جامعة أبو بكر بلقايد – تلمسان

Université Abou Bakr Belkaïd de Tlemcen

Faculté de Technologie

Département de Génie Biomédical

Laboratoire de Recherche de Génie Biomédical

MEMOIRE DE PROJET DE FIN D'ETUDES

pour obtenir le Diplôme de

MASTER en Génie Biomédical

Spécialité : **Informatique Biomédicale**

présenté par : **HAOUCHE Djahida**

Sécurisation des données de santé informatisées

Soutenu le 14 juin 2015 devant le Jury

M.	Bechar Hassene	Université de Tlemcen	Président
Mme.	Dali Youcef Lamia	Université de Tlemcen	Examinateur
M.	Abderrahim Med El Amine	Université de Tlemcen	Encadreur

Année universitaire 2014-2015

Remerciement

Je tiens en premier lieu à remercier mon directeur de projet monsieur Abderrahim Mohamed El Amine de m'avoir encadré et pour son disponibilité, ces conseils et l'effort qu'il a fourni pour la rédaction de ce mémoire.

Je souhaite adresser mes remerciements les plus sincères à tous les professeurs, intervenants et toutes les personnes qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé mes réflexions et ont accepté à me rencontrer et répondre à mes questions durant mes recherches.

Je remercie vivement les membres du jury, qui ont accepté d'évaluer mon travail. Je remercie Monsieur Bechar Hassene, qui a bien voulu présider le jury, et madame Dali Youcef Lamia d'avoir accepté de se joindre à ce jury comme examinatrice. Je leur suis très reconnaissante pour l'intérêt qu'ils ont porté à mes travaux de recherche.

Je ne peux oublier de remercie toute ma famille pour leur soutien et leurs encouragements continus.

Mes remerciements vont aussi à tous mes amis pour leur aimable présence et tous les bons moments que nous avons partagés ensemble.

Enfin et surtout, un grand merci à « ALLAH » qui m'a toujours aidé.

Table des matières

Résumé

Le contrôle d'accès, ou autorisation ; c'est-à-dire le mécanisme qui définit et impose ce qu'il est permis et interdit ; est un outil technique et organisationnel incontournable lorsqu'on envisage de garantir la sécurité d'un système. Ce domaine de recherche traite multiples problématiques relatives à la notion de droit dans un système.

Face à la diversité et à la taille croissante des systèmes d'information, les modèles historiques de contrôle d'accès ont trouvé leurs limites : trop rigides, insuffisamment sûrs ou difficiles d'administré. Ces limites ont conduit à la proposition du contrôle d'accès à rôles, dont le principe est de donner des permissions en fonction des rôles ; et dans la suite en fonction du contexte dans une organisation.

Dans le cadre de ce mémoire nous nous intéressons particulièrement à l'implémentation du modèle de contrôle d'accès à base d'organisation pour le domaine médicale. L'outil réalisé nous a permis de valider ce modèle et de proposer une nouvelle approche pour son implémentation semi-automatique.

Abstract

The access control or authorization; the mechanism which defines and imposes what is permitted and prohibited; is a major technical and organizational tool when looking to ensure the security of the system. This field of research treats multiple issues relating to the concept of law in system.

Faced to the diversity and the growing size of information systems, the historical Access Control models found their limits: too rigid, insufficiently sure or difficult to administered. These limits have led to the proposition of roles based access control; whose principle is to give permissions based on roles; and in the following depending on context in an organization.

As part of this thesis we are particularly interested to the implementation of an organization based access control for the medical field. The tool realized has allowed us to validate this model and to propose a new approach for it semi-automatic implementation.

ملخص

التحكـم في الوصـول أو الترخيـص؛ أي التقنيـة التي تحدد وتفرض ما هو مسموح وما هو ممنـوع؛ هي أداة تقنيـة وتنظيـمية لا مفر منها عند النظـر إلى ضمـان أمن أنظمة المعلومات حيث يتنـاول هذا المجـال قضايا متعددة تتعلـق بمفهـوم القانون في أنظمة المعلومات.

