utilisateur, le privilège exact qu'il obtient d'une équipe est déterminé par ses rôles et l'activité actuelle de l'équipe. Le modèle TT-RBAC peut donc offrir plus de flexibilité que le modèle RBAC traditionnel [72].

3.1.6 Modèle de CA basé sur les attributs (ABAC)

En 2005, E.Yuan et J.Tong ont proposé une politique de sécurité basée sur les attributs ABAC (Attribute Based Access Control) [73] dans le but de trouver des solutions concernant les difficultés que rencontrent les architectures web services en terme de sécurité. Ce modèle de CA définit les autorisations d'accès sur la base des caractéristiques de chaque entité, appelées attributs [74]. Ces attributs sont classés en quatre groupes qui se distinguent selon le type de l'entité à laquelle ils s'appliquent :

1. Les attributs des sujets : un sujet est une entité qui peut agir sur une ressource. À chaque sujet, on affecte des attributs qui définissent son identité et ses caractéristiques. Par exemple le nom, le prénom, etc. peuvent être considéré comme des attributs d'un sujet.
2. Les attributs des ressources : une ressource est une entité qui peut être accessible à un sujet. Par exemple dans le cadre médical, une ressource peut être un dossier dont des attributs comme son type (administratif ou médical), sa date de création, etc. peuvent être associés.
3. Les attributs d'action : une action est un service offert aux sujets comme une opération de lecture ou écriture, ces opérations ont aussi des attributs, par exemple le type, la date, etc.
4. Les attributs d'environnement : l'environnement peut être définit par des informations opérationnelles, techniques, liées à la situation ou encore au contexte dans lequel l'accès à l'information se produit. Le modèle de CA ABAC prend en compte la notion du contexte d'exécution du système, en

définissant des attributs d'environnement, comme par exemple : des attributs qui traitent des aspects temporels ou géographiques du scénario de CA.

3.1.6.1 Modèle de CA basé sur la politique (PBAC) Le CA basé sur la politique PBAC (Policy Based Access Control) est une harmonisation et une normalisation du modèle ABAC au niveau d'une entreprise, à l'appui d'objectifs concrets de gouvernance, ce modèle ne s'applique que dans des environnements centralisés. Il combine les attributs de la ressource, de l'environnement, du demandeur et de l'information relative à l'ensemble particulier de circonstances dans lesquelles la demande d'accès a été formulée, ce modèle utilise des ensembles de règles qui déterminent si l'accès est autorisé conformément à la politique de l'organisation concernant ces attributs et dans des circonstances données [75].

3.1.6.2 Avantages et inconvénients du modèle ABAC La politique de sécurité basée sur les attributs présente les avantages suivants [74] [76] [25] :

- La gestion de contexte en utilisant les entités d'environnement a permis d'obtenir des modèles plus souples, qui peuvent s'adapter à différentes situations.
- ABAC permet plus de flexibilité dans la prise de décision.
- Un modèle beaucoup plus adéquat pour résoudre le problème de CA au sein de l'architecture orientée services SOA (Service Oriented Architecture).
- L'utilisation des attributs offre une granularité très fine pour définir les règles de CA : il suffit de définir un attribut pour prendre en compte un nouveau paramètre entrant en jeu dans la définition des droits d'accès, qu'il s'applique aux sujets, aux ressources ou aux environnements.
- Avec les variétés d'attributs qui peuvent être assignés aux objets et aux sujets, ABAC offre une grande flexibilité relativement au nombre de sujets et d'objets qui peuvent être gérés par le système sans se préoccuper de l'aspect individuel des relations entre ces derniers.

Comme tous les autres modèles, le modèle ABAC souffre de quelques inconvénients dont nous pouvons citer [76] :

- Le modèle de CA ABAC présente plus de difficultés quant à la gestion et au contrôle des autorisations utilisateurs.
- La méconnaissance des politiques à prendre en charge par ce modèle peut augmenter sa complexité et réduire ses capacités.
- Plus difficile d'appliquer des politiques d'entreprise centralisées.

Dans la sous-section suivante, nous allons présenter un langage qui permet l'expression des politiques de sécurité ABAC.

3.1.6.3 Langage XACML (Langage eXtensible Access control MarkupLanguage) En 2005, l'OASIS (Organization for the Advancement of Structured Information Standards) a standardisé le langage de CA XACML basé sur le langage XML (Extensible Markup Language) [52] et qui permet l'expression de politiques selon une approche ABAC [77]. XACML inclut deux langages à savoir un langage réglementaire de type requêtes/réponses pour la prise de décision et un langage

pour la définition de politique [74]. Le langage de politique XACML décrit les exigences de CA en termes de contraintes sur les attributs des sujets, des ressources, des actions et de l'environnement [77]. Plus précisément, les attributs peuvent être des propriétés du sujet, de la ressource, de l'action, ou de l'environnement dans lequel la requête est faite. Les attributs ont un identifiant, un nom, un type de données, et une valeur [52].

Notions de langage XACML

Une politique de CA dans XACML est exprimée par un ensemble de règles et une cible (target). L'élément cible permet d'identifier la politique ou les règles applicables à une requête d'accès. Il spécifie les conditions que le sujet, la ressource et l'action doivent vérifier afin qu'une politique ou une règle soit applicable à la ressource requise. Une règle de CA est un ensemble de conditions et une décision (permit, ou deny). Ainsi, il est encore possible de regrouper les politiques de CA en des ensembles de politiques (PolicySet) et ce, pour structurer les politiques et les règles [5].

Architecture de gestion de langage XACML

L'architecture de gestion du langage XACML décrit les différentes entités et leurs rôles liés au processus de décision de CA. La figure 2.6 présente une version globale de cette architecture. Le *context handler* est l'entité du système qui est responsable de convertir les requêtes d'accès dans le format natif de l'application en une forme de contexte XACML. Il convertit également les décisions d'autorisation de la forme XACML en une réponse dans le format natif de l'application [5]. Les spécifications XACML décrivent l'architecture modulaire suivante [52] [5] [74] :

1. Le PAP (Policy Administration Point) prend les politiques écrites par les administrateurs de sécurité et les rend disponibles au PDP (Policy Decision Point). Ces politiques représentent la politique de gestion complète qui contrôle les décisions prises par le PDP.
2. L'utilisateur transfert sa requête au PEP (Policy Enforcement Point), point de mise en exécution des politiques.
3. Le PEP envoie la requête d'accès au *context handler* au format natif (langage supporté par le PEP), en y introduisant optionnellement les attributs des sujets, des ressources, des actions et de l'environnement.
4. Le *context handler* construit un contexte de requête XACML et l'envoie au PDP.
5. Le PDP peut demander au *context handler* des attributs supplémentaires pour le sujet, la ressource, et l'environnement.
6. Le *context handler* demande ces attributs du PIP (Policy Information Point).
7. Le PIP obtient les attributs demandés d'une source extérieure (base de données SQL, etc.) et retourne les attributs demandés au *context handler*.
8. Le *context handler* transfert les attributs demandés au PDP qui évalue la politique de CA.
9. Le PDP retourne le contexte de réponse XACML (incluant la décision d'autorisation) au *context handler* .

10. Le *context handler* traduit le contexte de réponse XACML au format de réponse du PEP et retourne la réponse au PEP qui applique la décision d'autorisation.

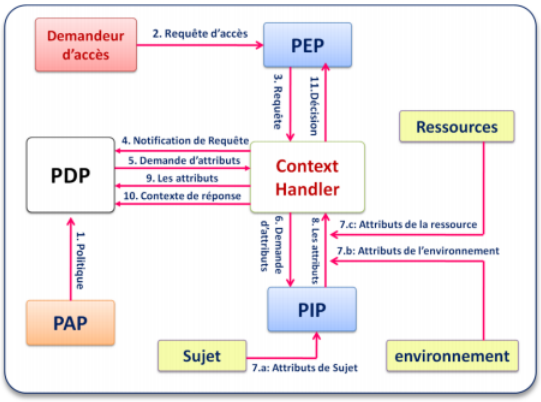


FIGURE 2.6 – Architecture de gestion de langage XACML [5]

D'après la littérature il existe des travaux qui ont utilisé le modèle de CA ABAC et le standard XACML dont nous citons :

- En 2012, M.ABAKAR à mis en œuvre une architecture de CA basée sur les attributs et le langage XACML [74] dont l'utilisateur demande un service à un fournisseur de services, celui-ci analyse la requête de l'utilisateur et déduit le règlement à partir de la base des règles de CA. Ce règlement contient des circonstances à satisfaire par l'utilisateur pour obtenir l'autorisation d'accès à la ressource demandée, il passe par trois modules : le module d'analyse de règlements, le module de récupération de données et le module de validation de règlements [74].
- En 2012, M.CHEAITO a proposé une méthodologie de conception et de développement d'un système d'autorisation adaptable aux différentes facettes que peut recouvrir le CA dans les organisations telles que l'hétérogénéité des pratiques organisationnelles, des technologies utilisées et des contextes à considérer [52]. Sa contribution est basée sur deux approches : le CA basé sur des attributs (ABAC) qui permet de spécifier des permissions par rapport à toute caractéristique liée à la sécurité des utilisateurs, des actions, des ressources, de l'environnement et la gestion à base de politiques (PBAC) qui garantit la flexibilité et l'adaptation à l'infrastructure existante. L'auteur a choisi le standard XACML comme technologie cible, car il met en œuvre ces deux approches.
- En 2015, BENDIAB a défini un système de CA flexible et puissant basé sur les attributs au niveau des APIs du Cloud Computing pour garantir un niveau de protection adéquat des ressources protégées accessibles au travers ces interfaces [5]. Elle a choisi le langage XACML pour implémenter les politiques de CA de son modèle.
- En 2016, R.Laborde a présenté des contributions à la gestion de la sécurité des infrastructures virtuelles, ces travaux reposent sur l'adaptabilité des systèmes de gestion à base de politiques. Les auteurs ont traité des aspects de prises de décisions et de mise en œuvre des politiques de sécurité [78].

Les réalisations ont été effectuées sur des implémentations du standard XACML, car ils utilisent cette technologie dans le cadre de leurs recherches sur la gestion des accès et des identités. Cependant, leurs concepts sont valides de manière plus générale pour les systèmes de gestion basés sur des politiques ABAC.

3.1.7 Modèle de CA à base d'organisation (Or-BAC)

Le modèle de CA Or-BAC (Organization Based Acces Control) a été proposé pour la première fois en 2003 par A. Abou El Kalam et al. [2], dans cette politique de sécurité, l'entité centrale est l'organisation [79] où une organisation peut être vue comme un groupe organisé de sujets [35], chacun joue un rôle spécifique et tous ses autres concepts sont définis par rapport à cette organisation. A partir des relations ternaires (habilite, utilise et considère), le modèle Or-BAC définit les relations qui existent entre les entités du niveau concret (sujets, objets, et actions) et les entités du niveau abstrait (rôles, vues et activités) [2]. La figure 2.7 montre la structuration des différentes entités du modèle Or-BAC et leurs relations.

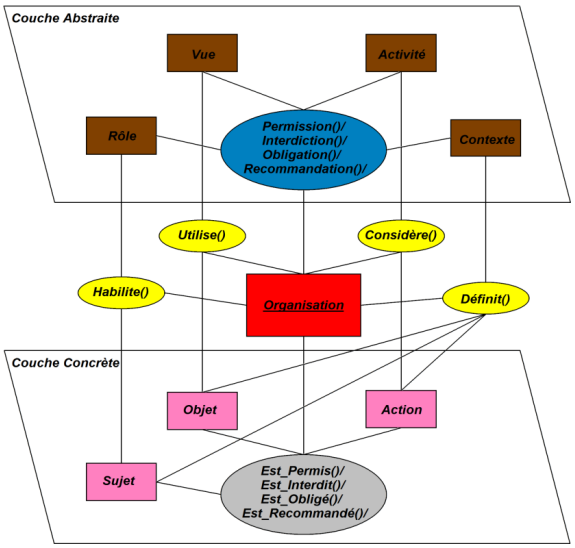


FIGURE 2.7 – Les différentes entités du modèle Or-BAC et leurs relations [6]

La politique de sécurité Or-BAC est basée sur un ensemble d'entités et de relations :

1. **Organisations**
   L'entité centrale dans le modèle de CA Or-BAC est l'organisation où une organisation peut être vue comme un groupe structuré d'entités actives, c'est-à-dire de sujets jouant certains rôles [2]. Par exemple dans le domaine médical, nous pouvons considérer "Hôpital, EPH (Établissement Publique Hospitalier), EPSP (Établissement Public de la Santé de Proximité), service des urgences, etc." comme des organisations.
2. **Sujets et Rôles**
   Dans la politique de sécurité Or-BAC, l'entité *Sujet* peut être soit une entité active, c'est-à-dire un utilisateur, par exemple, 'Asma', 'Mohamed', etc. soit

une organisation, par exemple, 'hôpital', 'le service des urgences de l'hôpital', etc. Tandis que l'entité *Rôle* est utilisée afin de relier les sujets et les organisations, et pour faciliter la mise à jour de la politique de CA lorsqu'un nouvel utilisateur est ajouté. Dans le domaine médical, les rôles "médecin" ," infirmier", sont joués par des utilisateurs alors que les rôles " service des urgences" ou " service de pédiatrie" sont joués par des organisations [2].

La figure 2.8 présente la relation *Habilite* qui est introduite afin de structurer le lien entre les trois entités : *Organisation*, *Rôle* et *Sujet*. Si *org* est une organisation, *s* est un sujet et *r* est un rôle, alors la relation *Habilite(org, s, r)* signifie que *org* habilite le sujet *s* à jouer le rôle *r*. Les exemples suivants illustrent le fait que les sujets sont soit des utilisateurs, soit des organisations :

– *Habilite(CHU Tlemcen, Mohamed, médecin)* : signifie que l'organisation *CHU Tlemcen* habilite le sujet *Mohamed* dans le rôle *médecin*.
– *Habilite(CHU Tlemcen, CH01, unité_des_urgences)* : signifie que l'organisation *CHU Tlemcen* habilite le sujet *CH01* dans le rôle *unité_des_urgences*.

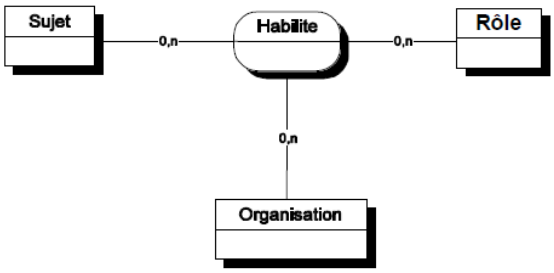


FIGURE 2.8 – La relation *Habilite* [2]

3. **Objets et Vues**

Dans le modèle de CA à base d'organisation, l'entité *Objet* représente principalement les entités non-actives comme les dossiers administratifs, les dossiers médicaux ou chirurgicaux des patients, etc. [35]. Pour structurer les objets et faciliter l'ajout de nouveaux objets au système, une entité comparable au rôle pour les sujets est nécessaire pour les objets, c'est l'entité *Vue* qui correspond, à un ensemble d'objets qui satisfait une propriété commune, c'est comme dans les bases de données relationnelles. Par exemple, la vue "dossier administratif" correspond à l'ensemble des informations administratives des patients, alors que la vue "dossier médical" correspond aux dossiers médicaux des patients [2].

La figure 2.9 présente la relation *Utilise* qui est introduite afin de structurer le lien entre les trois entités : *Organisation*, *Objet* et *Vue*. Si *org* est une organisation, *o* est un objet et *v* est une vue, alors La relation *Utilise(org, o, v)* signifie que *org* utilise l'objet *o* dans la vue *v*.

L'exemple suivant illustre la relation *Utilise* :

– *Utilise(CHU Tlemcen, F1.doc, dossier_administratif)* : signifie que l'organisation *CHU Tlemcen* utilise l'objet *F1.doc* comme un *dossier_administratif*.

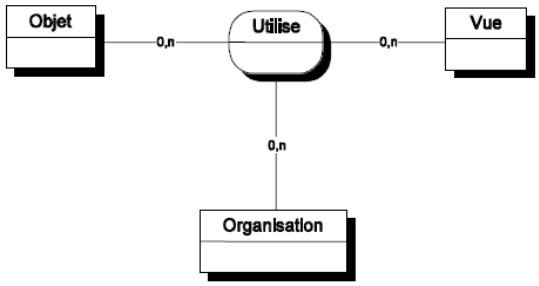


FIGURE 2.9 – La relation *Utilise* [2]

4. **Actions et Activités**

   Dans la politique de sécurité Or-BAC, l'entité *Action* englobe principalement les actions informatiques comme " lire", " écrire", " envoyer", etc. [35]. Tandis que l'entité *Activité* est une abstraction de l'entité *Action* et qui correspond à des actions qui ont un objectif commun, par exemple, " consulter", "modifier" , " transmettre", etc. [2].

   La figure 2.10 présente la relation *Considère* qui est introduite afin d'associer les trois entités : *Organisation*, *Action* et *Activité*. Si *org* est une organisation, α est une action et *a* est une activité, alors la relation *Considère(org, α, a)* signifie que *org* considère l'action α comme faisant partie de l'activité *a*.

   L'exemple suivant illustre la relation *Considère* :

   – *Considère(CHU Tlemcen, lire, consultation)* : signifie que l'organisation *CHU Tlemcen* considère l'action *lire* comme une *consultation*.

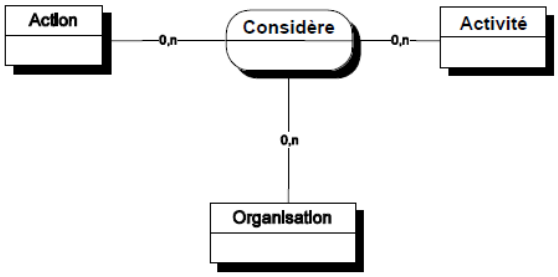


FIGURE 2.10 – La relation *Considère* [2]

5. **Contextes**

   Dans le modèle de CA Or-BAC l'entité *Contexte* est utilisée pour exprimer les circonstances réelles dans lesquelles les organisations accordent des permissions aux sujets afin de réaliser des activités sur des vues. Par exemple dans le domaine médical, l'entité *Contexte* permet d'exprimer des circonstances telles que " urgence" , "temps" , etc. Les contextes peuvent être vus comme des relations ternaires entre les sujets, les objets et les actions définis dans une certaine organisation [35] [2].

   La figure 2.11 présente la relation *Définit* qui est introduite afin de lier les cinq entités : *Organisation*, *Sujet*, *Action* , *Objet* et *Contexte* . Si *org* est une organisation, *s* est un sujet,α est une action, *o* est un objet et *c* est un contexte,

alors *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.

L'exemple suivant illustre la relation *Définit* :

– *Définit(CHU Tlemcen, Mohamed, lire, F1.doc, urgence)* : signifie que dans le contexte *urgence*, le sujet *Mohamed* est autorisé de *lire* le dossier *F1.doc* dans l'organisation *CHU Tlemcen*.

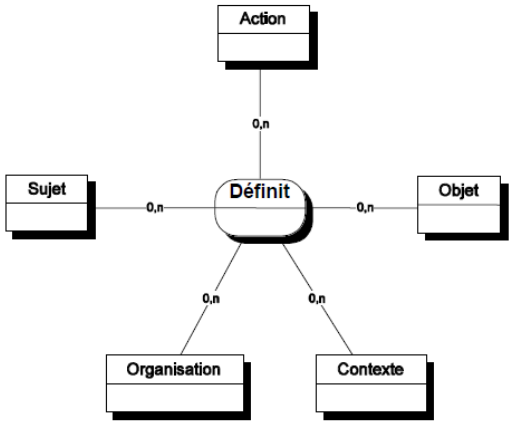


FIGURE 2.11 – La relation *Définit* [2]

6. **Spécification de la politique de sécurité Or-BAC**

La politique de sécurité basée sur le modèle Or-BAC réglemente les accès au système à travers des relations de *Permission*, *Interdiction*, *Obligation* et *Recommandation*. Par exemple la relation *Permission* 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 (voir figure 2.12) [2].

Si *org* est une organisation, *r* est un rôle, *a* est une activité, *v* est une vue et *c* est un contexte, alors *Permission(org, r, a, v, c)* signifie que l'organisation *org* accorde au rôle *r* la permission de réaliser l'activité *a* sur la vue *v* dans le contexte *c* [35].

L'exemple suivant illustre la relation *Permission* :

– *Permission(CHU Tlemcen, médecin, consulter, dossier_médical, urgence)* : signifie que *CHU Tlemcen* accorde aux *médecins* la permission de *consulter* n'importe quel *dossier_médical* dans le contexte de *l'urgence*.

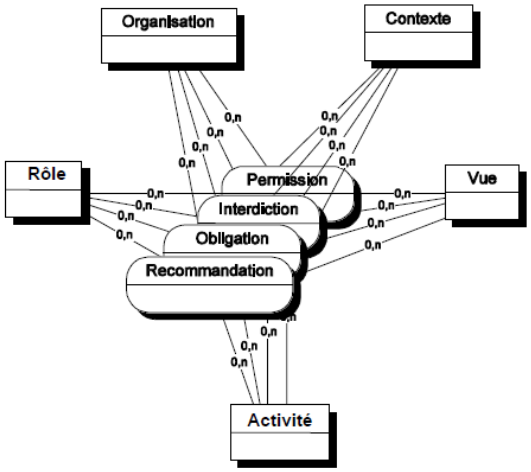


FIGURE 2.12 – Les relations *Permission, Interdiction, Obligation et Recommandation* [2]

Gestion et l'administration du modèle Or-BAC

En 2003, F. Cuppens and A.Miège proposent un modèle d'administration AdOr-BAC (Administration model for Or-BAC) efficace utilisant une structure organisationnelle pour un environnement de CA décentralisé basé sur des rôles [80]. Ce modèle permet de gérer toutes les relations qui existent entre les entités du modèle Or-BAC, il comporte les trois sous-modèles suivants [81] :

1. PRA (Permission-Role Assignment) : ce modèle permet la création et la suppression des permissions.
2. URA (User-Role Assignment) : ce modèle permet l'habilitation des sujets dans des rôles.
3. UPA (User-Permission Assignment) : ce modèle permet l'affectation de permissions à des utilisateurs.