نظرا للتنـوع والحجم المتزايد لأنظمة المعلومـات لقد وجدت النمـاذج التـاريخية لمراقبة الوصول للمعلومات حدودهـا فهي صـارمة جدا وغير آمنة بمـا فيه الكـفاية أو يصعب إدارتها. هذه القيـود أدت إلى اقتـراح نماذج جديدة للوصـول الى المعلومات بالإعتماد على الأدوارحيث يتم فيها اعطاء الصلاحيـات حسب الدور ووفقا للسيـاق داخل التنظيم.

في هذه المذكرة قمنا بتطوير برمجيات للتحكم في الوصول الى المعلومات خاصة بميدان أنظمة المعلومات الطبية مستندين على النموذج الذي يعتمد على الأدوار. البرمجيات المطورة سمحت لنا بالتحقق من صحـة النمـوذج المعتمد واقتـراح نهجـا جديـدا لتـنـفـيذه الشبـه التلقـائـي.

Introduction Générale

Introduction Générale

Depuis quelques années, les technologies de l'information et de la communication révolutionnent tous les secteurs, qu'ils soient industriels, commerciaux, administratifs ou médicale. Les systèmes de santé adoptent les nouvelles technologies pour la génération, le traitement, le stockage et la consultation de données. Cette adoption vise à assurer une meilleure qualité de service et un fonctionnement plus efficace pour une meilleure consultation.

A l'heure où les échanges d'informations sont de plus en plus nombreux et importants, l'accès à ces informations est devenu de plus en plus complexe. La sécurité des systèmes d'information hospitalière prend une importance particulière, En effet, la confidentialité et la disponibilité sont deux notions qui s'opposent dans les échanges d'informations concernant les patients. L'exploitation erroné par un utilisateur malhonnête d'un système d'information et de communication en santé (SICS) insuffisamment protégé peut rendre possible la divulgation de ces données personnelles, Les erreurs de saisie ou de conception peuvent entraîner des erreurs de diagnostic et de soins. Ces problèmes sont très complexes aux dimensions légales, éthiques et sociales.

Pour résoudre les problèmes de sécurité et protéger l'information du patient stockée de façon électronique, un mécanisme de contrôle d'accès est obligatoire afin d'assurer la confidentialité liée à ces informations et d'assurer le respect de la vie privée et le secret médical.

Problématique :

Un SICS peut être défini comme un grand réseau dédié à la santé. Il relie des utilisateurs multiples ; professionnels de santé, patients, personnes administratives, etc. Il met en jeu des technologies de communication, traitement, télémédecine, paiement, archivage, et manipule des informations hétérogènes : médicales, paramédicales, administratives et financières. Le système d'information ne doit pas provoquer une dégradation de la sécurité avec l'interaction entre les utilisateurs ou face à des personnes malintentionnées qui arrivent à s'infiltrer en exploitant une vulnérabilité du système afin de relevé les informations sensibles auxquelles elles n'ont pas d'accès légale. Ou face à un autre cas fréquent qui concerne les programmes malveillants (les virus, chevaux de Troie, etc.) qui

sont développés pour la nuisance d'un système, voire, modifier ou même collecter ses données pour les réutiliser à des fins malveillantes.

Dans un monde où les attaques de toutes sortes se multiplient, la construction d'applications sécurisées devient une nécessité. Dans de tels systèmes, la moindre faille peut avoir des répercussions très graves.

Donc la question qui se pose, c'est comment partager ces informations tout en protégeant le secret médical ? Et comment couvrir la richesse du dossier médicale par un modèle de contrôle d'accès ? Notre problématique est de développer une approche pour l'intégration automatique d'une politique de sécurité dans une application médicale réelle.