3.1.7.1 Avantages et inconvénients du modèle Or-BAC Le modèle de CA Or-BAC présente les avantages suivants [34] [35] [2] :

- Simple à mettre en exécution.
- La notion de rôle permet de simplifier la mise à jour de la politique de sécurité.
- Facilite l'intégration des utilisateurs et la gestion des autorisations.
- Spécification de ce qui est permis, interdit, obligé et recommandé.
- Prend en compte la notion de contexte dans l'expression des règles.

La politique de sécurité à base d'organisation souffre de l'inconvénient suivant [2] [6] :

- Des conflits peuvent apparaître dans la politique de sécurité.

Il existe des travaux qui ont utilisé le modèle de CA Or-BAC dont nous citons :

- C.Coma, N.Boulahia, F.Cuppens ont traité le problème de CA dans le milieu médical et le respect de la vie privée des patients [46], ils ont pu constater les

limites du modèle RBAC pour définir les problèmes contextuels. Pour pallier ce problème, les auteurs ont étudié un exemple de modélisation grâce au modèle Or-BAC dont les avantages de ce modèle sont l'abstraction des différents entités : des sujets, des actions, des objets, la prise en compte des contextes et la simplification de la gestion de la politique. Finalement, les auteurs ont utilisé le langage XACML pour exprimer la politique de CA aux documents patient partagés.

– En 2016, A.HASSANI a proposé deux extensions du modèle Or-BAC [6] :
  1. I-OrBAC (Integrity-OrBAC) : c'est un modèle qui prend en compte des contraintes liées à l'intégrité dans la prise de décision de CA localement au sein d'une organisation.
  2. DI-OrBAC (Distributed Integrity-OrBAC) : c'est une extension du modèle IOrBAC ayant pour objectif la satisfaction des exigences en matière d'intégrité dans un contexte distribué et collaboratif.
– En 2016, W. UTTHA a proposé un nouveau modèle de CA D-OrBAC (Distributed-Organisation Based Access Control) [82], qui est une extension du modèle Or-BAC et qui permet de protéger des ressources partagées. Dans ce modèle, l'auteur a associé des sujets avec des catégories (qui peuvent être déléguées aux autres sujets de différentes organisations) afin de résoudre le problème d'autorisation d'accès aux ressources partagées dans un environnement distribué avec plusieurs organisations partenaires, chacune de ces organisations possédant sa propre politique de sécurité. Il a utilisé un langage formel basé sur la logique du premier ordre pour représenter les différentes relations de son modèle.

3.2 Modèles de CA collaboratifs

Les modèles de CA pour la collaboration permettent le partage, l'échange et le transfert des données, des services et des ressources entre différents organisations inter-connectées et interdépendantes, ces modèles de CA peuvent être basés sur un mode de gestion de politique de sécurité centralisée ou décentralisée.

1. **Gestion centralisée de la sécurité :** cette première approche définie un système de gestion de politique de sécurité globale et centralisée [83] dont les décisions de CA sont mises en œuvre dans un point central appelé *super organisation* qui impose sa politique de sécurité à toutes les autres organisations [79]. Cette technique consiste à intégrer des composantes de la politique de sécurité globale dans chacune des politiques de sécurité des organisations. La politique de CA est gérée par la *super organisation*, autorité reconnue par l'ensemble des organisations, et elle est applicable sur tout l'environnement collaboratif. Cette méthode présente l'avantage de la mise en place d'une plate-forme unifiée pour appliquer différentes politiques de sécurité au sein d'un seul système central [74]. Néanmoins, cette plateforme n'apporte aucune structuration dans les interactions entre organisations, ce qui conduit à de grands risques d'incohérence entre les politiques de sécurité lorsque le système est de taille réaliste [79].
2. **Gestion décentralisée de la sécurité :** cette deuxième approche définie la sécurité d'organisations qui collaborent et qui consiste à regrouper ou même à

fusionner les politiques de sécurité des différentes organisations en une politique globale unique [79]. Cette approche a l'avantage de laisser à chaque organisation le contrôle de ses propres décisions de sécurité et de leurs mises en œuvre [74].

Il existe dans la littérature différents modèles de CA collaboratifs, dans ce qui suit nous allons analyser ces différents modèles de politiques de sécurité.

3.2.1 Modèle de CA Multi-OrBAC

Le modèle de CA Multi-OrBAC (MultiOrganization-Based Access Control) a été proposé en 2006 par A.Abou El Kalam et Y.Deswarte pour les applications complexes, hétérogènes, interopérables et distribuées [84]. Ce modèle permet de spécifier, dans un cadre homogène, plusieurs politiques de sécurité pour des organisations hétérogènes devant coopérer. L'objectif de ce modèle de CA est d'offrir à chacune de ces organisations une certaine souplesse (par exemple, sur le choix d'une plate-forme, de services, etc.) tout en respectant les contraintes imposées par une politique globale de sécurité.

Le modèle de CA Multi-OrBAC offre deux présentations complémentaires [84] :

- Une présentation de type génie logiciel utilisant le langage UML pour la mise en œuvre.
- Une présentation formelle avec la programmation logique par contraintes pour la validation.

La politique de CA basée sur le modèle Multi-OrBAC est une extension du modèle Or-BAC pour les systèmes multi-organisationnels, elle offre un formalisme qui permet de décrire les politiques de sécurité d'organisations coopérant dans un même système en éliminant l'ambiguïté dans la spécification et la vérification de sa cohérence, elle permet également la détection et la résolution de conflits entre les règles de la politique, entre les objectifs de la sécurité, ou entre les règles et les objectifs, comme elle permet la gestion de problèmes d'incohérence entre les politiques de sécurité hétérogènes de chaque organisation. L'inconvénient du modèle Multi-OrBAC réside dans le fait que la définition de la politique de sécurité de chaque organisation doit connaître, des entités appartenant à d'autres organisations, et suppose donc une confiance entre les organisations pour ce qui concerne la gestion de ces entités. Ceci pose le problème de confidentialité [79].

3.2.2 Modèle de CA d'organisation virtuelle

En 2006, B.Nasser a proposé le modèle de CA d'organisation virtuelle [85] qui permet de regrouper et collaborer un ensemble d'organisations qui unissent leurs compétences et ressources pour répondre à une opportunité qu'elles n'auraient pu prendre en charge seule. Une fois le service accompli, le regroupement est démantelé [74].

3.2.3 Modèle de CA O2O

Le modèle de CA O2O (Organization to Organization) a été proposé en 2006 par Coma, Cuppens et al. [86] dont le but été de gérer l'interopérabilité et la colla-

boration entre des entités ayant leurs propres politiques de sécurité définies dans différentes organisations. Ce modèle est une extension du modèle Or-BAC basée sur deux concepts clés [79] :

- VPO (Virtual Private Organization) : c'est une sous-organisation créée lorsqu'une organisation gère les accès venant des organisations externes à ses propres ressources.
- RSSO (Role Single-Sign-On) : c'est un concept qui permet à un sujet donné de garder le même rôle quelle que soit l'organisation à laquelle il accède, mais avec des privilèges définis par la VPO de l'organisation à laquelle il accède. Les privilèges diffèrent d'une VPO à une autre, chaque organisation appliquant sa propre politique de sécurité pour gérer l'interopérabilité.

3.2.4 Modèle de CA Poly-OrBAC

En 2009, A.Baina a proposé le modèle de CA Poly-OrBAC [79] qui se base sur le modèle de sécurité Or-BAC, utilisé pour spécifier la politique de sécurité locale à chaque organisation, et sur la technologie des services Web qui permet de fournir une plateforme de collaboration et d'interopérabilité entre les organisations, avec des extensions pour permettre de spécifier et de mettre en œuvre la sécurité sur les interactions. Cette plateforme est applicable dans le contexte d'une infrastructure critique en générale et plus particulièrement dans le cadre d'un réseau électrique [74].

3.3 Modèles de CA basés sur la confiance

En 2009, I.Ray el al. ont proposé un modèle qui permet de formaliser les relations de confiance [87]. La relation de confiance entre un « truster » (l'entité qui fait confiance à l'entité cible) et un « trustee » (l'entité cible qui est digne de confiance) est associée à un contexte et dépend de l'expérience, des connaissances, et de la recommandation que le « truster » à l'égard de « trustee » dans un contexte donné [88]. Dans cette politique, l'affectation des rôles aux utilisateurs se fait en fonction de la valeur du niveau de confiance, et se varie avec le changement de ce niveau [54].

3.3.1 Modèle de CA Trust-RBAC

En 2009, M.Toahchoodee et al. ont proposé le modèle Trust-RBAC qui est un modèle RBAC basé sur la confiance pour les systèmes d'informatique ubiquitaire [89]. Son principe repose sur ces trois points [54] [88] :

1. Les utilisateurs (humains ou périphériques) : sont évalués pour leur fiabilité avant qu'ils ne soient affectés à des différents rôles.
2. Les rôles : sont associés à une gamme de confiance indiquant le niveau de confiance minimal qu'un utilisateur a besoin d'atteindre avant qu'il puisse être affecté à ce rôle.
3. Les autorisations : sont associées avec le niveau de confiance nécessaire pour activer la permission à un utilisateur.

3.3.2 Modèle de CA basé sur trust et risque

En 2003, N. Dimmock a proposé un modèle qui utilise les notions humaines de confiance et de communauté comme base pour l'attribution de privilèges, et utilise également l'analyse de risque pour déterminer le degré de confiance requis pour attribuer un privilège particulier dans le CA basé sur la confiance [90]. Cette politique de sécurité prend des décisions sur la base de la confiance et de l'analyse des risques plutôt que sur la base d'informations d'identification seul [54].

3.4 Modèles de CA basés sur la vie privée

En 2005, Dafa-Alla et al. ont proposé le modèle de CA basé sur les rôles P-RBAC (Privacy Role Based Access Control), afin de protéger la confidentialité lors de l'exploration de données [91]. Les utilisateurs sont autorisés à accéder et donc à extraire différents ensembles de données en fonction de leurs rôles, ce modèle peut être utilisé par rapport aux technologies existantes et permet de préserver la vie privée des individus.

3.5 Modèles de CA sémantique

Dans le domaine de CA, les applications de la technologie du web sémantique envahissent aujourd'hui notre quotidien, pour cela de nouveaux modèles ont été proposé pour exploiter cette technologie. Dans ce qui suit nous allons présenter ces modèles de sécurité et leurs spécifications en utilisant les ontologies.

3.5.1 Modèle de CA SBAC

En 2006, A.Toninelli et al. ont proposé le modèle de CA SBAC (Semantic-Based Access Control Model) qui prend en compte le contexte sémantique, et qui considère ce contexte comme toute information caractérisant les ressources contrôlées et le monde qui les entoure [92]. Ce modèle est formé de trois entités : les sujets qui sont des entités actives exerçant une demande d'accès, les objets qui sont des entités passives accessibles et/ou modifiés par le sujet et les actions qui sont les opérations effectuées sur l'objet. La spécification de politique de sécurité est basée sur le langage OWL(Web Ontology Language) pour spécifier les ontologies (chaque entité est modélisée par une ontologie.) et sur le langage SWRL (Semantic Web Rule Language) pour coder les règles d'autorisations [54].

3.5.2 Modèle de CA ROWLBAC

En 2008, T.Finin et al ont proposé le modèle de CA ROWLBAC (Representing Role Based Access Control in OWL) qui étudie la relation entre le langage OWL et le modèle de CA RBAC [93]. Bien que OWL soit un langage d'ontologie Web et ne soit pas spécialement conçu pour exprimer des règles d'autorisation, il a été utilisé avec succès dans cette proposition. ROWLBAC propose deux approches possibles de RBAC avec OWL [94] :

– La première approche ontologique de ROWLBAC représente les rôles comme des classes et la structuration de ces classes repose sur la hiérarchie des rôles.
– La deuxième approche représente les rôles comme des instances de la classe *Role* et leurs relations à partir des attributs de ces instances.

3.5.3 Modèle de CA TSBAC

En 2008, AN. Ravari et al. ont proposé le modèle de CA TSBAC (Temporal Semantic-Based Access Control) qui est une extension du modèle SBAC avec intégration de l'aspect temporel [95]. Ce modèle améliore la spécification des règles d'autorisation définies par l'utilisateur en limitant l'intervalle de temps et l'expression temporelle sur l'historique des accès des utilisateurs. Dans cette politique de sécurité, un aspect dynamique est également associé aux permissions en fixant un intervalle de temps qui limite la durée de validité pour chacune des autorisations [54].

3.6 Modèles de CA basés sur l'intelligence artificielle

Dans nos jours, la technologie de l'intelligence artificielle est devenue un axe de recherche très important, pour cela, il existe dans la littérature des modèles de CA qui ont intégré cette technologie, dans ce qui suit nous allons présenter quelques modèles qui se basent sur les approches de l'intelligence artificielle.

3.6.1 Modèle de CA basé sur les systèmes multi-agents

En 2005, A.Omicini et al. ont proposé un modèle de CA intelligent en utilisant l'approche des systèmes multi-agents [96]. Les auteurs ont ajouté au modèle RBAC un nouveau concept celui de l'agent coordinateur de contexte ayant pour objectif d'interagir avec l'environnement et de coordonner les informations contextuelles [54].

3.6.2 Modèle de CA basé sur les réseaux de neurones

En 2007, TH.LIM et al. ont proposé un système intelligent qui utilise un algorithme de réseaux neurones et qui étend le modèle RBAC avec des contraintes de contexte [97] [98]. Les auteurs ont appliqué cette approche pour rendre le modèle intelligent lors de prise de décision [54].

4 Conclusion

Dans ce chapitre, nous avons présenté d'abord les concepts de la politique de sécurité ensuite, nous avons dressé un état de l'art complet sur les différents modèles de CA qui existent dans la littérature. Nous avons classé ces modèles en six classes :

– Les modèles de CA classiques traditionnels, conçus pour gérer la sécurité et le CA d'une organisation.

- Les modèles de CA collaboratifs, conçus pour gérer la sécurité d'un ensemble d'organisations qui doivent coopérer et collaborer.
- Les modèles de CA basés sur la confiance, conçus pour gérer les droits d'accès selon un niveau de confiance calculé.
- Les modèles de CA basés sur la préservation de la vie privée, conçus pour protéger la confidentialité et la vie privée des utilisateurs.
- Les modèles de CA basés sur l'aspect sémantique, conçus pour ajouter l'aspect sémantique lors de la fusion des données contextuelles.
- Les modèles de CA basés sur les technologies d'intelligence artificielle, conçus pour intégrer la technologie de l'intelligence artificielle.

Dans le chapitre suivant, nous allons présenter notre proposition du modèle de CA pour le DM dans le cas d'une organisation de santé algérienne.

Chapitre 3

Modélisation du CA pour le DM

1 Introduction

L'accessibilité aux ressources d'information dans les systèmes de santé est un aspect très important. Le travail de cette thèse porte sur la protection des données médicales et s'est centré principalement sur le CA dans les systèmes d'information en santé. Il s'agit donc de proposer une modélisation rigoureuse permettant de prendre en charge tous les aspects liés à la gestion sécurisée du DM informatisé.

L'objectif de ce chapitre est de proposer un modèle pour le CA au DM, le cas d'une organisation de santé algérienne. Pour se faire nous allons se baser sur une modélisation XML de ce DM que nous avons préalablement établi (voir le modèle XLM du DM en annexe A). Avant de présenter le modèle proposé, nous allons d'abord, dans ce qui suit, effectuer une comparaison entre les différents modèles de CA. Cette dernière va nous permettre de choisir le modèle le plus approprié pour notre cas d'étude.

2 Comparaison des modèles de CA

Dans le domaine de CA, nous pouvons constater que les politiques de sécurité de base sont : DAC, MAC, RBAC, TBAC, TMAC et Or-BAC (voir le chapitre précédent) ; les autres modèles sont des extensions proposées pour répondre à des différentes exigences et aussi pour améliorer les modèles traditionnels.

Le tableau 3.1 présente les propriétés caractérisant un modèle de CA.

Propriétés	Définitions
Rôle	C'est un ensemble de sujets à qui la même règle de sécurité est appliquée (par exemple : médecin, infirmier, etc.)
Équipe	C'est un ensemble d'utilisateurs, ayant des rôles différents et qui coopèrent afin de réaliser une tâche ou un objectif commun.
Contexte	Spécifie des règles de CA spécifiques à certaines circonstances concrètes qui entourent un fait .
Permission	Autoriser un utilisateur a effectué une action. Par exemple : les médecins ont le droit de modifier des informations dans le dossier médical de patient.
Interdiction	Interdire un utilisateur a effectué une action. Par exemple : les médecins n'ont pas le droit de supprimer les identifications des patients.
Obligation	Ce sont des actions automatiques obligatoires dans un système, par exemple : chaque fois qu'un médecin accède à un dossier d'un patient qui ne le traite pas, un message est automatiquement envoyé à son chef de rayon.
Recommandation	Action permet de définir des règles de sécurité utilisant une modalité de recommandation.
Confidentialité	Concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées.
Intégrité	Ensemble de moyens et techniques permettant de restreindre la modification des données aux personnes autorisées.
Modèle dynamique	La modification des droits d'accès est facile.
Mise à jour	L'action qui permet à mettre *à niveau*, un outil informatique.

TABLE 3.1 – Propriétés des modèles de CA

Dans cette section, nous allons faire la synthèse des modèles de CA de base, sans prendre en considération les extensions. Selon cette étude comparative, nous allons choisir le modèle de CA le plus approprié pour notre cas d'étude.

Sur la base des propriétés déduites dans le tableau 3.1, nous avons construit le tableau 3.2 qui représente un comparatif des modèles d'accès étudiés. Le signe plus « + » dans le tableau indique la présence de la propriété de la ligne dans le modèle de la colonne.

Propriétés/Modèles	DAC	MAC	RBAC	TBAC	TMAC	Or-BAC
Rôle			+		+	+
Équipe					+	
Contexte						+
Permission	+	+	+	+	+	+
Interdiction						+
Obligation						+
Recommandation						+
Confidentialité		+			+	+
Intégrité	+	+	+	+	+	+
Modèle dynamique			+		+	+
Mise à jour			+		+	+

TABLE 3.2 – Comparaison des modèles de CA

Le tableau 3.2 montre clairement que le modèle Or-BAC est le plus complet par rapport aux autres.

Nos travaux [99], [100], [18], ainsi d'autres travaux comme [46] [35] [2] ont montré que le modèle de CA à base d'organisation Or-BAC est le plus approprié dans le domaine médical, il représente sans doute le meilleur choix à implémenter dans le cadre des systèmes d'information en santé.

3 Proposition du modèle de CA

Sur la base de la politique de sécurité à base d'organisation Or-BAC, nous avons proposé un modèle de CA pour le DM pour une organisation de santé algérienne [101] [102]. Nous allons décrire dans ce qui suit les différentes entités et relation de notre modèle proposé et qui sont modélisés graphiquement en utilisant les diagrammes de classes UML.

3.1 Organisations

Une organisation peut être vue comme un groupe organisé d'entités actives, c'est-à-dire de sujets jouant certains rôles [35] [2]. Dans notre cas, nous avons plusieurs organisations :

1. EPSP Établissement Public de Santé de Proximité
2. EPH Établissement Publique Hospitalier
3. EHS Établissement Hospitalier Spécialisé
4. Hôpital
   - □ Direction
     - Sous-direction des ressources humaines
       - Bureau de la gestion des ressources humaines
       - Bureau de la formation
     - Sous-direction des finances et des moyens
       - Bureau de budget et de la comptabilité

    - Bureau des moyens généraux et des infrastructures
    - Bureau des marchés publics
  - Sous-direction des services de santé
    - Bureau d'organisation
    - Bureau de contractualisation et calcul de coûts
    - Bureau des entrées
  - Sous-direction de la maintenance
    - Bureau de la maintenance des équipements médicaux
    - Bureau de la maintenance des équipements connexes
- Les services hospitaliers
  - Services de pédiatrie
    - Pédiatrie
    - Néonatalogie
  - Service de réanimation
    - Observation
    - Réanimation
  - Service de gynécologie
    - Maternité
    - Gynécologie
  - Service de médecine interne
    - Médecine homme
    - Médecine femme
    - Hémodialyse
  - Service de chirurgie générale
    - Chirurgie homme
    - Chirurgie femme
  - Service de psychiatrie
- Plateau technique
  - Service de laboratoire
    - Microbiologie
    - Biochimie
  - Service de radiologie
    - Radiologie
    - Ecographie
  - Service de pharmacie
    - Gestion des produits pharmaceutiques
    - Distribution des produits pharmaceutiques
  - Urgences
    - Unité médicale
    - Unité chirurgicale
- Les services préventifs
  - Service d'épidémiologie
    - Information sanitaire
    - Hygiène hospitalier
  - Service de médecine de travail

Dans notre proposition, nous avons regroupé toutes ces organisations dans une seule entité appelée « organisations de santé ». La figure 3.1 présente la mo-

délisation de cette entité en utilisant le diagramme de classe UML.

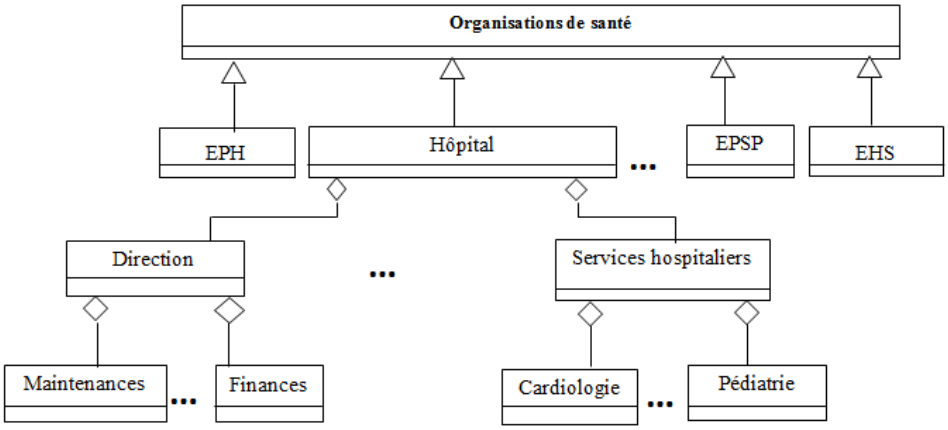


FIGURE 3.1 – Modélisation UML de l'entité *organisations de santé*

3.2 Sujets et rôles

3.2.1 *Sujets*

Dans le modèle de CA Or-BAC, l'entité *Sujet* peut être soit une entité active, c'est-à-dire un utilisateur, par exemple, 'Asma', 'Mohamed', etc. soit une organisation, par exemple, 'hôpital', 'le service des urgences de l'hôpital', etc. [2]. Dans notre proposition, nous avons considéré l'entité *Sujet* comme entité active et qui peut-être :

- Une personne (”Asma”, ”Mohamed”, etc.)
- Un objet connecté (”Bee [1] : c'est un objet connecté pour le contrôle des injections et de taux de glycémies pour les personnes diabétiques”, ”Blink [2] : c'est un objet connecté pour faire un examen oculaire chez soi", etc.).

3.2.1.1 Les objets connectés Un objet connecté est un objet physique équipé de capteurs ou d'une puce qui lui permettent de transcender son usage initial pour proposer de nouveaux services. Il s'agit d'un matériel électronique capable de communiquer avec un ordinateur, un smartphone ou une tablette via un réseau sans fil (Wi-Fi, Bluetooth, réseaux de téléphonie mobile, etc.), qui le relie à Internet ou à un réseau local. Cet objet connecté peut être contrôlé à distance et remplit généralement deux rôles :

- Objet connecté classique : il joue le rôle de capteur pour surveiller l'apparition d'un événement ou d'une mesure spécifique (mesure de poids, surveiller le sommeil, etc.).

1. http ://www.medecingeek.com/bee-objet-connecte-pour-le-suivi-des-injections-et-glycemies-pour-les-diabetiques/
2. https ://www.eyes-road.com/objets-connectes-optique-5317/

– Objet connecté intelligent : il joue le rôle d'actionneur pour réaliser une action suite à un événement spécifique mesuré ou détecté (par exemple déclenchement d'une alarme en cas d'un taux élevé de l'insuline).

Les objectés connectés envahissent aujourd'hui notre quotidien, voici quelques exemples :

– Suivre le jogging.
– Mesurer le poids.
– Surveiller le sommeil.
– Contrôler le taux d'insuline (Bee).
– Faire un examen oculaire chez soi (Blink)
– Un pansement connecté (SensiumVitals) qui est capable de mesurer l'activité cardiaque, la respiration, et la température. Ce pansement est connecté au smartphone de l'infirmière en charge du patient, ce qui lui permet de garder un œil à distance sur ses constantes.
– Des tensiomètres connectés.
– En endoscopie, il existe même une caméra sans fil de la taille d'une gélule que l'on peut ingérer afin de contrôler à distance le bon fonctionnement du système digestif.

Les objets connectés offrent les avantages suivants [103] :

– Permettent de récolter et de restituer des données de manière plus efficace,
– Permettent de faciliter le travail des professionnels de santé, tout en améliorant la prise en charge des patients, particulièrement lorsqu'ils ont à faire à de multiples interlocuteurs.
– Très efficaces dans le domaine de la prévention.
– Aident et accélèrent le diagnostic, ou juste confirment qu'une personne est en bonne santé.
– Permettent de maintenir une surveillance médicale continue.
– La mise en place de surveillances à domicile permettrait de mieux gérer les coûts d'hospitalisation qui sont aujourd'hui très élevés.

Par ailleurs, les limites des objets connectés sont [103] :

– La fiabilité des données.
– La sécurité des données.
– Le développement des technologies sans fil implique une exposition au piratage de ces données.
– Il n'y a de régulation éthique ni sur la collecte, ni sur l'utilisation de ces données personnelles.

La figure 3.2 présente la modélisation de l'entité *Sujet* en utilisant le diagramme de classe UML.

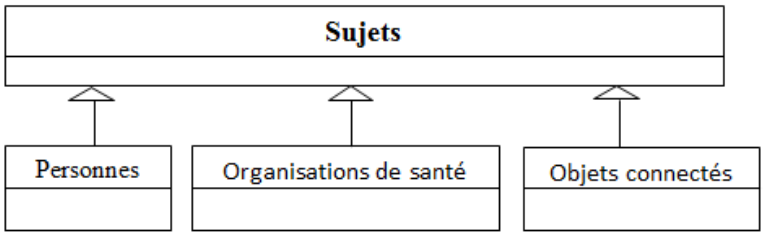


FIGURE 3.2 – Modélisation UML de l'entité *Sujet*

3.2.2 *Rôles*

L'entité *Rôle* est utilisée afin de relier les sujets et les organisations et pour faciliter la mise à jour de la politique de CA lorsqu'un nouvel utilisateur est ajouté [2]. Dans le domaine médical par exemple, les rôles "médecin" ," infirmier", sont joués par des utilisateurs alors que les rôles " service des urgences" ou " service de pédiatrie" sont joués par des organisations. Dans notre proposition, nous avons identifié les rôles suivants (voir figure 3.3) :

1. Acteurs : (voir figure 3.4)
   - Patients.
   - Pharmaciens.
2. Personnels médicaux : (voir figure 3.5)
   - Professeur.
   - Maitre de conférences A (MCA).
   - Maitre de conférences B (MCB).
   - Médecin assistant.
   - Médecin spécialiste.
   - Médecin résident.
   - Médecin généraliste.
   - L'interne.
   - L'externe.
3. Personnels paramédicaux : (voir figure 3.6)
   - Aide-soignant.
   - Infirmier.
   - Cadre de santé.
   - Coordinateur.
   - Laborantin.
   - Manipulateur RX.
   - Anesthésiste.
   - Kinésithérapie.
   - Sage-femme.
   - Psychologue.
   - Secrétaire médicale.
4. Objets connectés : (voir figure 3.7)
   - Objets connectés classiques.
   - Objets connectés intelligents.

Les figures suivantes présentent la modélisation des différents rôles proposés en UML.

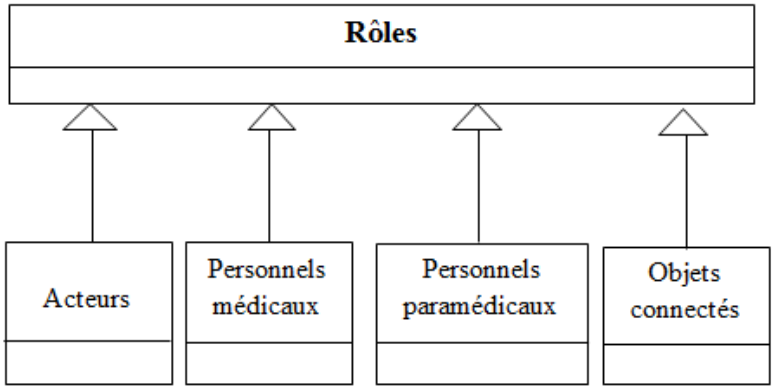


FIGURE 3.3 – Modélisation UML de l'entité *Rôle*

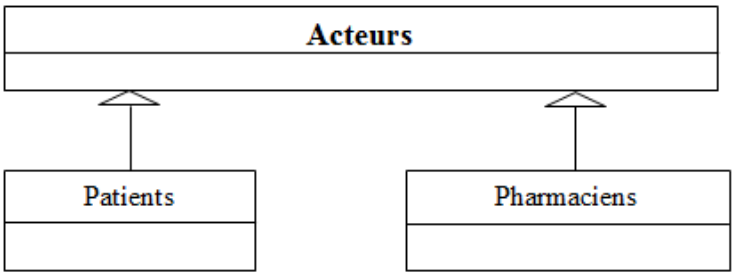


FIGURE 3.4 – Modélisation UML du rôle *Acteurs*

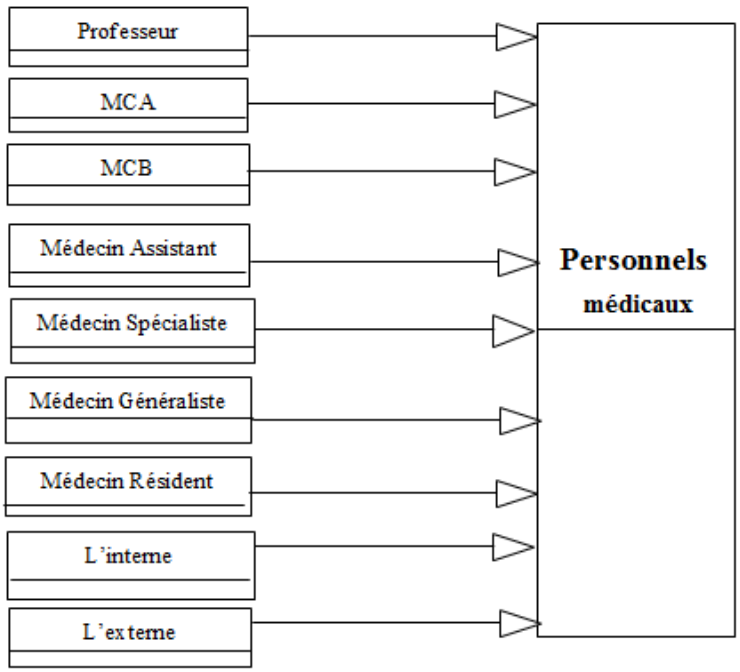


FIGURE 3.5 – Modélisation UML du rôle *Personnels médicaux*

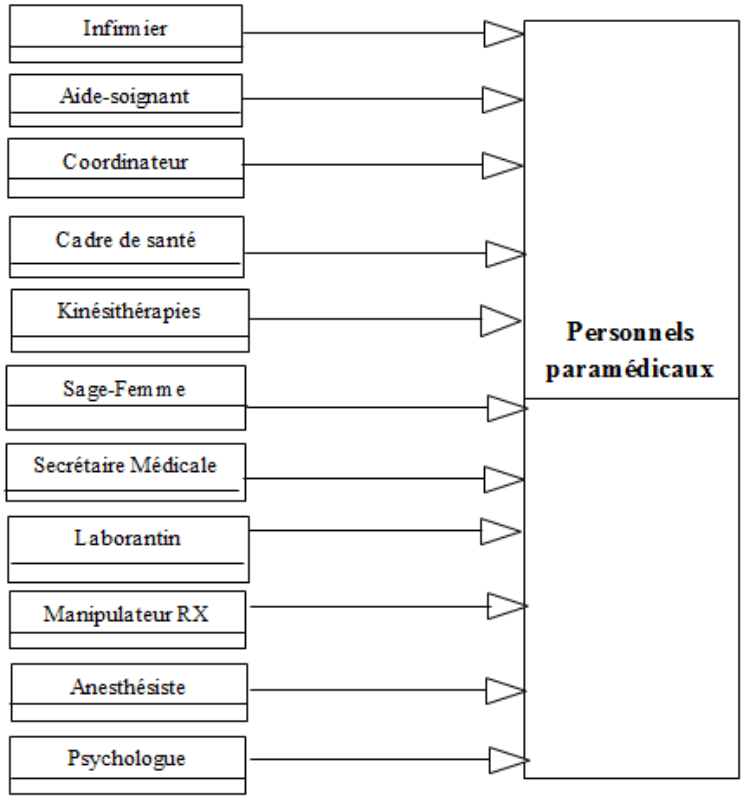


FIGURE 3.6 – Modélisation UML du rôle *Personnels paramédicaux*

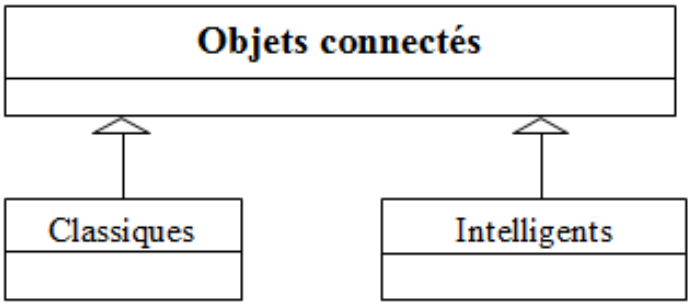


FIGURE 3.7 – Modélisation UML du rôle *Objets connectés*

3.2.3 *Relation Habilite*

Dans notre proposition, nous avons utilisé la relation *Habilite* pour structurer le lien entre les trois entités :

- *Organisation* : dans notre modèle, c'est l'organisation de santé.
- *Sujet* : dans notre modèle, ce sont les entités actives, c'est-à-dire les utilisateurs (personnes ou des objets connectés),
- *Rôle* : ce sont les différents rôles identifiés dans la section précédente.

Voici un exemple qui illustre cette relation : *Habilite (Organisation de santé, Mohamed, spécialiste)* signifie que "*Organisation de santé* habilite le sujet *Mohamed* dans le rôle *spécialiste*". La figure 3.8 présente la modélisation UML de la relation *Habilite*.

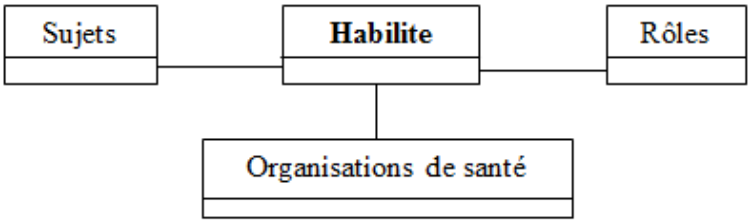


FIGURE 3.8 – Modélisation UML de la relation *Habilite*

3.3 Objets et vues

3.3.1 *Objets*

L'entité *Objet* représente principalement les entités non-actives comme les informations administratives des patients, les rapports chirurgicaux, etc. Dans notre modèle, les objets sont l'ensemble des données du DM (voir section 3.2 Structure du DM dans le chapitre 1).

3.3.2 *Vues*

L'entité *vue* représente un ensemble d'objets qui satisfait une propriété commune, par exemple la vue " dossiers administratifs" correspond à l'ensemble des

informations administratives des patients, alors que la vue " dossiers médicaux" correspond à l'ensemble des données médicales du dossiers médicaux des patients [35]. Dans notre modèle, nous avons dégagé les vues suivantes (Vues (objets de la vue)) :

- Identification (identifiant, nom, prénom, date de naissance, sexe, profession, prénom père, nom mère, prénom mère, nationalité, situation familiale, nom époux, groupage, téléphone, adresse, email, numéro de sécurité sociale).
- Rencontre (nom médecin, prénom médecin, date de rencontre, interrogatoire, lettre d'admission, motifs d'hospitalisation, le type de pris en charge prévue, prescriptions effectuées).
- Personne de confiance (nom, prénom, date de naissance, lien de parenté, téléphone, adresse, email).
- Garde malade (nom, prénom, date de naissance, lien de parenté, téléphone, adresse, email).
- Données pour objets connectés classiques (poids, longueur, sommeil, force musculaire, mouvement, mouvement fœtaux, indice de masse corporelle).
- Données pour objets connectés intelligents (température, fréquence cardiaque, fréquence respiratoire, pression artérielle, taux d'insuline, micro circulation sanguine, détection de chute, EEG, ECG, EMG.)
- Les données médicales générales (antécédents (personnels, familiaux), historiques des consultations, allergies et intolérances reconnues, prothèses et appareillage).
- Les données de soins (pathologies en cours, traitements prescrits et administrés, soins reçus).
- Examens biologiques (catégories, date, résultats, comptes rendus, URL).
- Examens d'imageries (catégories, date, résultats, comptes rendus, URL).
- Les données de prévention (facteurs de risque individuels, traitements préventifs prescrits, calendrier des vaccinations).
- Les données de la chirurgie (design de la chirurgie, heure de la chirurgie, nom chirurgien, prénom chirurgien, nom anesthésiste, prénom anesthésiste, protocole de la chirurgie, compte-rendu).
- Compte-rendu d'accouchement (heure de l'accouchement, nom sage-femme, prénom sage-femme, nom gynécologue, prénom gynécologue, nom anesthésiste, prénom anesthésiste, protocole de la césarienne, compte-rendu).
- Résumé de sortie (mode de sortie, certificat de sortie, ordonnances, rendez-vous).
- Don d'organes (le consentement écrit par le patient).

La figure 3.9 présente la modélisation UML des différentes vues de notre modèle.

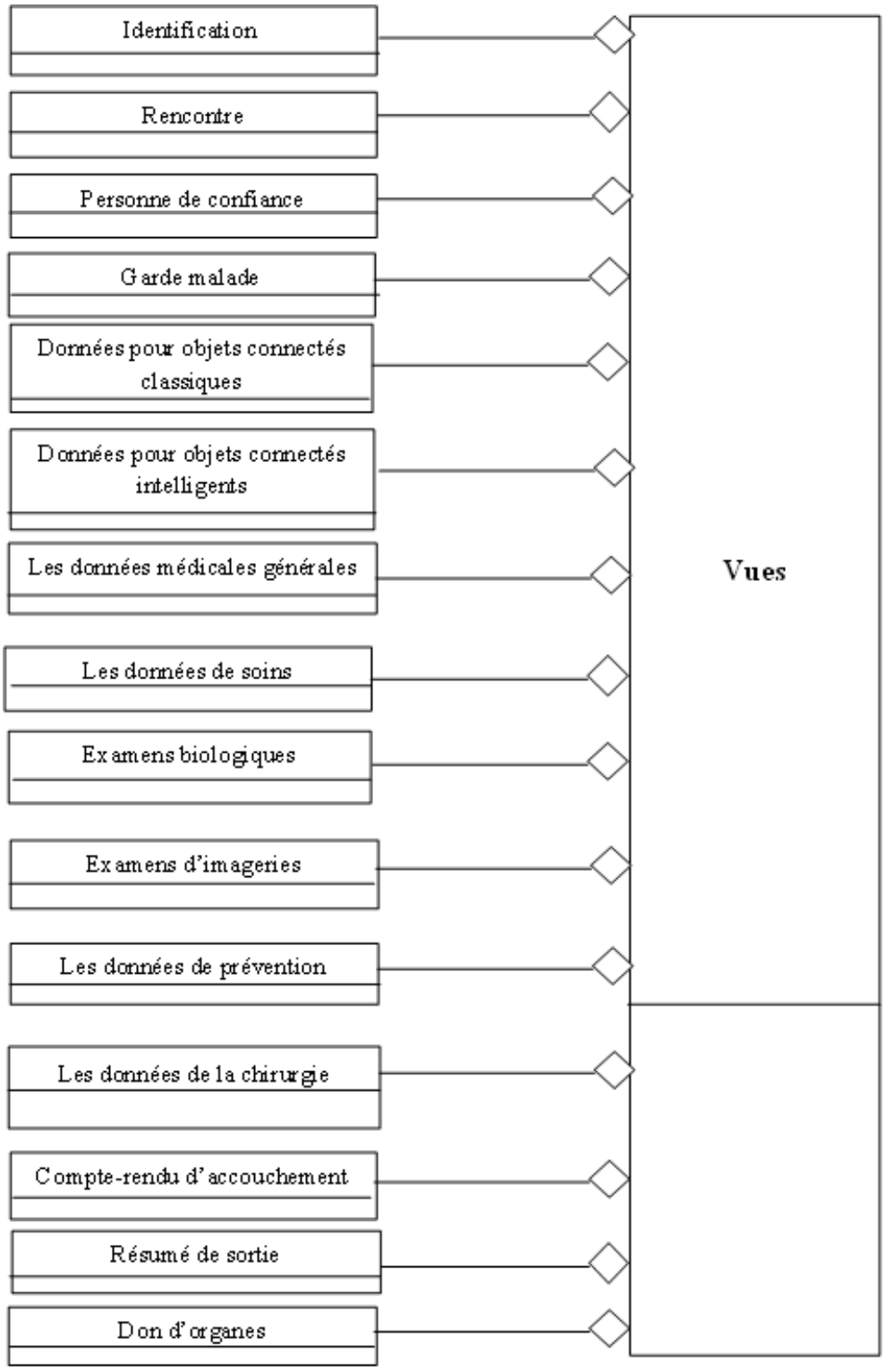


FIGURE 3.9 – Modélisation UML de l'entité *Vue*

3.3.3 *Relation Utilise*

Dans notre proposition, nous avons utilisé la relation *Utilise* pour structurer le lien entre les trois entités :

– *Organisation* : dans notre modèle, c'est l'organisation de santé.
– *Objet* : dans notre modèle, ce sont toutes les informations du DM.
– *Vue* : ce sont les différentes vues identifiées dans la section précédente.

Voici un exemple qui illustre cette relation : *Utilise(Organisation de santé, F1.doc, dossier_administratif)* : signifie que "l'organisation *Organisation de santé* utilise l'objet *F1.doc* comme un *dossier_administratif* ". La figure 3.10 présente la modélisation UML de la relation *Utilise*.