Objectifs du mémoire

L'objectif de la sécurisation des systèmes d'information et de communication est de garantir qu'aucun préjudice ne puisse violer les objectifs de sécurité.

Dans ce mémoire de master on s'intéresse essentiellement aux techniques de contrôle d'accès au dossier médical informatisé. Ce contrôle représente une composante importante de la sécurité du système d'information hospitalier. Le contrôle d'accès consiste à vérifier si un sujet demandant l'accès à un objet possède bien les droits nécessaires pour le faire et il va générer une décision. Cette décision peut être positive pour permettre l'accès à l'objet ou négative pour y refuser l'accès. Ceci permet de minimiser le risque de dommages indésirables et conduit à protéger les informations et les ressources sensibles.

La sécurité et le domaine de la santé

1. Introduction

L'infrastructure informatique au sein de n'importe quel hôpital est un environnement robuste qui nécessite une disponibilité constante ; Malheureusement cette disponibilité est, trop souvent, au détriment de la sécurité de l'information.

L'une des tendances de croissance les plus rapides de la technologie est la connectivité de tous les supports de communication sur un réseau unique homogène. Cette conversation permet à de nombreuses fonctions disparates de se réunir pour incorporer dans les limites d'un seul réseau d'information. L'intégration de ces technologies peut introduit des vulnérabilités dans le réseau d'information de l'hôpital.

Le dossier médical est au cœur du dispositif du réseau, il envisage le partage des données médicales entre tous les acteurs de santé.

Le problème de la sécurité est devenu de plus en plus important dans ce nouveau monde de l'information du patient confidentielle et accessible.

2. Dossier médical informatisé

Le dossier du malade est défini par l'Agence d'Accréditation et d'Evaluation en Santé (ANAES) comme «le support de l'ensemble des informations recueillies concernant la prise en charge du patient et dont les composantes sont le dossier médical, le dossier de soins infirmiers et le dossier administratif » [19].

Le dossier médical informatisé est la mémoire numérique de toutes les informations (Notes, compte rendus, bilans, résultats, prescriptions…) concernant un malade, constamment mises à jour, parce que l'état du malade se modifie, ce dossier permet aux médecins et à d'autres dispensateurs de soins de santé primaires de conserver, récupérer et manipuler électroniquement l'information recueillie lors des consultations des patients. Ainsi que le regroupement et le partage entre les professionnels et les établissements de santé des informations utiles à la coordination et à la continuité des soins.

Il assure la traçabilité de toutes les actions effectuées et permet de suivre et de comprendre le parcours hospitalier du patient. Il est un élément primordial de la qualité des soins

3. Historique du dossier médical

Avant, les observations des soignants étaient une simple prise de notes et d'observations. Courant XIVème siècle, la notion "dossier du patient " a apparu comme un support écrit, il servait à la réunion et la conservation (archivage) des notes du médecin. Autrement dit, il permettait au médecin de rien oublier de l'histoire de son patient.

Egalement, les informations peuvent être partagées avec d'autres médecins, équipes soignantes et/ou la famille.

A la fin du XVIIème siècle apparait « le dossier médical personnel » pour chaque patient. À titre d'exemple Il était utilisé comme un cahier de registre à l'Hôtel-Dieu à Paris. Cependant le contenu était succinct.

La complexité des prises en charges, l'optimisation de la qualité des soins et l'évolution sociétale en termes de droits des personnes hospitalisées ont contribué à la valorisation de dossier médical.

Depuis 1970, les dossiers de soins infirmiers font partie des dossiers médicaux. L'ensemble est devenu un outil de communication et de transmissions des données entre les professionnels de santé et ce quel que soit leurs type d'exercice (secteurs hospitalier et libéral) [20].

En conclusion, le dossier médical comporte des notes prises par les médecins lors des consultations est aujourd'hui un document médico-juridique et administratif.