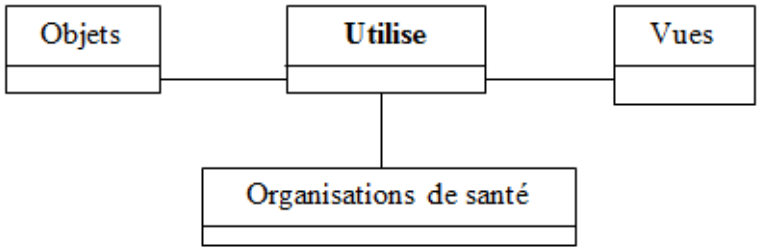


FIGURE 3.10 – Modélisation UML de la relation *Utilise*

3.4 Actions et activités

3.4.1 *Actions*

L'entité *Action* englobe principalement les actions informatiques comme " lire", "écrire", etc [35]. Dans notre modèle, nous avons les deux actions :

– Lire.
– Écrire.

3.4.2 *Activités*

L'entité *Activité* est une abstraction de l'entité *Action* qui correspond à des actions qui ont un objectif commun [2]. Dans notre modèle, nous avons les activités suivantes :

– Consulter.
– Modifier.
– Ajouter.
– Supprimer.
– Transférer.

3.4.3 Relation *Considère*

Dans notre proposition, nous avons utilisé la relation *Considère* pour structurer le lien entre les trois entités :

– *Organisation* : dans notre modèle, c'est l'organisation de santé.
– *Action* : dans notre modèle, ce sont lire et écrire.
– *Activité* : ce sont les différentes activités identifiées dans la section précédente.

Voici un exemple qui illustre cette relation : *Considère (Organisation de santé, lire, consultation)* : signifie que "l'organisation *Organisation de santé* considère l'action *lire* comme une *consultation*". La figure 3.11 présente la modélisation UML de la relation *Considère*.

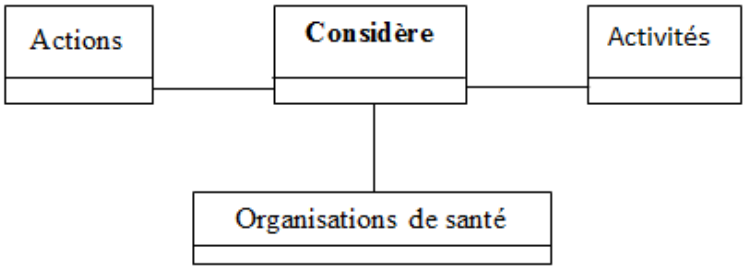


FIGURE 3.11 – Modélisation UML de la relation *Considère*

3.5 Contextes

L'entité *contexte* spécifie les circonstances concrètes dans lesquelles les organisations accordent des permissions à des rôles pour réaliser des activités sur des vues. Dans notre proposition, nous avons utilisé la relation *Définit* à fin de lier les cinq entités : *Organisation*, *Sujet*, *Action* , *Objet* et *Contexte* qui sont déjà identifiées précédemment. L'exemple suivant illustre la relation *Définit* : *Définit(Organisation de santé, Mohamed, lire, F1.doc, urgence)* : signifie que "dans le contexte *urgence*, le sujet *Mohamed* est autorisé de *lire* le dossier *F1.doc* dans l'organisation *Organisation de santé*". La figure 3.12 présente la modélisation UML de la relation *Définit*.

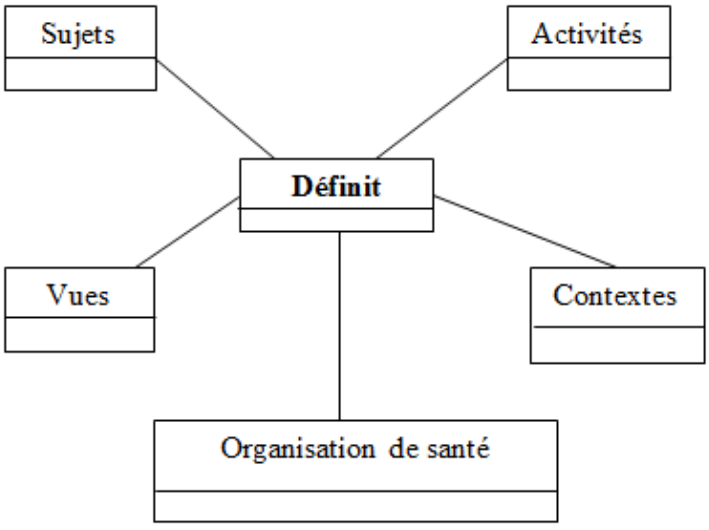


FIGURE 3.12 – Modélisation UML de la relation *Définit*

Dans notre modèle, nous avons identifié les contextes suivants :

1. Urgence (U) : ce contexte est activé dans le cas d'urgence.

2. Temporel (T) : ce sont des contextes régissant la durée de validité des droits d'accès au dossier médical. Dans notre modèle, nous avons identifié deux contextes [35] :
   – T1 : heures de travail (I) :
   $$h \geqslant 8h$$
   &
   $$h \leqslant 17h$$
   – T2 : heures de travail (II) :
   $$h \geqslant 17h$$
   &
   $$h \leqslant 8h$$
3. Spatial (S) : ce contexte peut être physique dépendant d'une position, ou logique (appartenance à un réseau, Cellule GSM, etc.). Dans notre modèle, nous avons identifié deux contextes :
   – S1 : à l'intérieur de l'organisation de santé.
   – S2 : hors de l'organisation de santé.
4. Composé : à partir des contextes précédents nous avons construit par composition les contextes suivants :
   – T3 : T1&T2.
   – S3 : S1&S2.
   – T3S3 : T3&S3.
   – UT3S3 : U&T3&S3.
   – T1S1 : T1&S1.
   – UT1S1 : U&T1&S1
   – T1S2 : T1&S2.
   – UT1S2 : U&T1&S2.
   – T2S1 : T2&S1.
   – UT2S1 : U&T2&S1.
   – T2S2 : T2&S2.
   – UT2S2 : U&T2&S2.
   – T1S3 : T1&S3.
   – UT1S3 : U&T1&S3.
   – T2S3 : T2&S3.
   – UT2S3 : U&T2&S3.
   – S1T3 : S1&T3.
   – US1T3 : U&S1&T3.
   – S2T3 : S2&T3.
   – US2T3 : U&S2&T3.

La figure 3.13 présente la modélisation UML de l'entité *contexte*.

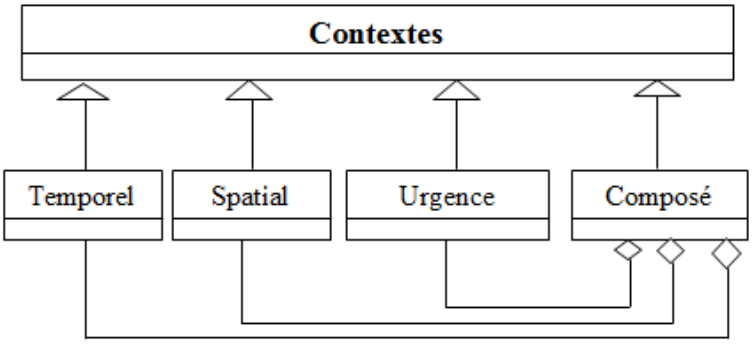


FIGURE 3.13 – Modélisation UML de l'entité *Contexte*

4 Spécification de la politique de sécurité

En utilisant les entités et les relations introduites dans la section précédente, nous allons définir la politique de sécurité appliquée à une organisation de santé. Cette politique de sécurité réglemente les accès au système à travers des permissions, pour cela, nous avons introduit une nouvelle entité appelée *Permission* afin de relier entre les *Organisations*, les *Rôles*, les *Vues*, les *Activités* et les *Contextes*. Voici un exemple qui illustre la spécification de la politique de sécurité à base de modèle de CA Or-BAC : L'organisation de santé accorde au professeur la permission de consulter la vue identification dans le contexte d'urgence. Cette règle de sécurité est exprimée comme suit :

Permission (Organisation de santé, professeur, consulter, identification, urgence).

La figure 3.14 présente la modélisation UML de l'entité *Permission* qui relie les différents concepts du modèle de CA Or-BAC.

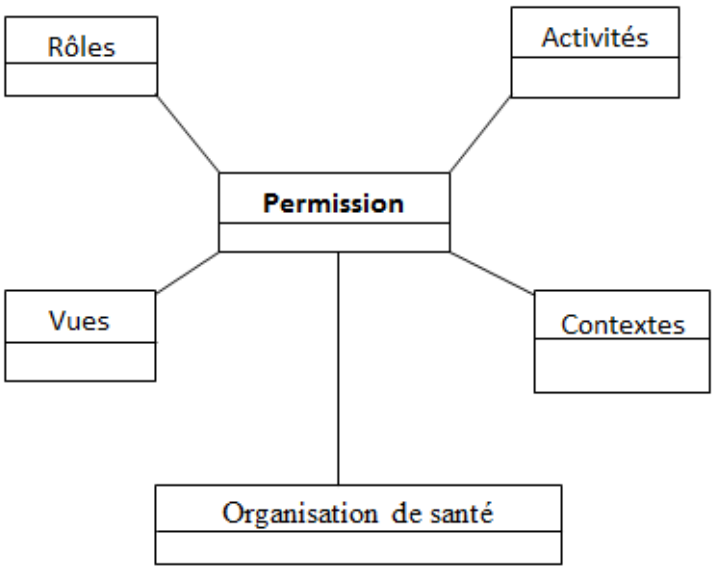


FIGURE 3.14 – Modélisation UML de l'entité *Permission* qui relie les différents concepts du modèle de CA Or-BAC

Dans le cadre de notre étude, nous avons construit 1595 règles de permissions pour les différents rôles. Une analyse plus fine de ces règles nous a permis de faire une optimisation du nombre de ces règles. La conséquence est un nombre réduit de règles, nous permettant ainsi une maintenance facile de notre politique de CA.

Dans notre proposition, nous avons passé par quatre propositions d'amélioration sous la forme de contributions pour obtenir à la fin un nombre de règles optimal :

Contribution 01

Dans la première contribution, nous avons affecté les droits d'accès des différents rôles sur les différentes vues selon les contextes *" U, T1, T2, S1, S2, T3 et S3"*. Ces permissions sont définies selon des avis de plusieurs experts qui travaillent dans des organisations de santé différentes. Avec cette modélisation, nous avons élaboré 1595 règles de permissions, par exemple le rôle professeur a 135 règles de permissions tandis que l'infirmier possède 42 règles de permissions. Nous avons organisé ces droits d'accès sous la forme d'un tableau de 25 lignes et 16 colonnes (voir Tableau 3.3), les lignes représentent les rôles tandis que les colonnes représentent les vues. L'intersection des lignes et colonnes forme les différentes permissions accordées selon les contextes. Par exemple, dans la première ligne, nous pouvons lire les règles suivantes : le professeur a le droit de consulter et transférer la vue *Identification* dans le contexte *U* (urgence), *T3*(T1&T2) et *S3*(S1&S2) mais il n'a que le droit de consulter la vue *Don d'organes* dans les différents contextes.

	Identification	...	Don d'organes
Professeur	consulter (U, T3, S3) transférer (U, T3, S3)	...	consulter (U, T3, S3)
...	...	...	...
Infirmier	consulter (U, S1, T3)	...	-

TABLE 3.3 – Répartition des droits d'accès

Contribution 02

Nous avons constaté que les mêmes règles de CA se répètent pour des contextes différents, par exemple dans le tableau 3.3 le droit d'accès en consultation pour le rôle professeur sur la vue *identification* est défini par les règles de permissions suivantes :

Permission (Organisation de santé, professeur, consulter, Identification, U).

Permission (Organisation de santé, professeur, consulter, Identification, T3).

Permission (Organisation de santé, professeur, consulter, Identification, S3).

Nous avons dans cet exemple la même règle qui se répète trois fois pour les contextes U, T3 et S3. Pour pallier ce problème et à fin de minimiser le nombre de règles, nous avons augmenté le nombre de contextes composés de deux contextes (T3, S3) à 20 contextes : *T3 (T1&T2), S3 (S1&S2)T3S3 (T3&S3), UT3S3 (U&T3&S3), T1S1 (T1&S1), UT1S1 (U&T1&S1), T1S2 (T1&S2), UT1S2 (U&T1&S2), T2S1 (T2&S1), UT2S1 (U&T2&S1), T2S2 (T2&S2), UT2S2 (U&T2&S2), T1S3 (T1&S3), UT1S3 (U&T1&S3), T2S3 (T2&S3), UT2S3 (U&T2&S3), S1T3 (S1&T3), US1T3 (U&S1&T3), S2T3 (S2&T3), US2T3 (U&S2&T3).*

Avec cette modélisation le droit d'accès en consultation pour le rôle professeur sur la vue *Identification* est traduit en une seule règle de permission :

Permission (Organisation de santé, professeur, consulter, Identification, UT3S3).

Cette deuxième contribution a amélioré notre modèle en diminuant le nombre de règles de 1595 à 533. Par exemple pour le rôle professeur, nous avons 45 règles au lieu de 135 règles.

Contribution 03

Afin de réduire encore plus le nombre de règles, nous avons proposé d'utiliser la politique de CA mixte qui prend en compte les permissions et les interdictions. Pour cela, nous avons introduit une nouvelle entité appelée *Interdiction* qui relie les organisations, les rôles, les vues, les activités et les contextes.

Par exemple : *L'organisation de santé* interdit au *professeur* de *supprimer* la vue *Identification* dans le contexte composé *UT3S3*. Cette règle de sécurité est exprimée comme suite :

Interdiction(Organisation de santé, professeur, supprimer, Identification, UT3S3).

En règle générale, si un rôle a plusieurs règles de permissions (interdictions) pour une vue et peu de règles d'interdictions (permissions) pour cette vue alors nous pouvons définir pour ce rôle uniquement les règles d'interdictions (permissions) pour cette vue.

Par exemple le rôle professeur est permis d'ajouter, consulter, modifier et transférer dans la vue *Rencontre* dans le contexte *UT3S3*, donc il a quatre règles de permissions :

Permission (Organisation de santé, professeur, consulter, Rencontre, UT3S3).
Permission (Organisation de santé, professeur, ajouter, Rencontre, UT3S3).
Permission (Organisation de santé, professeur, modifier, Rencontre, UT3S3).
Permission (Organisation de santé, professeur, transférer, Rencontre, UT3S3).

Et ce professeur n'a pas le droit de supprimer dans la vue *Rencontre* dans le contexte *UT3S3*, donc il a une seule règle d'interdiction :

Interdiction(Organisation de santé, professeur, supprimer, Rencontre, UT3S3).

En conséquence, nous défissions les règles d'interdictions pour le professeur dans la vue *Rencontre* dans le contexte UT3S3. Tans dit que pour la vue *Garde malade* le professeur a uniquement le droit de consulter dans le contexte *UT3S3*, donc il a une seule règle de permission :

Permission (Organisation de santé, professeur, consulter, Garde malade, UT3S3).

Et ce professeur n'a pas le droit ni de modifier, ni d'ajouter, ni de transférer, ni de supprimer dans la vue *Garde malade* dans le contexte *UT3S3* donc il a quatre règles d'interdictions :

Interdiction(Organisation de santé, professeur, modifier, Garde malade, UT3S3).
Interdiction(Organisation de santé , professeur, ajouter, Garde malade, UT3S3).
Interdiction(Organisation de santé, professeur, transférer, Garde malade, UT3S3).
Interdiction(Organisation de santé, professeur, supprimer, Garde malade, UT3S3).

Alors dans ce cas, nous allons définir les règles de permissions pour le professeur dans la vue *Garde malade* dans le contexte *UT3S3*.

Avec cette nouvelle politique (mixte) nous avons élaboré 267 (178 permissions et 89 interdictions) règles au lieu de 533 règles de permissions, par exemple pour le professeur nous avons 18 règles (9 permissions et 9 interdictions) au lieu de 45 règles de permissions.

Contribution 04

Dans notre politique de sécurité, nous avons remarqué qu'il y a des rôles qui possèdent les mêmes règles de CA, pour cela, nous avons regroupé ces rôles dans un seul rôle. Avec cette modélisation, nous avons regroupé les rôles suivants :

1. Rôle *cadre médical* regroupe :
   - professeur
   - MCA
   - MCB
   - Médecin assistant
   - Médecin spécialiste
2. Rôle *cadre paramédical* regroupe :
   - Aide-soignant
   - Infirmier
   - Cadre de santé
   - Coordinateur

En utilisant cette nouvelle catégorisation de rôles, nous avons pu diminuer le nombre de règles de 263 règles à 172 règles de CA dont 48 règles d'interdictions et 124 règles de permissions. Toutes les règles de permissions et d'interdictions de notre politique de CA finale sont présentées sous la forme d'un tableau en annexe (voir annexe F).

La figure 3.15 représente la modélisation UML de notre politique de CA.

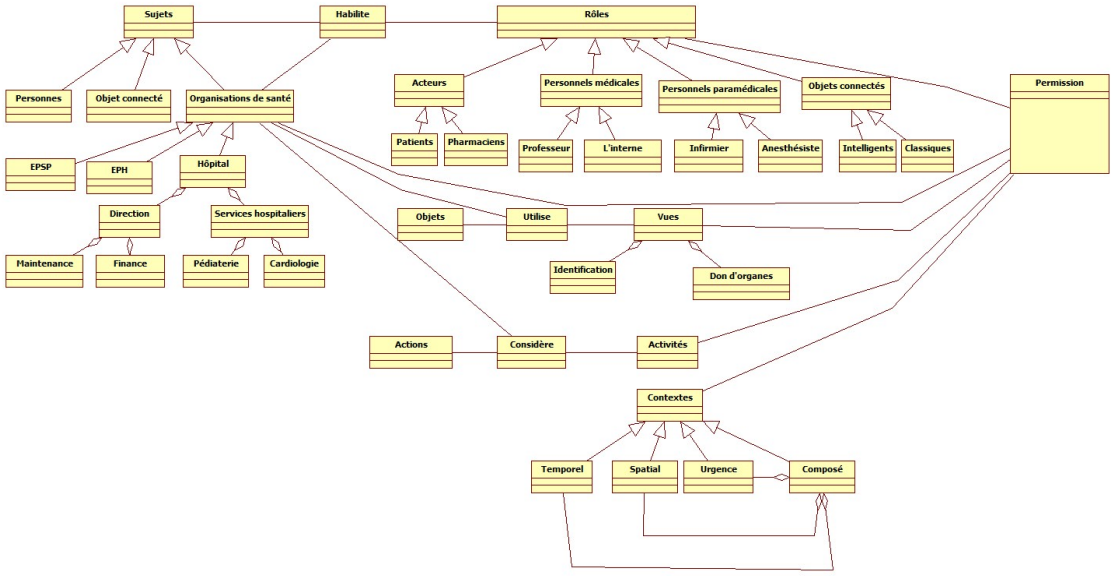


FIGURE 3.15 – Modélisation UML de notre politique de CA

5 Conclusion

Dans ce chapitre, nous avons d'abord réalisé une comparaison entre les différents modèles de CA de base, ce qui nous a permis de choisir le modèle de CA le plus adapté et le plus approprié, pour le domaine traité dans le cadre de cette thèse, à savoir le modèle à base d'organisation. Ensuite, sur la base de la

modélisation XML du DM développée dans le chapitre un, nous avons proposé un modèle pour le CA à ce dossier en se basant sur le modèle Or-BAC. Les différentes entités et relations du modèle proposé ont été modélisées graphiquement en utilisant les diagrammes de classe UML.

En se basant sur les entités trouvées de notre modèle de CA, nous avons passé par quatre contributions pour obtenir à la fin un nombre de règles optimal [104] :

1. *Contribution 1* : Nous avons construit dans un premier temps 1595 règles de permissions pour les différents rôles.
2. *Contribution 2* : Nous avons constaté que l'ajout de certains contextes composés peut diminuer le nombre de règles de permissions ce qui a une conséquence la réduction de la complexité du modèle proposé. À cet effet, nous avons réduit dans un second temps, le nombre de règles de 1595 à 533.
3. *Contribution 3* : Puisque dans le modèle Or-BAC nous pouvons définir même les interdictions, nous avons donc proposé d'ajouter les règles d'interdictions. Avec cette proposition, nous avons pu élaborer 267 règles de CA (178 permissions et 89 interdictions).
4. *Contribution 4* :Nous avons constaté aussi qu'il existe des rôles qui ont les mêmes règles d'accès et par conséquent nous pouvons les regrouper dans un seul rôle. Ce constat nous a permis de diminuer encore plus le nombre de règles à savoir de 267 à 172 dont 124 permissions et 48 interdictions.

Dans le chapitre suivant, nous allons présenter l'implémentation et la validation de cette politique de sécurité en utilisant deux outils : *MotOr-BAC* et *Protégé*.

Chapitre 4

Implémentation et validation de la politique de CA

1 Introduction

En se basant sur le modèle de CA proposé dans le chapitre précédent, ce chapitre est consacré à la description de l'implémentation et la validation de ce modèle. Pour se faire, nous avons utilisé deux outils différents à savoir : l'outil *MotOrBAC* qui permet de développer et valider les modèles de CA basés sur Or-BAC, et l'outil *Protégé* qui permet aussi de construire et valider la politique de CA sous la forme d'une ontologie.

2 Implémentation et validation de la politique de CA

Dans cette section, nous allons présenter pour chaque outil :
- Le principe de son fonctionnement ainsi que son architecture.
- L'implémentation et la validation de notre politique de sécurité en utilisant cet outil.
- Les résultats obtenus de cette implémentation.

2.1 *MotOrBAC*

L'outil MotOrBAC [1] (Moteur Or-BAC) permet de concevoir, charger et sauvegarder des politiques de sécurité. Il a été proposé dans le cadre de recherche entamé dans [7] [105] *MotOrBAC* est développé en langage Java, il permet l'implémentation et l'administration du modèle de CA Or-BAC.

Étant donné que le modèle Or-BAC permet l'expression de politiques mixtes contenant à la fois des permissions et des interdictions, MotOrBAC inclut un algorithme de détection de conflits et des stratégies de résolution de conflits pour aider les utilisateurs à trouver et résoudre les conflits. Ainsi, avec cet outil, il est possible de passer du général (abstrait) au particulier (concret) dans l'expression d'une politique de sécurité. En désignant des sous-organisations de l'organisa-

1. http ://motorbac.sourceforge.net/index.php ?page=download&=fr

tion mère, on peut même déléguer certaines tâches d'administration à des sujets jouant des rôles différents.

L'architecture de *MotOrBAC* est présentée dans la figure 4.1. Ce prototype est composé de quatre modules [106] :

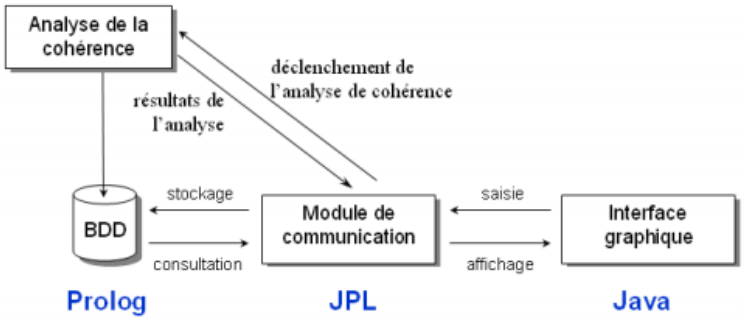


FIGURE 4.1 – Architecture de MotOrBAC [7]

- L'analyseur de cohérence de la politique : ce module permet de valider automatiquement les règles d'une politique de sécurité en détectant la redondance et l'inconsistance des règles.
- La sauvegarde des données : les données relatives aux éléments de la politique de sécurité sont enregistrées et représentées en XML (ou Prolog).
- Le module de communication : il joue le rôle d'intermédiaire entre les différents modules.
- L'interface graphique : est utilisée pour simplifier la saisie ou la modification des politiques de sécurité. Pour une description plus détaillée de cette interface voir annexe I.

2.1.1 Implémentation du modèle proposé avec *MotOrBAC*

Sur la base du modèle, développé dans le chapitre précédent, de la politique de sécurité du DM dans le cas d'une organisation de santé algérienne, nous avons implémenté cette politique avec *MotOrBAC* [104].

nous avons commencé par l'implémentation de la hiérarchie de l'organisation de santé (voir figure 4.2).

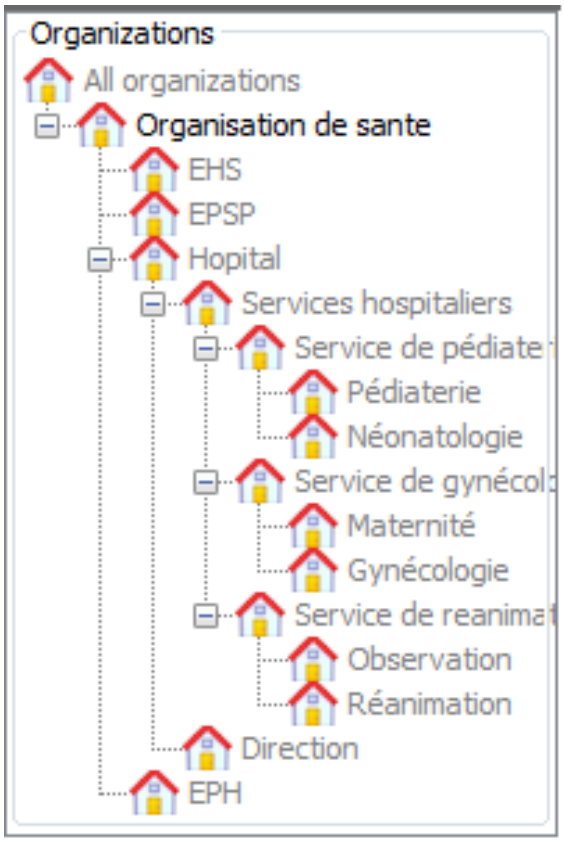


FIGURE 4.2 – Hiérarchie de l'organisation de santé du modèle proposé avec MotOrBAC

Nous avons ensuite implémenté les rôles de notre modèle (voir figure 4.3) et nous avons habilité des sujets à des rôles différents.

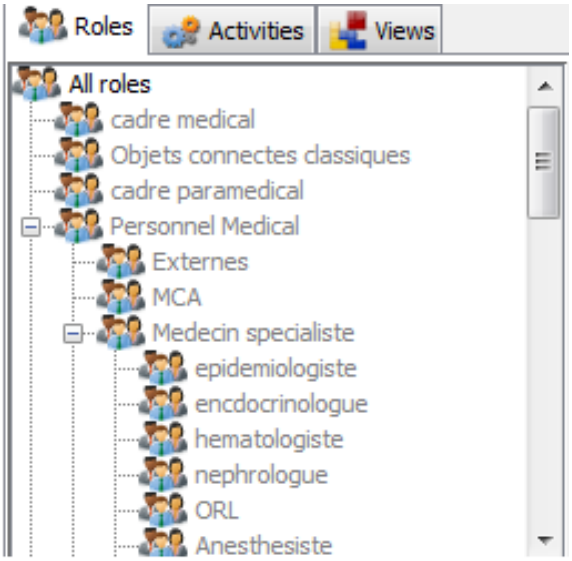


FIGURE 4.3 – Hiérarchie des rôles du modèle proposé avec MotOrBAC

Par la suite nous avons implémenté toutes les vues de notre politique (voir figure 4.4), et nous avons également spécifié les objets que la vue utilise.

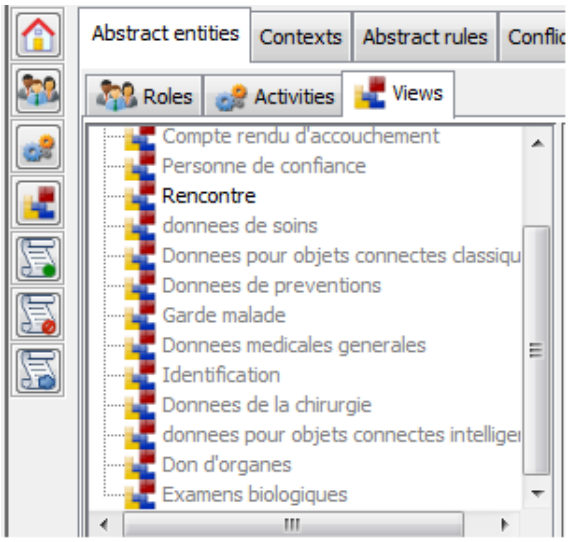


FIGURE 4.4 – Hiérarchie des vues du modèle proposé dans MotOrBAC

Nous avons aussi spécifié les différentes activités (voir figure 4.5), et les différentes actions.

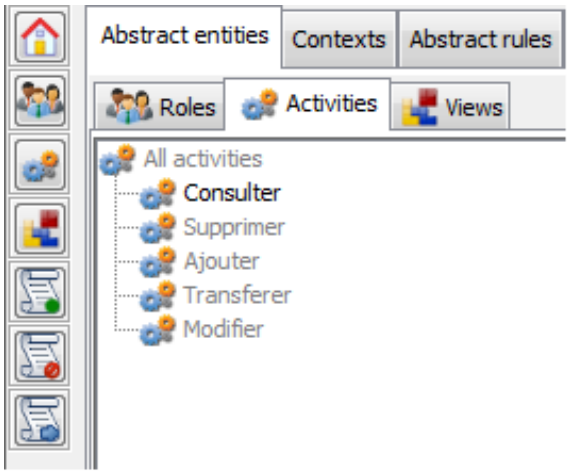


FIGURE 4.5 – Hiérarchie des activités

Nous avons spécifié tous les contextes de notre politique de sécurité (voir figure 4.6).

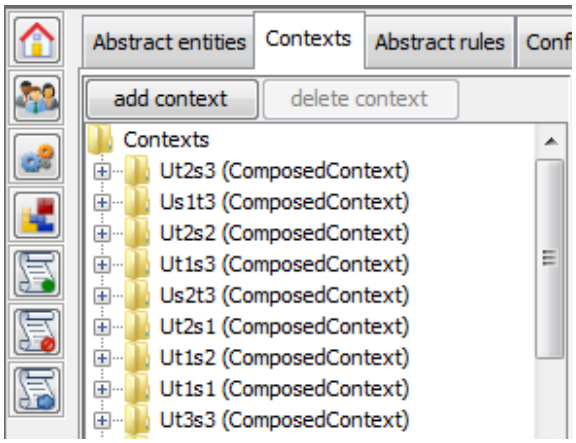


FIGURE 4.6 – Spécification des contextes du modèle proposé avec MotOrBAC

Finalement, nous avons défini les différentes règles de permissions (voir figure 4.7) et d'interdictions de notre politique de sécurité. Il y a lieu à constater que MotOrBAC valide au fur et à mesure les règles du modèle et signale d'éventuel conflit existant entre les règles (voir figure 4.8), ce qui permet de faire des corrections et ainsi obtenir un modèle de CA valide.

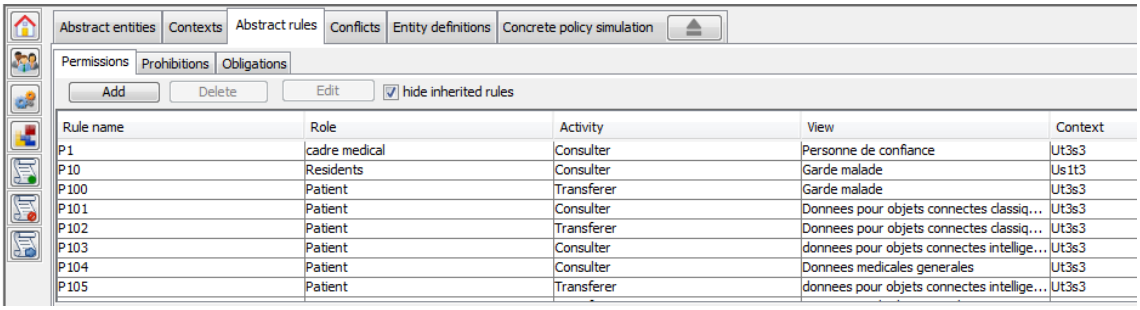


FIGURE 4.7 – Spécification des règles de permissions du modèle proposé avec MotOrBAC

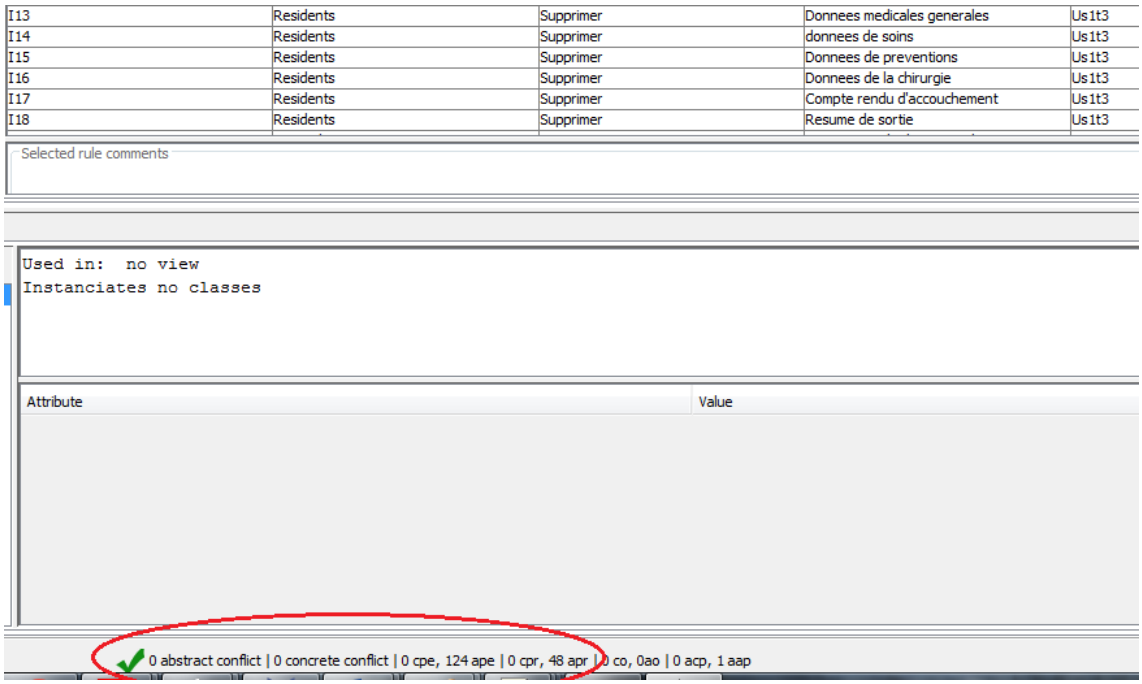


FIGURE 4.8 – Validation de la politique de sécurité du modèle proposé avec MotOrBAC

2.1.2 Discussion

Pour la validation et l'implémentation de la spécification de notre modèle de CA, nous avons utilisé *MotOrBAC*, cet outil est gratuit, disponible et facile à utiliser. Il permet d'analyser, spécifier et simuler une politique de sécurité. Ainsi, il est possible de passer du niveau abstrait au niveau concret, et même de déléguer certaines tâches d'administration à des sujets jouant des rôles différents. Ce dernier nous a permis d'implémenter toutes les règles de permissions (124 règles) et d'interdictions (48 règles) de notre politique de sécurité. Le résultat de cette opération est un fichier XML qui décrit notre spécification de CA (voir annexe G qui représente une partie de cette spécification). Il y a lieu à noter que MotOrBAC ne permet pas de faire l'optimisation du modèle de CA en nombre de règles, autrement l'utilisateur doit introduire le modèle final optimisé. Doter cet outil avec un module permettant d'introduire le modèle de CA de départ et aider l'utilisateur à optimiser son modèle en lui proposant les optimisations nécessaires ne fait qu'augmenter l'efficacité de l'outil en question.

2.2 *Protégé*

Protégé [107] [108] crée au Stanford Medical Informatics de l'Université de Stanford, est un outil pour le développement des ontologies, il est distribué en open source. Il permet le contrôle, la visualisation et l'édition des ontologies. Protégé permet de manipuler des formats très divers comme OWL, RDF (Resource Description Framework), etc. L'interface graphique de Protégé regroupe plusieurs fonctionnalités comme la création des classes, des propriétés, des instances, des relations, etc. et permet également de visualiser graphiquement une

ontologie, et même exporter une ontologie en fichier XML (figure 4.9) :

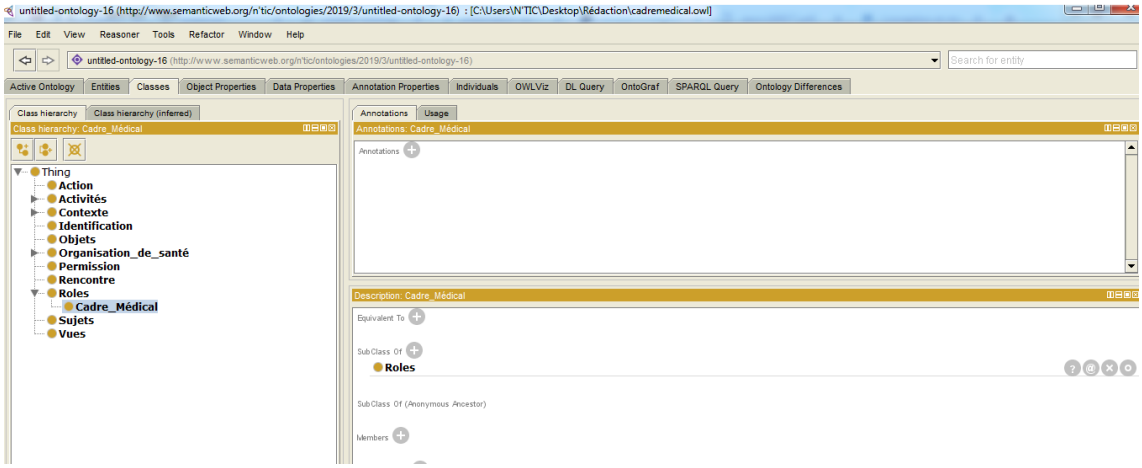


FIGURE 4.9 – Interface graphique de *Protégé*

2.2.1 Implémentation de la politique de sécurité avec *Protégé*

Sur la base du modèle de CA que nous avons proposé, nous avons implémenté ce dernier avec Protégé. Nous avons d'abord défini la hiérarchie des classes de notre modèle, ensuite, nous avons définis les différentes propriétés qui vont être utilisées pour relier les différentes classes entre eux.

Pour spécifier les règles de notre politique de sécurité nous avons ajouter une classe permission (interdiction) qui permet de relier les différentes entités de notre modèle, la figure 4.10 montre une partie de l'ontologie développée :

– Un cadre médical est permis de consulter la vue identification dans le contexte composé UT3S3.

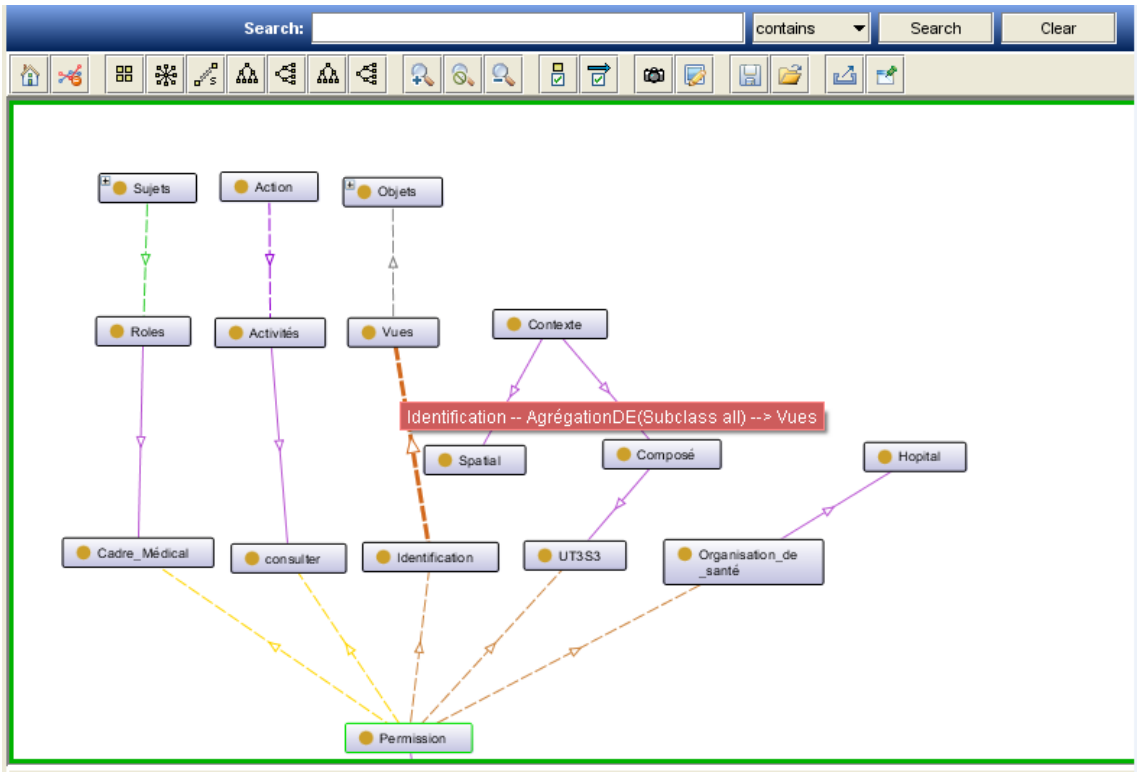


FIGURE 4.10 – Une partie du modèle de CA proposé avec Protégé

2.2.2 Discussion

Pour la validation et l'implémentation de la spécification de notre modèle de CA, nous avons utilisé *Protégé*, c'est un outil gratuit, facile et simple à utiliser, il nous a permis d'implémenter les différente classes et objets du modèle de CA que nous avons proposé. Le module de la visualisation graphique du modèle introduit dans Protégé nous a été d'une aide précieuse dans l'élaboration de notre modèle de CA. Pour valider et vérifier la cohérence de notre modèle nous avons utilisé le module de raisonnement intégré dans Protégé. Le module exporter de Protégé permet de sauvegarder notre modèle dans un fichier avec un format approprié (RDF, OWL,...) (voir annexe H qui présente une partie de cette spécification).

3 Conclusion

Dans ce chapitre, nous avons présenté la partie implémentation et la validation de notre modèle de CA pour une organisation de santé algérienne en utilisant l'outil *MotOrBAC* et *Protégé*. Ces deux outils nous ont permis d'implémenter toutes les règles de permissions et d'interdictions de notre modèle. Le résultat obtenu par ces deux outils est un fichier XML qui décrit notre modèle de CA.

La validation du modèle proposé à l'aide de ces deux outils nous a permis un passage sûr vers une spécification implémentable et en conséquence le développement d'un ensemble d'outils simples et efficaces pour la prise en charge de cet aspect dans l'application de gestion du DM.

Conclusion générale

Le DM informatisé comprend toutes les informations concernant un malade, ce dossier permet de stocker, rechercher et manipuler l'information saisie lors des consultations des patients. Il permet de partager les données du patient avec les professionnels et les établissements de santé ce qui a une conséquence la coordination et la continuité des soins. La gestion des données du patient suppose donc l'existence des outils efficaces pour le CA.