4. Bénéfice du dossier médical informatisé

La traçabilité du suivi permet une analyse de la qualité des prises en charge. Il est alors un moyen d'améliorer la qualité des soins, ceci dans le but d'une meilleure gestion de la santé de population. De plus, l'accès du patient à son dossier médical permet de lui fournir une information éclairée de son état et de sa prise en charge. Par conséquent l'intérêt est double, pour le professionnel et le patient.

L'informatisation de ce dossier sert a gagner beaucoup de temps car elle fait en quelques secondes des tâches qui autrefois demandaient des heures. Ces taches sont gérées avec précision et sans fatigue.

Le tableau ci-dessous montre certains avantages du dossier informatisé par rapport au dossier papier :

	Traditionnel	informatisé
Stockage et communication des informations	+	+++
Lisibilité du dossier	+	++
Accès à distance	0	++++
Chaînage des épisodes de soins	+	+++
Traitement et aide à la décision	0	++
Suggestions diagnostiques ou thérapeutiques	0	+++
Traitement des données multimédias	0	+++
Recherche clinique, épidémiologique	+	+++
Sécurité de l'information	++	+
confidentialité	+	+

Tableau1 : les possibilités offertes par le dossier papier et le dossier informatisé [25]

Non	peu	moyen	fort	très fort
0	+	++	+++	++++

Le dossier informatisé permet d'avoir des aides à la décision, la plupart des logiciels de dossier destinés au cabinet du médecin libéral intègre des aides à la prescription et à la vérification de l'ordonnance (détection des incompatibilités médicamenteuses). Concernant la sécurité des dossiers, l'informatique présente des avantages par exemple dans la possibilité de vérifier et de tracer les accès, mais une faille dans le système de sécurité peut permettre d'accéder ou de détruire une grande quantité de dossiers en très peu de temps alors que dans le cas de dossier papier, l'accès est limité par un nombre limité de dossiers.

5. Droits du patient sur son dossier médicale

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

- droit au respect de sa vie privée et du secret des informations la concernant.

« Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant. » [21]

Le milieu hospitalier doit respecter deux grands principes : le respect de la vie privée et le secret médical. Un malade hospitalisé peut demander à ce que sa présence ne soit pas diffusée. Cette requête est légitime surtout lorsque la divulgation de l'information peut nuire la population (on peut citer en particulier les toxicomanes, les politiciens, les jeunes mères,...). Il est alors nécessaire de préserver l'identité et le secret de l'admission du patient dans les divers dossiers le concernant.

- Tous les professionnels de santé ont l'obligation de ne divulguer aucune information concernant la santé des patients : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie. » [22]
- Toute personne a accès à l'ensemble des informations concernant sa santé [23]

Tout patient de plus que 14 ans a le droit d'accès à son dossier sauf si le médecin traitant ou designer juge que cela risque de causer un préjudice grave à sa santé

- Dossier d'un patient décédé [24]

Les héritiers d'un patient décédé peuvent consulter son dossier, mais doivent indiquer le motif de leur demande.

Le droit d'accès des héritiers est limité aux informations nécessaires à l'établissement de la cause du décès, à la défense de la mémoire du défunt ou pour faire valoir leur droits.

Conformément à l'article 34 de la loi informatique et libertés modifiée, une société s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.[26]

6. Sécurisation des dossiers patient informatisé

Le DMP (Dossier Médical Personnel) pose de manière forte le problème de la sécurité et de la protection des données personnelles de santé. Censé être un facilitateur de contact entre les médecins, les professionnels de santé et les patients, et il peine encore à se faire un chemin dans le monde médical, en délivrant une information fiable et sécurisée attachée au patient.

La sécurité du dossier médicale informatisé repose sur : [27]

- la mise en œuvre de contrôles a priori :

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

- Le contrôle a posteriori des actions des utilisateurs :

Ce contrôle est fondé sur une traçabilité et une responsabilité totales des actions effectuées par l'ensemble des utilisateurs, et toute personne a une Mauvaise utilisation sera pénalisés.