L'objectif de ce travail de recherche est centré sur le CA dans les systèmes d'information en santé et plus spécifiquement sur les modèles de CA. Il s'agit donc de proposer une modélisation rigoureuse permettant de prendre en charge tous les aspects liés à la gestion sécurisée du dossier médical informatisé.

Dans un premier temps, à la suite d'une analyse de l'existant, nous avons proposé un modèle en XML pour le DM dans le contexte d'une organisation de santé algérienne. Sur la base de cette modélisation, dans un second temps, après une étude comparative des modèles de CA existants et un choix du modèle le plus approprié dans le cadre notre étude, nous avons développé un modèle pour le CA à ce dossier en se basant sur le modèle Or-BAC. Les différentes entités et relations du modèle proposé ont été modélisées graphiquement en utilisant les diagrammes de classe UML. Grâce à une analyse plus profonde des règles de CA, nous avons pu réduire le nombre de ces règles de 1595 à 172 dont 124 règles de permissions et 48 règles d'interdictions.

L'implémentation et la validation du modèle proposé à l'aide des outils MotOrBAC et Protégé nous ont permis un passage sûr vers une spécification valide et implémentable et en conséquence le développement d'un ensemble d'outils simples et efficaces pour la prise en charge de l'aspect CA au DM.

Perspectives

Avant de clôturer cette thèse, il est important de renseigner sur les éventuelles pistes de développement envisageables à nos travaux de recherche :

1. *Automatisation de la procédure d'optimisation des règles d'accès :* Tous les modèles proposés dans la littérature produisent un nombre de règles non optimisé et c'est l'administrateur chargé d'affecter les différents droits d'accès aux différents rôles du CA qui, d'une façon ad-hoc et manuelle, peut envisager de faire une analyse et optimisation de ces règles de CA. Il serait donc envisageable d'automatiser la procédure d'optimisation de ces règles

afin de faciliter le travail de l'administrateur du système pour produire un nombre réduit de règles d'accès.

2. *Intégration de la politique de CA :* en effet, dans ce travail de recherche nous avons modélisé l'aspect CA pour le DM dans le contexte d'une organisation de santé algérienne, pour mettre en œuvre cet aspect dans un logiciel de gestion du DM il est intéressant de développer un outil d'aide à son intégration automatique. Pour se faire nous pouvons compter sur l'approche de POA (Programmation Orientée Aspect) qui permet de traiter séparément les préoccupations transversales qui relèvent souvent de la technique, des préoccupations métier qui construit le cœur d'une application. Le choix de cette technique est du grâce aux nombreux avantages qu'elle présente comme :
   – Une maintenance aisée,
   – Une meilleure réutilisation des différents modules,
   – Une simplification et une amélioration de code,
   – Un gain de productivité.

   Dans notre application, le programme codé en orienté aspect peut être découpé en deux parties disjointes :

   (a) Les classes pour la partie métier qui représente le DM informatisé.

   (b) Les aspects pour la partie technique qui représente notre spécification de CA.

   La POA est l'outil le plus adapté pour intégrer notre politique de sécurité dans un système de gestion du DM.

Bibliographie

[1] C. Gonnetan, *Avantages et incovénients du dossier médical informatisé dans le cadre de l'odontologie médico-légale*, Ph.D. thesis, Université de Nantes, 2017.

[2] Anas Abou El Kalam, Rania El Baida, Philippe Balbiani, Salem Benferhat, Frédéric Cuppens, Yves Deswarte, Alexandre Miege, Claire Saurel, and Gilles Trouessin, "Or-bac : un modèle de contrôle d'accès basé sur les organisations," *Cahiers francophones de la recherche en sécurité de l'information*, vol. 1, pp. 30–43, 2003.

[3] S Boulares, "Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès," *Mémoire de Maître en Sciences, Université du Québec en Outaouais*, 2010.

[4] Romuald Thion and Stéphane Coulondre, "Contrôle d'accès pour les modèles à rôles en environnement pervasif," in *XXIIème Congrès INFORSID, Atelier "Sécurité des Systèmes d'Information", SSI'04*, Biarritz, France, May 2004, p. 00.

[5] BENDIAB GUELTOUM, *Sécurité des applications métiers au niveau du Cloud Computing : Contrôle d'accès au niveau des APIs du Cloud Computing*, Ph.D. thesis, Université Abdelhamid Mehri, Constantine 2, 2015.

[6] Abdeljebar Ameziane El Hassani, *Le contrôle d'accès des réseaux et grandes infrastructures critiques distribuées*, Ph.D. thesis, 2016.

[7] Frédéric Cuppens, Nora Cuppens-Boulahia, and Céline Coma, "Motorbac : un outil d'administration et de simulation de politiques de sécurité," in *Security in Network Architectures (SAR) and Security of Information Systems (SSI), First Joint Conference*, 2006, pp. 6–9.

[8] MOUTEL G, "Evolution du dossier medical, nouveaux enjeux de la relation mÉdecins-soignantspatients : Approche historique, medicale, médicolegale et ethique," 2004.

[9] Comité éditorial pédagogique de l'UVMaF, "Le dossier médical," 2011-1012.

[10] Claire Gekiere and Serge Soudan, "Dossier patient informatisé et confidentialité : évolution des modèles et des pratiques.«le diable gît dans les détails»," *L'information psychiatrique*, vol. 91, no. 4, pp. 323–330, 2015.

[11] "https ://medium.com/doctolib/dossier-m(consulté le 26/11/2018)," .

[12] "https ://www.dmp.fr/ (consulté le 26/11/2018)," .

[13] A.Benoudah N.Guendoussi A.Belaidi M.Abderrahim, "Conception et réalisation d'une application pour la gestion du dossier médical personnel

(etude de cas : Chu algérien)," M.S. thesis, Université Abou Bekr Belkaid Tlemcen, Faculté de Technologie, 2017.

[14] "https ://goo.gl/mx4hgs (consulté le 20/12/2018)," .

[15] "http ://www.gestionbienetre.com/lelogiciel.html (consulté le 20/12/2018)," .

[16] "https ://goo.gl/0glsqe (consulté le 20/12/2018)," .

[17] "https ://dawhois.com/site/elixir-sante.com.html (consulté le 20/12/2018)," .

[18] N.Debian F.Zegmali A.Belaidi M. Abderrahim, "Développement d'un modèle pour ie contrôle d'accès au dossier médical personnel (etude de cas : Chu algérien)," M.S. thesis, Université Abou Bekr Belkaid Tlemcen, Faculté de Technologie, 2017.

[19] "https ://goo.gl/ltzmzw (consulté le 06/01/2019)," .

[20] "https ://www.medimust.com/ (consulté le 06/01/2019)," .

[21] "https ://fr.wikipedia.org/wiki/mediboard (consulté le 07/01/2019)," .

[22] "http ://www.secuinfo.fr/les-methodes-de-controle-dacces/ (consulté le 15/01/2019)," .

[23] A.Haddad, "Modélisation et vérification de politique de sécurité," M.S. thesis, Université Joseph Fourier Genève, 2005.

[24] Butler W Lampson and In Protection, "5th princeton symposium on information science and systems," *ACM Operating Systems Review*, vol. 8, no. 1, pp. 437–443, 1971.

[25] Guillaume Harry, "Iam-gestion des identités et des accès : concepts et états de l'art," 2013.

[26] Michael A Harrison, Walter L Ruzzo, and Jeffrey D Ullman, "Protection in operating systems," *Communications of the ACM*, vol. 19, no. 8, pp. 461–471, 1976.

[27] Anita K Jones, Richard J Lipton, and Lawrence Snyder, "A linear time algorithm for deciding security," in *17th Annual Symposium on Foundations of Computer Science (sfcs 1976)*. IEEE, 1976, pp. 33–41.

[28] Anas Abou El Kalam, *Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales*, Ph.D. thesis, Institut National Polytechnique de Toulouse-INPT, 2003.

[29] Laurent Poinso, "Chap. ii : Politiques et modèles de sécurité," Tech. Rep., UMR 7030 - Université Paris 13 - Institut Galilée.

[30] Ravi S Sandhu, "The typed access matrix model," in *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*. IEEE, 1992, pp. 122–136.

[31] Ravi S Sandhu and Srinivas Ganta, "On testing for absence of rights in access control models," in *Computer Security Foundations Workshop VI, 1993. Proceedings*. IEEE, 1993, pp. 109–118.

[32] M.Merabat K. El Hadj Mimoune, "Etude de sécurité en base de données avec une application pour le contrôle d'accès," M.S. thesis, Université Abou Bakr Belkaid, 2011.

[33] G. BUJDOSÓ, "Elaboration de modèles d'accès à des ressources partagées dans un groupe," M.S. thesis, Université de Savoie et de l'Ecole Nationale Supérieure des Mines de Saint-Etienne, 2000.

[34] Saïda Medjdoub, *Modèle de contrôle d'accès pour XML :" Application à la protection des données personnelles"*, Ph.D. thesis, Université de Versailles-Saint Quentin en Yvelines, 2005.

[35] Djahida Haouche, "Sécurisation des données de santé informatisées.," M.S. thesis, Université Abou Bakr Belkaid Tlemcen, 2015.

[36] A Abou El Kalam, "Politiques de sécurité pour les systèmes d'informations médicales," *Cinquièmes Journées Doctorales en Informatiques et Réseaux (JDIR*, pp. 201–210, 2002.

[37] Alban Gabillon, "Contrôler les accès aux données numériques," 2013.

[38] D Elliott Bell and Leonard J La Padula, "Secure computer system : Unified exposition and multics interpretation," Tech. Rep., MITRE CORP BEDFORD MA, 1976.

[39] Kenneth J Biba, "Integrity considerations for secure computer systems," Tech. Rep., MITRE CORP BEDFORD MA, 1977.

[40] David D Clark and David R Wilson, "A comparison of commercial and military computer security policies," in *1987 IEEE Symposium on Security and Privacy*. IEEE, 1987, pp. 184–184.

[41] IKHLASS HATTAK, *ANALYSE FORMELLE DES POLITIQUES DE SÉCURITÉ*, Ph.D. thesis, UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS, Département d'informatique et d'ingénierie, 2010.

[42] David FC Brewer and Michael J Nash, "The chinese wall security policy," in *Proceedings. 1989 IEEE Symposium on Security and Privacy*. IEEE, 1989, pp. 206–214.

[43] Mickaël Salaün, *Intégration de l'utilisateur au contrôle d'accès : du processus cloisonné à l'interface homme-machine de confiance*, Ph.D. thesis, Institut National des Télécommunication, 2018.

[44] Ravi Sandhu, "Role hierarchies and constraints for lattice-based access controls," in *European Symposium on Research in Computer Security*. Springer, 1996, pp. 65–79.

[45] David F Ferraiolo, Ravi Sandhu, Serban Gavrila, D Richard Kuhn, and Ramaswamy Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[46] Céline Coma—Nora Cuppens-Boulahia and Frédéric Cuppens, "Analyse et modélisation de contrôles d'accès au système ged," .

[47] Romuald Thion and Stéphane Coulondre, "Intégration du contexte spatio-temporel dans le contrôle d accés basé sur les rôles," *Revue des Sciences et Technologies de l'Information-Série ISI : Ingénierie des Systèmes d'Information*, vol. 10, pp. 89–117, 2004.

[48] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari, "Trbac : A temporal role-based access control model," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 191–233, 2001.

[49] Dana Al Kukhun and Florence Sèdes, "La mise en œuvre d'un modèle de contrôle d'accès adapté aux systèmes pervasifs," *Document numérique*, vol. 12, no. 3, pp. 59–78, 2009.

[50] Wonil Kim Chae, Song-Hwa and Dong-Kyoo Kim, "ut-rbac : Ubiquitous role-based access control model," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 89.1 : 238-239*, 2006.

[51] Maria Luisa Damiani, Elisa Bertino, Barbara Catania, and Paolo Perlasca, "Geo-rbac : a spatially aware rbac," *ACM Transactions on Information and System Security (TISSEC)*, vol. 10, no. 1, pp. 2, 2007.

[52] Marwan Cheaito, *Un cadre de spécification et de déploiement de politiques d'autorisation*, Ph.D. thesis, Université de Toulouse, Université Toulouse III-Paul Sabatier, 2012.

[53] Seon-Ho Park, Young-Ju Han, and Tai-Myoung Chung, "Context-role based access control for context-aware application," in *International Conference on High Performance Computing and Communications*. Springer, 2006, pp. 572–580.

[54] ZERKOUK Meriem, *Modèles de contrôle d'accès dynamiques*, Ph.D. thesis, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2015.

[55] Devdatta Kulkarni and Anand Tripathi, "Context-aware role-based access control in pervasive computing systems.," in *Proceedings of the 13th ACM symposium on Access control models and technologies. ACM*, 2008.

[56] A Abou El Kalam and Yves Deswarte, "Contrôle d'accès basés sur les rôles, les groupes d'objets et le contexte : Étude de cas dans les systèmes d'information et de communication en santé," in *Actes de la conférence Sécurité et Architecture des Réseaux (SAR'02)*, 2006.

[57] Romuald Thion and Stéphane Coulondre, "Intégration du contexte spatio-temporel dans le contrôle des accès mobiles basé sur les rôles," 2005.

[58] KHELIFA Nor Eddine, *Intégration du modèle de contrôle d'accès RBAC (Role Based Access control) dans les diagrammes UML (Cas d'Utilisation et Séquence).*, Ph.D. thesis, université d'Oran, 2011.

[59] Aaron Elliott and Scott Knight, "A new paradigm for role-based access control," 2018.

[60] Marc-André Laverdière-Papineau, *Finding Differences in Privilege Protection and their Origin in Role-Based Access Control Implementations*, Ph.D. thesis, École Polytechnique de Montréal, 2018.

[61] Roshan K Thomas and Ravi S Sandhu, "Towards a task-based paradigm for flexible and adaptable access control in distributed applications," in *Proceedings on the 1992-1993 workshop on New security paradigms*. ACM, 1993, pp. 138–142.

[62] Piero Andrea Bonatti Bertino, Elisa and Elena Ferrari, "Trbac : A temporal role-based access control model.," *ACM Transactions on Information and System Security (TISSEC) 4.3 : 191-233.*, 2001.

[63] Gustave KOUALOROH, "Audit et definition de la politique de sécurité du réseau informatique de la first bank," M.S. thesis, Université de Yaoundé I, 2008.

[64] George Coulouris, Jean Dollimore, and Marcus Roberts, "Role and task-based access control in the perdis groupware platform," in *Symposium on Access Control Models and Technologies : Proceedings of the third ACM workshop on Role-based access control*. Citeseer, 1998, vol. 22, pp. 115–121.

[65] Sejong Oh and Seog Park, "Task–role-based access control model," *Information systems*, vol. 28, no. 6, pp. 533–562, 2003.

[66] Ji-Bo Deng and Fan Hong, "Task-based access control model [j]," *Journal of software*, vol. 1, no. 011, 2003.

[67] F. Jian-Biao and Y. Chang-Chun, "A mix of role and task-based access control model research," in *2010 Third International Conference on Information and Computing*, June 2010, vol. 3, pp. 66–69.

[68] K Roshan and R Thomas, "Tmac : A primitive for applying rbac in collaborative environment," in *2nd ACM Workshop on RBAC, Fairfax, Virginia, USA*, 1997, pp. 6–7.

[69] Christos K Georgiadis, Ioannis Mavridis, George Pangalos, and Roshan K Thomas, "Flexible team-based access control using contexts," in *Proceedings of the sixth ACM symposium on Access control models and technologies*. ACM, 2001, pp. 21–27.

[70] Weigang Wang, "Team-and-role-based organizational context and access control for cooperative hypermedia environments," in *Hypertext*. Citeseer, 1999, vol. 99, pp. 37–46.

[71] Christos K Georgiadis, Ioannis K Mavridis, Georgia Nikolakopoulou, and George I Pangalos, "Implementing context and team based access control in healthcare intranets," *Medical informatics and the internet in medicine*, vol. 27, no. 3, pp. 185–201, 2002.

[72] W. Zhou and C. Meinel, "Team and task based rbac access control model," in *2007 Latin American Network Operations and Management Symposium*, Sep. 2007, pp. 84–94.

[73] Eric Yuan and Jin Tong, "Attributed based access control (abac) for web services," in *IEEE International Conference on Web Services (ICWS'05). IEEE*, 2005.

[74] Mahamat Ahmat Abakar, *Etude et mise en oeuvre 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*, Ph.D. thesis, Saint-Etienne, 2012.

[75] Recommandation UIT-T X.1550, "Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents," 2017.

[76] Omar Abahmane, *Contrôle de flux d'informations basé sur la granularité*, Ph.D. thesis, Université du Québec en Outaouais, 2015.

[77] Romain Laborde and Thierry Desprats, "Gestion de conditions stables dans xacml : intérêt d'une approche par notification," *Gestion de REseaux et de Services (GRES)*, pp. 161–168, 2008.

[78] Romain Laborde, *Contributions à la gestion de la sécurité des infrastructures virtuelles*, Ph.D. thesis, Université Toulouse 3 Paul Sabatier, 2016.

[79] Amine Baïna, *Controle d'accès pour les grandes infrastructures critiques. Application au réseau d'énergie électrique.*, Ph.D. thesis, INSA de Toulouse, 2009.

[80] Frédéric Cuppens and Alexandre Miège, "Administration model for orbac," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer, 2003, pp. 754–768.

[81] Frédéric Cuppens and Alexandre Miege, "Or-bac organization based access control," *Distribution des données à grande Echelle (DRUIDE), Le Croisic, France*, 2004.

[82] Worachet Uttha, *Etude des politiques de sécurité pour les applications distribuées : le problème des dépendances transitives : modélisation, vérification et mise en oeuvre*, Ph.D. thesis, Aix-Marseille, 2016.

[83] Sabrina De Capitani Di Vimercati and Pierangela Samarati, "Access control in federated systems.," in *NSPW*, 1996, vol. 96, pp. 87–99.

[84] A Abou El Kalam and Yves Deswarte, "Multi-orbac : un modèle de contrôle d'accès pour les systèmes multiorganisationnels," *3rd Security of Information Systems (SSI), Seignosse-Landes, France*, pp. 6–9, 2006.

[85] Bassem Nasser, *Organisation virtuelle : gestion de politique de contrôle d'accès inter domaines*, Ph.D. thesis, Toulouse 3, 2006.

[86] Frédéric Cuppens, Nora Cuppens-Boulahia, and Céline Coma, "O2o : Virtual private organizations to manage security policy interoperability," in *International Conference on Information Systems Security*. Springer, 2006, pp. 101–115.

[87] Indrakshi Ray, Indrajit Ray, and Sudip Chakraborty, "An interoperable context sensitive model of trust," *Journal of Intelligent Information Systems*, vol. 32, no. 1, pp. 75–104, 2009.

[88] Sourour Jemili, *Analyse de risque dans les systèmes de contrôle d'accès*, Ph.D. thesis, Université du Québec en Outaouais, 2013.

[89] Manachai Toahchoodee, Ramadan Abdunabi, Indrakshi Ray, and Indrajit Ray, "A trust-based access control model for pervasive computing applications," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2009, pp. 307–314.

[90] Nathan Dimmock, "How much is" enough"? risk in trust-based access control," in *WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises, 2003.* IEEE, 2003, pp. 281–282.

[91] Anour F Dafa-Alla, Eun Hee Kim, Keun Ho Ryu, and Yong Jun Heo, "Pr-bac : An extended role based access control for privacy preserving data mining," in *Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05)*. IEEE, 2005, pp. 68–73.

[92] Alessandra Toninelli, Rebecca Montanari, Lalana Kagal, and Ora Lassila, "A semantic context-aware access control framework for secure collaborations in pervasive computing environments," in *International semantic web conference*. Springer, 2006, pp. 473–486.

[93] Tim Finin, Anupam Joshi, Lalana Kagal, Jianwei Niu, Ravi Sandhu, William Winsborough, and Bhavani Thuraisingham, "R owl bac : representing role based access control in owl," in *Proceedings of the 13th ACM symposium on Access control models and technologies*. ACM, 2008, pp. 73–82.

[94] Céline Coma, *Interopérabilité et cohérence de politiques de sécurité pour les réseaux auto-organisants*, Ph.D. thesis, Télécom Bretagne, 2009.

[95] Ali Noorollahi Ravari, Morteza Amini, and Rasool Jalili, "A temporal semantic-based access control model," in *Computer Society of Iran Computer Conference*. Springer, 2008, pp. 559–568.

[96] Andrea Omicini, Alessandro Ricci, and Mirko Viroli, "Rbac for organisation and security in an agent coordination infrastructure," *Electronic Notes in Theoretical Computer Science*, vol. 128, no. 5, pp. 65–85, 2005.

[97] Tae-Hum Lim and Sang-Uk Shin, "Intelligent access control mechanism for ubiquitous applications," in *6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)*. IEEE, 2007, pp. 955–960.

[98] Aymen Kamoun, *Adaptation d'architectures logicielles de contrôle d'accès dans les environnements collaboratifs ubiquitaires*, Ph.D. thesis, Université Toulouse 1 Capitole, 2014.

[99] Belaidi Asma Abderahim Mohamed El Amine, "Vers l'implémentation d'un modèle de contrôle d'accès pour les systèmes d'informations en santé," in *International Conference on Cryptography and its Applications ICCA'16, U.S.T.O university, Oran, Algeria*, 2016.

[100] Belaidi Asma Abderrahim Mohammed El Amine, "Vers l'implémentation d'un modèle de contrôle d'accès pour les systèmes d'informations en santé," in *Journée Doctorale de Génie Biomédical, Université de Tlemcen, Algérie*, 2016.

[101] Belaidi Asma Abderrahim Mohammed El Amine, "Le contrôle d'accès du dossier médical informatisé, de la modélisation à l'implémentation (cas d'une organisation de santé algérienne)," in *Journée Doctorale en Génie Biomédical, Université de Tlemcen, Algérie*, 2018.

[102] Belaidi Asma Abderrahim Mohammed El Amine, "Vers une modélisation et implémentation de la sécurité du dossier médical informatisé," in *Colloque sur l'Optimisation et les Systèmes d'Information COSI'2018, Oran (Algérie)*, 2018.

[103] Matthieu Billet Nicolas Morisset Thomas Kolovratek, Quentin Gilmant, "Les objets connectés médicaux," 2015.

[104] Belaidi Asma Abderrahim Mohammed El Amine, "Access control to the electronic health records : A case study of an algerian health organization," *Int. J. Medical Engineering and Informatics*, 2019.

[105] Fabien Autrel, Frédéric Cuppens, N Cuppens-Boulahia, and Celine Coma, "Motorbac 2 : a security policy tool," in *3rd Conference on Security in Network Architectures and Information Systems (SAR-SSI 2008), Loctudy, France*, 2008, pp. 273–288.

[106] Khalid Bouriche, *Gestion de l'incertitude et codage des politiques de sécurité dans les systèmes de contrôle d'accès*, Ph.D. thesis, Artois, 2013.

[107] Natalya Fridman Noy, Ray W Fergerson, and Mark A Musen, "The knowledge model of protege-2000 : Combining interoperability and flexibility," in *International Conference on Knowledge Engineering and Knowledge Management*. Springer, 2000, pp. 17–32.

[108] M.NACER MA.HANINI, "Conception et réalisation d'une interface graphique pour visualiser une ontologie," M.S. thesis, Université de Larbi Tébessi –Tébessa-, Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie, Département : Département Mathématiques et Informatique, 2016.

Annexes

Annexe A : DTD du DM

< !DOCTYPE DMP [

< !ELEMENT DM (Donnees-administratives,donnees-de-mesures,donnees-concourantes-a-la-coordination-qualite-continuite-des-soins-et-prevention,espace-d-expression-du-titulaire)>

< !ELEMENT Donnees-administratives (Identification, rencontre, personnes-de-confiance, garde-malade)>

< !ELEMENT donnees-de-mesures (Poids, taille, sommeil, force, mouvement, mouvemen-fœtaux, indice-de-masse-corporelle, potentiel-hydrogene, temperature, frequence-cardiaque, frequence-respiratoire, pression-arterielle, taux-d-insuline, micro-circulation-sanguine, detection-de-chute, EEG, ECG, EMG)>

< !ELEMENT donnees-concourantes-a-la-coordination-qualite-continuite-des-soins-et-prevention (Donnees-medicales-generales, donnees-de-soins, donnees-de-prevention, donnees-de-la-chirurgie,compte-rendu-d-accouchement, resume-de-sortie)>

< !ELEMENT espace-d-expression-du-titulaire (Le-consentement-du-patient)>

< !ELEMENT Identification (Identifiant, nom, prenom, date-de-naissance, sexe, profession, prenom-pere, nom-mere, prenom-mere, nationalite, situation-familiale, nom-epoux, groupage, telephone, adresse, e-mail, numero-de-securite-sociale)>

< !ELEMENT rencontre(Nom-medecin, prenom-medecin, specialite-du-medecin, date-de-rencontre, interrogatoire, lettre-d-admission, motifs-d-hospitalisation, decisions)>

< !ELEMENT personnes-de-confiance (Nom, prenom, date-de-naissance, lien-de-parente, telephone, adresse, e-mail)>

< !ELEMENT garde-malade (Nom, prenom, date-de-naissance, lien-de-parente, telephone, adresse, e-mail)>

< !ELEMENT Donnees-medicales-generales (Antecedents, historiques-des-consultations, allergies, intolerances-reconnues, protheses, appareillage)>

< !ELEMENT donnees-de-soins (Examens-biologiques, examens-d-imageries, pathologies-en-cours, traitements-prescrits-et-administres, soins-reçus)>

< !ELEMENT donnees-de-prevention (Facteurs-de-risque-individuels, traitements-preventifs-prescrits, calendrier-des-vaccinations)>

< !ELEMENT donnees-de-la-chirurgie (Design-de-la-chirurgie, heure-de -la chirurgie, nom-chirurgien, prenom-chirurgien, nom-anesthesiste, prenom-anesthésiste, protocole-de-la chirurgie, compte-rendu)>

< !ELEMENT compte-rendu-d-accouchement (heure-de-l'accouchement, nom-sage-femme, prenom-sage-femme, nom-gynecologue, prenom-gynécologue, nom-

anesthésiste, prenom-anesthésiste)>
<!ELEMENT resume-de-sortie (mode-de-sortie, certificat-de-sortie, ordonnances, rendez-vous)>
<!ELEMENT Examens-biologiques(categories, date, resultats, comptes-rendus, URL)>
<!ELEMENT examens-d-imageries(categories, date, resultats, comptes-rendus, URL)>
<!ELEMENT rendez-vous (id-RDV, date-RDV, heure-RDV, id-service)>
<!ELEMENT ordonnances (id-ordo,id-medic, mode-application, posologie, nbr-fois, periode)>
<!ELEMENT certificat-de-sortie (id-certif, id-hosp, type-certif, motif-hosp, cause-certif, date-certif)>
<!ELEMENT Identifiant (#PCDATA)>
<!ELEMENT nom (#PCDATA)>
<!ELEMENT prenom (#PCDATA)>
<!ELEMENT date-de-naissance (#PCDATA)>
<!ELEMENT sexe (Masculin|Feminin)>
<!ELEMENT profession (#PCDATA)>
<!ELEMENT prenom-pere (#PCDATA)>
<!ELEMENT nom-mere (#PCDATA)>
<!ELEMENT prenom-mere (#PCDATA)>
<!ELEMENT nationalite (#PCDATA)>
<!ELEMENT situation-familiale (celibataire| marie| divorce | veuf)>
<!ELEMENT nom-epoux (#PCDATA)>
<!ELEMENT groupage (#PCDATA)>
<!ELEMENT telephone (#PCDATA)>
<!ELEMENT adresse (#PCDATA)>
<!ELEMENT e-mail (#PCDATA)>
<!ELEMENT numero-de-securite-sociale (#PCDATA)>
<!ELEMENT Nom-medecin (#PCDATA)>
<!ELEMENT prenom-medecin(#PCDATA)>
<!ELEMENT specialite-du-medecin(#PCDATA)>
<!ELEMENT date-de-rencontre (#PCDATA)>
<!ELEMENT interrogatoire (#PCDATA)>
<!ELEMENT lettre-d-admission (#PCDATA)>
<!ELEMENT motifs-d-hospitalisation (#PCDATA)>
<!ELEMENT decisions (#PCDATA)>
<!ELEMENT nom (#PCDATA)>
<!ELEMENT prenom (#PCDATA)>
<!ELEMENT date-de-naissance (#PCDATA)>
<!ELEMENT lien-de-parente (#PCDATA)>
<!ELEMENT telephone (#PCDATA)>
<!ELEMENT adresse (#PCDATA)>
<!ELEMENT e-mail (#PCDATA)>
<!ELEMENT Poids (#PCDATA)>
<!ELEMENT taille (#PCDATA)>
<!ELEMENT sommeil (#PCDATA)>

<!ELEMENT force (#PCDATA)>
<!ELEMENT mouvement(#PCDATA)>
<!ELEMENT mouvemen-fœtaux (#PCDATA)>
<!ELEMENT indice-de-masse-corporelle (#PCDATA)>
<!ELEMENT potentiel-hydrogene (#PCDATA)>
<!ELEMENT temperature (#PCDATA)>
<!ELEMENT frequence-cardiaque (#PCDATA)>
<!ELEMENT frequence-respiratoire (#PCDATA)>
<!ELEMENT pression-arterielle (#PCDATA)>
<!ELEMENT taux-d-insuline(#PCDATA)>
<!ELEMENT micro-circulation-sanguine(#PCDATA)>
<!ELEMENT detection-de-chute(#PCDATA)>
<!ELEMENT EEG (#PCDATA)>
<!ELEMENT ECG (#PCDATA)>
<!ELEMENT EMG (#PCDATA)>
<!ELEMENT Antecedents (Personnel | Familial)>
<!ELEMENT historiques-des-consultations (#PCDATA)>
<!ELEMENT allergies (#PCDATA)>
<!ELEMENT intolerances-reconnues (#PCDATA)>
<!ELEMENT protheses(#PCDATA)>
<!ELEMENT appareillage (#PCDATA)>
<!ELEMENT categories (#PCDATA)>
<!ELEMENT date (#PCDATA)>
<!ELEMENT resultats (#PCDATA)>
<!ELEMENT comptes-rendus (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT pathologies-en-cours (#PCDATA)>
<!ELEMENT traitements-prescrits-et-administres(#PCDATA)>
<!ELEMENT soins-reçus(#PCDATA)>
<!ELEMENT Facteurs-de-risque-individuels(#PCDATA)>
<!ELEMENT traitements-preventifs-prescrits(#PCDATA)>
<!ELEMENT calendrier-des-vaccinations(#PCDATA)>
<!ELEMENT Design-de-la-chirurgie(#PCDATA)>
<!ELEMENT heure-de -la chirurgie(#PCDATA)>
<!ELEMENT prenom-chirurgien(#PCDATA)>
<!ELEMENT nom-anesthesiste (#PCDATA)>
<!ELEMENT prenom-anesthésiste (#PCDATA)>
<!ELEMENT protocole-de-la chirurgie (#PCDATA)>
<!ELEMENT compte-rendu (#PCDATA)>
<!ELEMENT heure-de-l'accouchement(#PCDATA)>
<!ELEMENT nom-sage-femme(#PCDATA)>
<!ELEMENT prenom-sage-femme(#PCDATA)>
<!ELEMENT nom-gynecologue (#PCDATA)>
<!ELEMENT prenom-gynécologue (#PCDATA)>
<!ELEMENT protocole-de-la chirurgie (#PCDATA)>
<!ELEMENT mode-de-sortie(#PCDATA)>
<!ELEMENT id-RDV (#PCDATA)>

<!ELEMENT date-RDV (#PCDATA)>
<!ELEMENT heure-RDV (#PCDATA)>
<!ELEMENT id-service (#PCDATA)>
<!ELEMENT id-ordo (#PCDATA)>
<!ELEMENT id-medic (#PCDATA)>
<!ELEMENT mode-application (#PCDATA)>
<!ATTLIST mode-application quantite CDATA #REQUIRED>
<!ELEMENT posologie (#PCDATA)>
<!ELEMENT nbr-de-fois (#PCDATA)>
<!ATTLIST nbr-de-fois par CDATA #REQUIRED>
<!ELEMENT periode (#PCDATA)>
<!ELEMENT id-certif (#PCDATA)>
<!ELEMENT type-certif (#PCDATA)>
<!ELEMENT cause-certif (#PCDATA)>
<!ELEMENT date-certif (#PCDATA)>
<!ELEMENT Le-consentement-du-patient (#PCDATA)>
]>

Annexe B : Bulletin d'admission

CENTRE HOSPITALO-UNIVERSITAIRE
TLEMCEN

– BULLETIN D'ADMISSION –

IDENTIFICATION DU PATIENT

N° D'ADMISSION 16/00/009138 | CHIRURGIE GENERALE | 30/10/2016

Qualité du patient vis à vis de l'assurance :

AGE : 36 Ans

Nom : LAISSOUF Prénoms : BADR EDDINE Sexe : MASCULIN

Date de Naissance : 04/10/1980 Lieu de Naissance : TLEMCEN W. TLEMCEN

Fil(le)s de : LAHCEN Et de : MEDIANI MIMOUNA

Nationalité : Algerienne Profession : Indépendant

Situation familiale : Marié (e) Epoux(se) de : KHADRAOUI KHADIDJA

Adresse de résidence : N°15 LA CIPA TLM TLEMCEN W. TLEMCEN

Nom et Prénoms de la personne à contacter : SON EPOUSE N° de tél :( ) . .

Adresse de contact : DR/BENSEHANE

IDENTIFICATION DE L'ASSURE

IMMATRICULATION | N° DE PRISE EN CHARGE S.S | DATE

Nom : Prénoms :

Date De Naissance :

Caisse D'affiliation :

Employeur :

HOSPITALISATION

Service d'hospitalisation : CHIRURGIE GENERALE Date d'entrée : 30/10/2016 Heure : 12 h 29

Nom Unité : CHIRURGIE B N° de lit : 0 Medecin Traitant : DR/BENSEHANE

Mode d'entrée : ADMISSION NORMALE N° Prise en charge (Santé) :

Etablissement d'origine :

ACCIDENT

Type d'accident :

Date de l'évènement : Heure : h Lieu :

Patient Transporté par : Références :

Autorité chargée de l'enquête :

Figure-Bulletin d'admission

Annexe C : Fiche navette

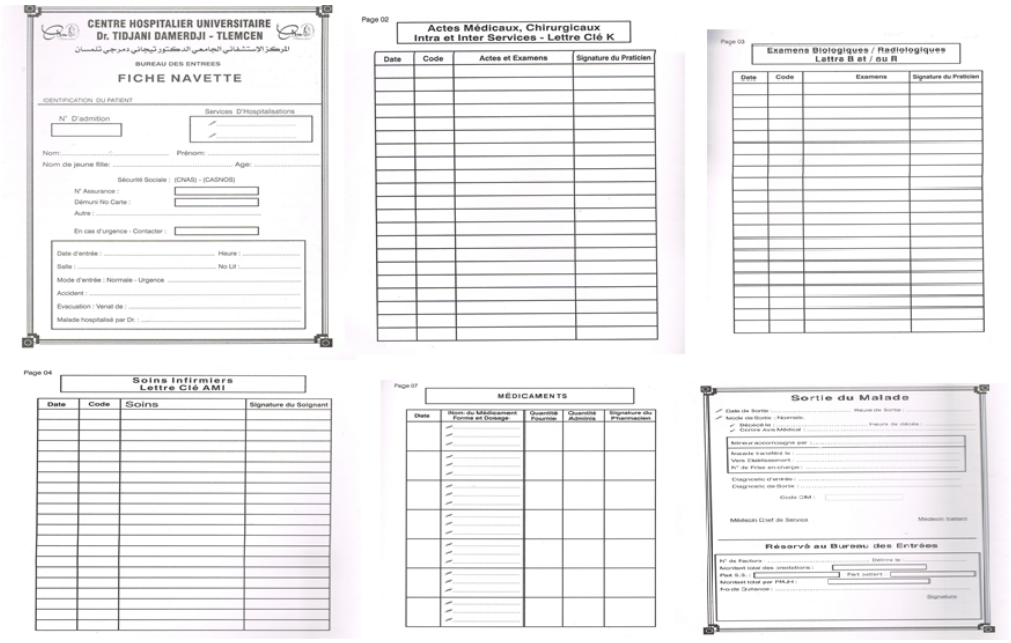


Figure-Fiche navette pour une hospitalisation

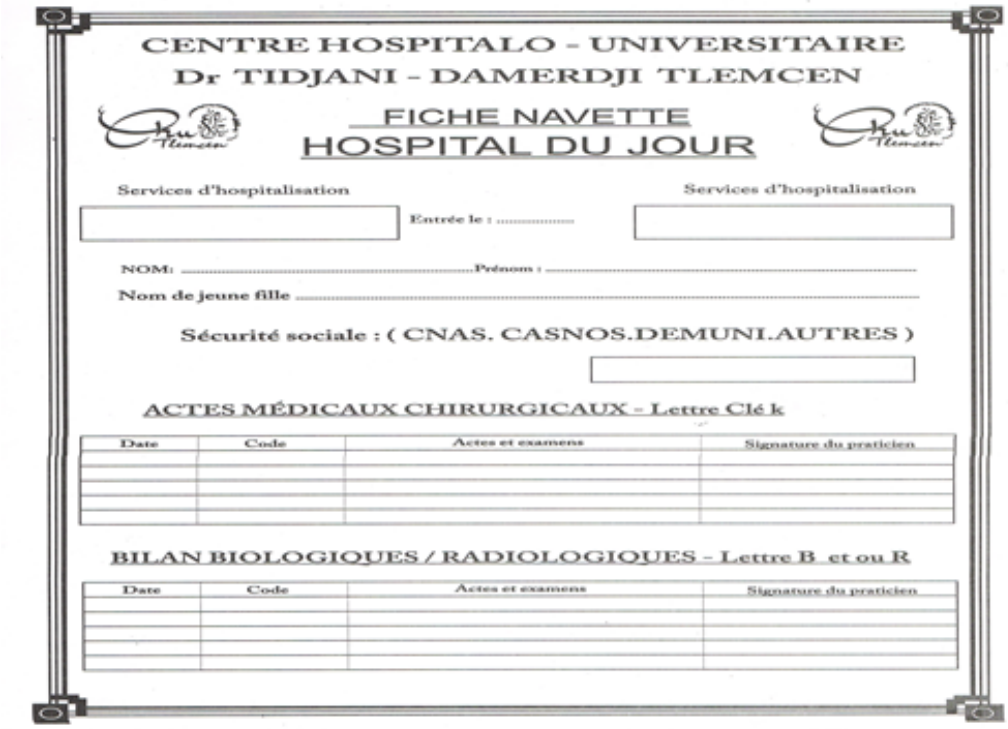
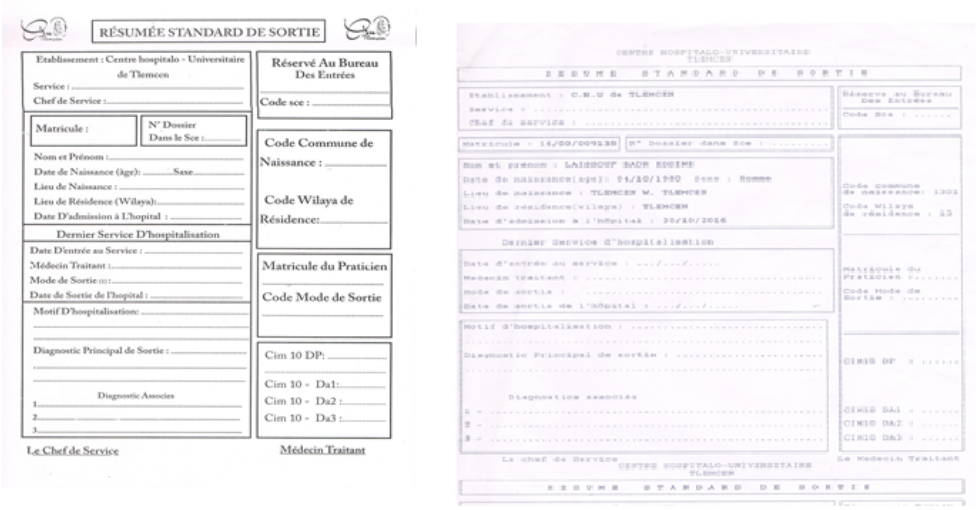


Figure-Fiche navette pour un hôpital du jour

Annexe D : Résumé standard de sortie



RÉSUMÉE STANDARD DE SORTIE

Etablissement : Centre hospitalo - Universitaire de Tlemcen
Service :
Chef de Service :

Réservé Au Bureau Des Entrées
Code sce :

Matricule :
N° Dossier Dans le Sce :

Nom et Prénom :
Date de Naissance (âge): Sexe
Lieu de Naissance :
Lieu de Résidence (Wilaya):
Date D'admission à L'hopital :

Code Commune de Naissance :
Code Wilaya de Résidence:

Dernier Service D'hospitalisation
Date D'entrée au Service :
Médecin Traitant :
Mode de Sortie :
Date de Sortie de l'hopital :

Matricule du Praticien
Code Mode de Sortie

Motif D'hospitalisation:
Diagnostic Principal de Sortie :
Diagnostic Associés
1
2
3

Cim 10 DP:
Cim 10 - Da1:
Cim 10 - Da2 :
Cim 10 - Da3 :

Le Chef de Service
Médecin Traitant

Figure-Résumé standard de sortie

Annexe E : Logiciel PATIENT

Annexe E.1 : Transfert inter-service

Numéro d'entrée :

Nom : x prénom : y

Entré le : 23/10/2016

Service d'origine : gastrologie

Code de service	Date évacuation	Heure évacuation	Code salle	Num lit	Désignation unité

Figure-Transfert inter-service

Annexe E.2 : Renseignement

N entrées	Nom prénom	Epoux	Date de sortie	Service
0015/84	X y	c	22/10/2016	neurologie

Figure-Renseignement

Annexe E.3 : Informations de sortie

Numéro d'entrée : préposé:

Nom et prénom : Age :

Date d'entrée :

Service / unité d'origine :

Service /unité de sortie :

Date de sortie:

Mode de sortie

- Normale
- Par décès
- Evacuation
- Evasion
- Contre avis médical
- Transfert étranger