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

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

Les gestionnaires des dossiers médicaux contrôle l'accès aux dossiers des patients et préserve la confidentialité et l'intégrité des données personnelles contenues dans ces dossiers. Il trace les accès et enregistre toutes les actions d'un patient sur son Dossier Médical Personnel. Toutefois, lorsqu'un utilisateur accède à des données dans un système en ligne, ces données sont aussi temporairement présentes dans la machine utilisée. Si cette machine n'est pas protégée, il peut faire l'objet d'une attaque et héberger un code malveillant capable d'exploiter ces données. Dans ce cas l'accès au système à partir d'un terminal protégé contre les attaques Internet et les codes malveillants est une précaution essentielle de la sécurité. [27]

6.1 Les concepts de sécurité

Dans le monde médical d'aujourd'hui, les technologies jouent un rôle plus important que jamais, il est essentiel pour les organisations médical de protéger leurs actifs, leurs systèmes et leurs réseaux d'information, toute en évitant la perte de l'information.

La sécurité des systèmes d'information assurer les cinq concepts suivant :

6.1.1 La disponibilité

Ce concept permet de maintenir le bon fonctionnement du système en fournissant de l'information aux utilisateurs autorisés aux moments où ils en ont besoin.

6.1.2 L'intégrité

Les informations ne peuvent être modifiées que par les personnes autorisées. Cela signifie que le système informatique doit empêcher toute modification par des utilisateurs non autorisés ou toute modification incorrecte par des utilisateurs autorisés, c'est-à-dire garantir que les données sont bien celles que l'on croit être.

Ce concept permet au d'autre utilisateur de lire l'information mais ils n'ont pas le droit de la modifier.

Une fonction de hashage est utilisée pour contrôler l'intégrité de données, elle associe à une chaine binaire. La figure 1 illustre comment utiliser une fonction de hashage pour vérifier l'intégrité d'un document numérique.

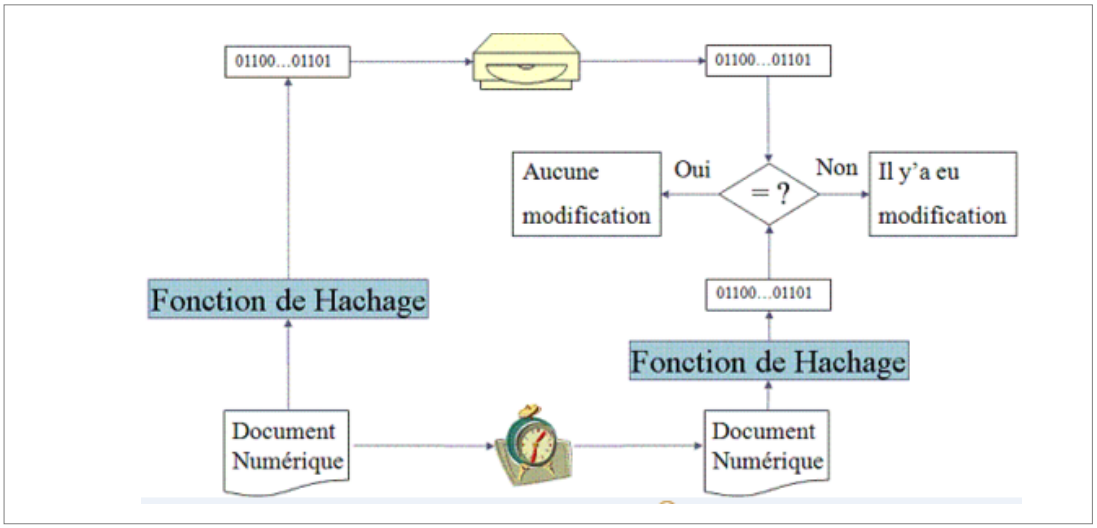

Figure 1 : Intégrité de données [28]

Initialement le code de hashage du document numérique est calculé et stocké dans un endroit sûr. Ultérieurement ce code est recalculé et comparé à celui qui a été stocké.