Figure-Informations de sortie

Annexe E.4 : Décomptes

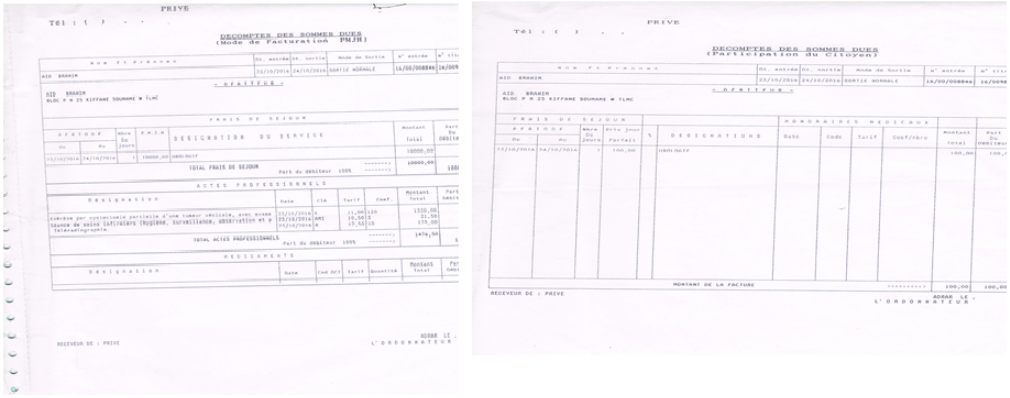
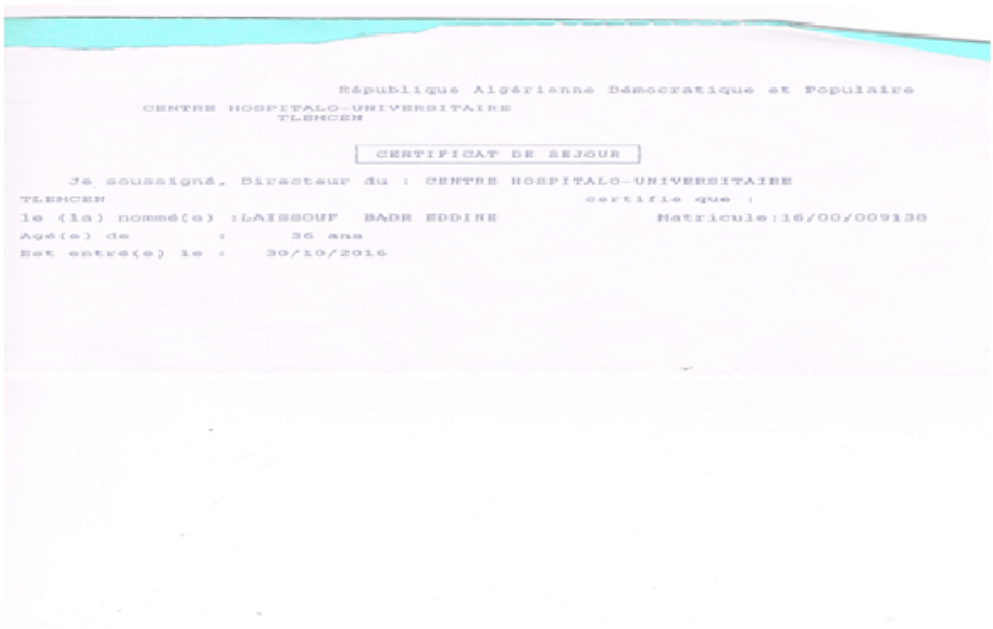


Figure-Décomptes

Annexe E.5 : Certificat de séjour



République Algérienne Démocratique et Populaire
CENTRE HOSPITALO-UNIVERSITAIRE
TLEMCEN

CERTIFICAT DE SEJOUR

Je soussigné, Directeur du : CENTRE HOSPITALO-UNIVERSITAIRE
TLEMCEN certifie que :
le (la) nommé(e) :LAISSOUF BADR EDDINE Matricule:16/00/009130
Agé(e) de : 36 ans
Est entré(e) le : 30/10/2016

Figure-Certificat de séjour

Annexe E.6 : Données nationales

✓Services

Libellé famille	Code service	Désignation du service
Service de médecine	109	Urgence médicales Médecine interne
Service de chirurgie	201	Urgence chirurgicales ORL
Laboratoires	301	Laboratoire central

✓Etablissement nationale

Code établissement	Désignation établissement
21050000310	C.H.U de Batna
	C.H.U Blida

Figure-Données nationales

Annexe E.7 :Maintenance

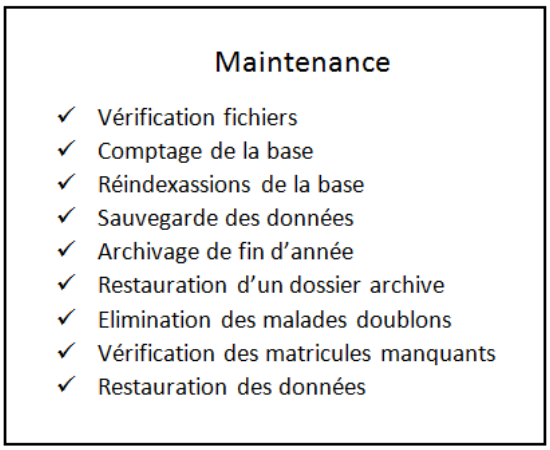


Figure-Maintenance

Annexe E.8 :Mise à jour des utilisateurs dans logiciel « PATIENT »

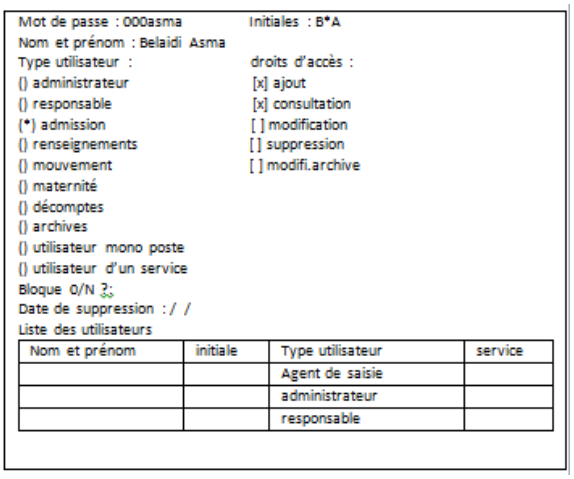


Figure-Mise à jour des utilisateurs logiciel « PATIENT »

Annexe F : Politique de CA

L'annexe F présente notre politique de CA avec catégorisation de rôles sous forme d'un tableau. Ce tableau est divisé en 18 lignes qui représentent les différents rôles de notre modèle et en 16 colonnes qui représentent les différentes vues dégagées, l'intersection des lignes et colonnes forme les différentes permissions et interdictions accordées selon les contextes. Puisque ce tableau est de taille grande donc nous avons divisé ce dernier en quatre tableaux.

	Identification	Rencontre	Personne de confiance	Garde Malade
Cadre Médical	consulter transférer (UT3S3)	ne pas supprimer (UT3S3)	consulter (UT3S3)	consulter (UT3S3)
Résident	consulter (UT3S1)	ne pas supprimer (UT3S1)	consulter (UT3S1)	consulter (UT3S1)
Généraliste	consulter (UT3S1)	ne pas supprimer (UT3S1)	consulter (UT3S1)	consulter (UT3S1)
L'interne	consulter (UT1S1)	consulter (UT1S1)	-	-
L'externe	consulter (UT1S1)	consulter (UT1S1)	-	-
Cadre paramédical	consulter (UT1S1)	consulter (UT1S1)	-	-
Laborantin	consulter (UT1S1)	-	-	-
Manipulateur RX	consulter (UT1S1)	-	-	-
Anesthésiste	consulter (UT1S1)	consulter (UT1S1)	-	-
Kinésithérapie	consulter (UT1S1)	consulter (UT1S1)	-	-
Sage-femme	consulter (UT3S1)	ne pas supprimer (UT3S1)	consulter (UT3S1)	consulter (UT3S1)
Psychologue	consulter (UT1S1)	consulter (UT1S1)	-	-
Secrétaire médicale	ne pas supprimer (UT1S1)	-	ne pas supprimer (UT1S1)	ne pas supprimer (UT1S1)
Pharmacien	consulter (UT1S1)	-	-	-
Patient	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)
OCC	consulter (T3S3)	-	-	-
OCI	consulter (UT3S3)	-	-	-

Table-Répartition des droits

	Données OCC	Données OCI	Données Médicales Générales	Données de Soins
Cadre Médical	consulter transférer (UT3S3)	consulter transférer (UT3S3)	ne pas supprimer (UT3S3)	ne pas supprimer (UT3S3)
Résident	consulter transférer (UT3S1)	consulter transférer (UT3S1)	ne pas supprimer (UT3S1)	ne pas supprimer (UT3S1)
Généraliste	consulter transférer (UT3S1)	consulter transférer (UT3S1)	ne pas supprimer (UT3S1)	ne pas supprimer (UT3S1)
L'interne	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)
L'externe	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)
Cadre paramédical	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	ne pas supprimer (US1T3)
Laborantin	-	-	-	-
Manipulateur RX	-	-	-	-
Anesthésiste	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)
Kinésithérapie	consulter (UT1S1)	consulter (UT1S1)	ne pas supprimer (UT1S1)	-
Sage-femme	consulter (UT3S1)	consulter (UT3S1)	ne pas supprimer (UT3S1)	ne pas supprimer (UT3S1)
Psychologue	consulter (UT1S1)	consulter (UT1S1)	ne pas supprimer (UT1S1)	ne pas supprimer (UT1S1)
Secrétaire médicale	-	-	-	-
Pharmacien	-	-	-	ne pas supprimer (UT1S1)
Patient	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)
OCC	ne pas supprimer ne pas transférer (T3S3)	-	-	-
OCI	-	ne pas supprimer ne pas transférer (UT3S3)	-	-

Table-Répartition des droits

	Examens Biologiques	Examens d'Imagerie	Données de Prévention	Données de la Chirurgie
Cadre Médical	ne pas supprimer (UT3S3)	ne pas supprimer (UT3S3)	ne pas supprimer (UT3S3)	ne pas supprimer (UT3S3)
Résident	consulter transférer (UT3S1)	consulter transférer (UT3S1)	ne pas supprimer (UT3S1)	ne pas supprimer (UT3S1)
Généraliste	consulter transférer (UT3S1)	consulter transférer (UT3S1)	ne pas supprimer (UT3S1)	consulter (UT3S1)
L'interne	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)
L'externe	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	-
Cadre paramédicale	-	-	ne pas supprimer (US1T3)	-
Laborantin	ne pas supprimer (UT1S1)	-	-	-
Manipulateur RX	-	ne pas supprimer (UT1S1)	-	-
Anesthésiste	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	ne pas supprimer (UT1S1)
Kinésithérapie	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)	consulter (UT1S1)
Sage-femme	consulter (UT3S1)	consulter (UT3S1)	ne pas supprimer (UT3S1)	-
Psychologue	-	-	consulter (UT1S1)	-
Secrétaire médicale	-	-	-	-
Pharmacien	-	-	-	-
Patient	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)	consulter transférer(US3T3)
OCC	-	-	-	-
OCI	-	-	-	-

Table-Répartition des droits

	Compte-rendu d'accouchement	Résumé de Sortie	Don d'Organes
Cadre Médical	ne pas supprimer (UT3S3)	ne pas supprimer (UT3S3)	consulter (UT3S3)
Résident	ne pas supprimer (UT3S1)	ne pas supprimer (UT3S1)	-
Généraliste	consulter (UT3S1)	ne pas supprimer (UT3S1)	-
L'interne	consulter (UT1S1)	consulter (UT1S1)	-
L'externe	-	-	-
Cadre paramédicale	-	consulter (US1T3)	-
Laborantin	-	-	-
Manipulateur RX	-	-	-
Anesthésiste	ne pas supprimer (UT1S1)	consulter (UT1S1)	-
Kinésithérapie	-	ne pas supprimer (UT1S1)	-
Sage-femme	ne pas supprimer (UT3S1)	consulter (UT3S1)	-
Psychologue	-	ne pas supprimer (UT1S1)	-
Secrétaire médicale	-	ne pas supprimer (UT1S1)	ne pas supprimer (UT1S1)
Pharmacien	-	-	-
Patient	consulter transférer(US3T3)	consulter transférer(US3T3)	ne pas supprime(US3T3)
OCC	-	-	-
OCI	-	-	-

Table-Répartition des droits

Annexe G : Politique de CA avec MotOrBAC

L'annexe G représente une partie en XML de notre modèle de CA exporté à partir de l'outil MotOrBAC.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<XmlOrbacPolicy>
<attributes>
<name>copy of modelisation</name>
<creationDate>2019.04.16 19 :02 :13</creationDate>
<modificationDate>2019.04.16 19 :02 :13</modificationDate>
<version>1.0</version>
<information/>
</attributes>
...
</organization>
<organization name="EHS"/>
<organization name="Organisation de sante">
<role name="hematologiste"/>
<role name="Kinesitherapie"/>
<role name="Objets connectes Intelligents"/>
<role name="Laborantaire"/>
<role name="Objets connectes classiques"/>
<role name="Cadre de sante"/>
....
<activity name="Consulter"/>
<activity name="Transferer"/>
<activity name="Supprimer"/>
<activity name="Ajouter"/>
<activity name="Modifier"/>
....
<view name="Donnees pour objets connectes classiques"/>
<view name="Resume de sortie"/>
<view name="Compte rendu d'accouchement "/>
<view name="donnees de soins"/>
<view name="Personne de confiance"/>
<view name="Identification"/>
...
</organization>
...
</context>
<context evaluated_at_derivation_time="false" name="Us1t3" type="ComposedContext">
<definition organization="EHS">urgence &amp ; s1t3</definition>
<definition organization="Organisation de sante">urgence &amp ; s1t3</definition>
<definition organization="EPSP">urgence &amp ; s1t3</definition>
<definition organization="EPH">urgence &amp ; s1t3</definition>
</context>
....
</object>
<object name="I18A">
<instance_of name="inhibition_class"/>
<attribute name="authority" value="Organisation de sante"/>
```

<attribute name="grantee" value="Generaliste"/>
<attribute name="context" value="Us1t3"/>
<attribute name="privilege" value="Supprimer"/>
<attribute name="target" value="Donnees medicales generales"/>
</object>
....
</object>
<object name="P14">
<instance_of name="license_class"/>
<attribute name="authority" value="Organisation de sante"/>
<attribute name="grantee" value="Residents"/>
<attribute name="context" value="Us1t3"/>
<attribute name="parentLicense" value="null"/>
<attribute name="grantor" value="null"/>
<attribute name="privilege" value="Transferer"/>
<attribute name="target" value="Donnees pour objets connectes classiques"/>
</object>
...
<comments>
<abstract_rules/>
</comments>
</XmlOrbacPolicy>

Annexe H : Politique de CA avec Protégé

L'annexe H représente une partie en XML de notre modèle de CA exporté à partir de l'outil Protégé.

< ?xml version="1.0" ?>
< !DOCTYPE rdf :RDF [
< !ENTITY owl "http ://www.w3.org/2002/07/owl#" >
< !ENTITY xsd "http ://www.w3.org/2001/XMLSchema#" >
< !ENTITY rdfs "http ://www.w3.org/2000/01/rdf-schema#" >
< !ENTITY rdf "http ://www.w3.org/1999/02/22-rdf-syntax-ns#" >
< !ENTITY untitled-ontology-16 "http ://www.semanticweb.org/n&apos ;tic/ontologies
/2019/3/ untitled-ontology-16#" >
]>
<rdf :RDF xmlns="http ://www.semanticweb.org/n&apos ;tic/ontologies/2019/3/
untitled-ontology-20#"
xml :base="http ://www.semanticweb.org/n&apos ;tic/ontologies/2019/3/
untitled-ontology-20"
...
< !–
////////////////////////////////////
Object Properties
////////////////////////////////////
–>

```
    <!– http ://www.semanticweb.org/n&apos ;tic/ontologies/2019/3/untitled-
ontology-16#AgrégationDE –>
    <rdf :Description rdf :about="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#AgrégationDE"/>
    <!– http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#Considère –>
    <rdf :Description rdf :about="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/
    untitled-ontology-16#Considère"/>
    ...
    <!–
    ////////////////////////////////////
    Classes
    ////////////////////////////////////////////
    –>
    <!– http ://www.semanticweb.org/n&apos ;tic/ontologies/2019/3/untitled-
ontology-16#Action –>
    <owl :Class rdf :about="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/
    untitled-ontology-16#Action">
    <rdfs :subClassOf>
    <owl :Restriction>
    <owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/
    untitled-ontology-16#Considère"/>
    <owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/
    untitled-ontology-16#Activités"/>
    </owl :Restriction>
    </rdfs :subClassOf>
    </owl :Class>
    ...
    <!– http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#Interdiction –>
    <owl :Class rdf :about="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#Interdiction">
    <rdfs :subClassOf>
    <owl :Restriction>
    <owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#DE"/>
    <owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
    ontologies/2019/3/untitled-ontology-16#Cadre_Médical"/>
    </owl :Restriction>
    </rdfs :subClassOf>
    <rdfs :subClassOf>
    <owl :Restriction>
    <owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
```

ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Organisation_de_santé"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Rencontre"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#DE"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Supprimer"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#UT3S3"/>
</owl :Restriction>
</rdfs :subClassOf>
</owl :Class>
...
<!– http ://www.semanticweb.org/n&apos ;tic/ontologies/2019/3/
untitled-ontology-16#Permission –>
<owl :Class rdf :about="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Permission">
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#Organisation_de_santé"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/
ontologies/2019/3/untitled-ontology-16#DE"/>

<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#Cadre_Médical"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#DE"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#consulter"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#UT3S3"/>
</owl :Restriction>
</rdfs :subClassOf>
<rdfs :subClassOf>
<owl :Restriction>
<owl :onProperty rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#Dans"/>
<owl :allValuesFrom rdf :resource="http ://www.semanticweb.org/n&apos ;tic/ ontologies/2019/3/untitled-ontology-16#Identification"/>
</owl :Restriction>
</rdfs :subClassOf>
<untitled-ontology-16 :permis>Permission de Cadre_Médical de Consulter dans Identification dans le contexte UT3S3</untitled-ontology-16 :permis>
</owl :Class>
...
< !– Generated by the OWL API (version 3.4.2) http ://owlapi.sourceforge.net –>

Annexe I : Interface graphique du MotOrBAC

L'annexe I représente l'interface graphique du MotOrBAC qui est divisée en six parties :

1. Cet onglet est utilisé pour afficher les politiques chargées avec chaque politique appartient à un onglet.
2. Ce menu est utilisé pour spécifier une politique abstraite qui est composée de :
   * Organisations : pour la création d'une hiérarchie d'organisations.
   * Abstract entities : pour la création d'une hiérarchie de trois entités abstraites : des rôles, des activités et des vues.

- Contexts : : utilisé pour spécifier les contextes.
- Abstract rules : pour spécifier les règles de permissions, interdictions et obligations.
- Conflits : pour afficher les conflits détectés dans la politique et d'aider l'administrateur à les corriger.
- Entity definitions : pour spécifier les définitions des entités que la politique doit respecter.
- Concret policy simulation : pour simuler la politique concrète qui s'applique aux sujets, actions et objets et qui est dérivée d'une politique abstraite.

3. Ce menu est utilisé pour créer, fermer, charger, enregistrer, exporter et mettre à jour une politique de sécurité.
4. Ce menu est utilisé pour spécifier une politique concrète qui est composée de :
   - Sujets : pour la création, la suppression et la modification des sujets.
   - Actions : pour la création, la suppression et la modification des actions.
   - Objets : pour la création, la suppression et la modification des objets.
5. Administration : l'interface inclut une fonction d'administration implémentant le modèle *Ad-OrBAC* pour administrer les politiques Or-BAC. La fonction d'administration est utilisée pour exprimer ou de mettre à jour la politique de sécurité du système d'information AdOrBAC : cette partie contient des boutons pour activer ou désactiver l'évaluation des politiques AdOrBAC et de la gérer.
6. Barre d'état en bas : la barre d'état au bas de l'interface affiche diverses informations : l'utilisateur AdOrBAC connecté, le nombre de conflits abstraits et concrets, le nombre de permissions et d'interdictions.

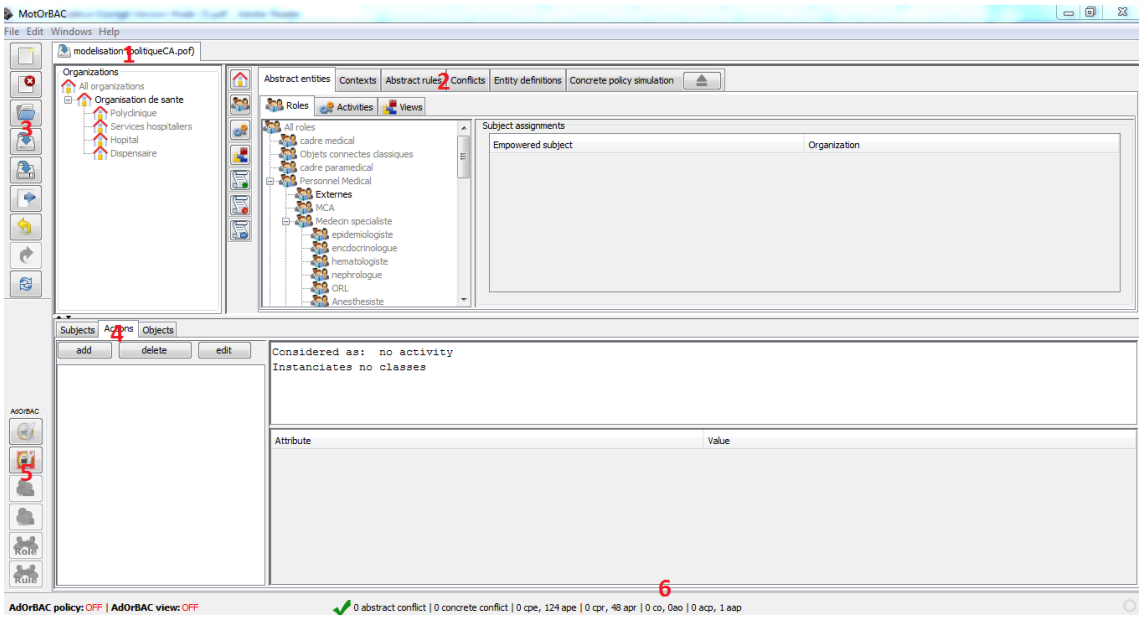


Figure-Interface graphique de *MotOrBAC*