Si les deux valeurs sont égales alors le document n'a pas été modifié. Sinon, le document a subit une modification.

6.1.3 La confidentialité

Les informations n'appartiennent pas à tout le monde. Seuls ceux qui en ont le droit peuvent y accéder. Ceci signifie que le système informatique doit empêcher les utilisateurs non autorisés de lire une information confidentielle, et empêcher les utilisateurs autorisés de divulguer une information à d'autres utilisateurs sauf l'autorisation.

Exemple de solution c'est le Verrouillage avec clés ou le chiffrement qui est une transformation cryptographique qui transforme un message clair en un message incompréhensible dit chiffré.

Il existe deux types de chiffrement :

6.1.3.1 Les crypto-systèmes symétriques

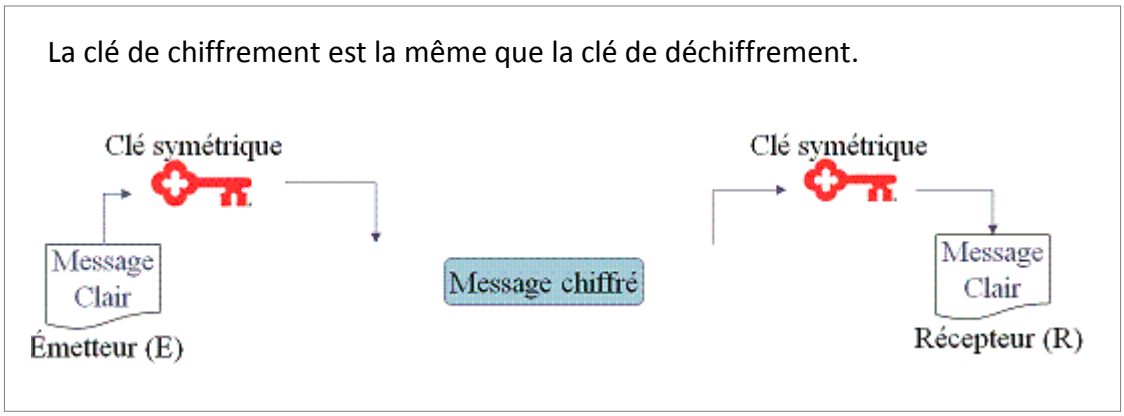

Figure 2(a) : Chiffrement symétrique [28]

L'algorithme est une séquence de transformations sur les données et la clé. Ces systèmes ont l'avantage d'être efficace en termes de temps de calcul, tant pour le chiffrement que pour le déchiffrement, mais on souffre d'un problème de distribution de clés et le secret absolu qui doit l'entourer. Ce type est vu comme un coffre-fort dont la clé est partagée par les utilisateurs autorisés. Si un utilisateur non-autorisé parvient par un moyen quelconque à obtenir cette clé, il pourra déchiffrer tous les données.

6.1.3.2 Les crypto-systèmes asymétriques

La cryptographie asymétrique est aujourd'hui indissociable de l'utilisation des réseaux ouverts, Le principe du chiffrement est illustré dans la figure 2(b). Chaque personne dispose d'une paire de clé :

- Clé publique : publiée dans des annuaires publics. n'importe qui peut récupérer cette clé, en tester l'origine c'est-à-dire dans notre exemple vérifier qu'elle appartient à Bob et l'utiliser pour chiffrer l'information qu'elle peut envoyer confidentiellement à Bob.
- Clé privée : connue uniquement par son propriétaire, Bob dans la figure 2(b) qui doit la garder secrète et qui va l'utiliser en particulier pour déchiffrer l'information qu'il reçoit et qui ont été chiffrés avec son clé publique.

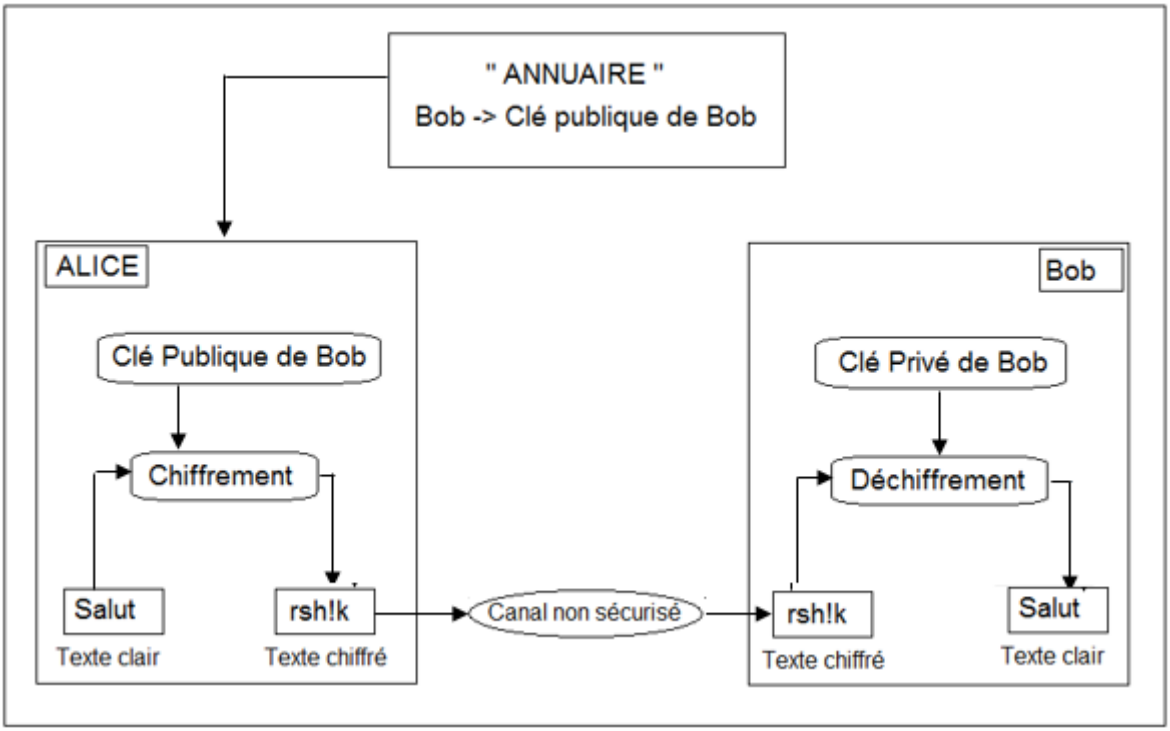

Figure 2(b) : Chiffrement symétrique [30]

Evidemment, les deux clé sont mathématiquement liées mais choisies de telle sorte qu'il soit pratiquement impossible de calculer la valeur de la clé privé à partir de la clé publique. Ces fonctions sont à sens unique, la plupart d'elles sont basée sur l'exponentielle dans un groupe fini et son inverse.

Ce type résoudre le problème distribution des clés et Assure l'authentification et la non-répudiation, mais ce sont des systèmes très lent.

6.1.4 La non-répudiation

Dans le contexte de la sécurité informatique, la répudiation définit le comportement d'une personne qui nie malhonnêtement avoir reçu ou envoyé certaines informations au cours d'une transaction ou une communication au travers d'un réseau, alors que ce n'est pas le cas. La non-répudiation constitue justement un moyen efficace pour identifier l'auteur d'une transaction. Ce protocole de sécurité permet de prouver la participation d'une entité dans un échange de données, c'est-à-dire de garantir qu'une transaction ne peut être niée.

La signature digitale est un mécanisme cryptographique qui permet d'assurer le non répudiation de l'origine.

L'émetteur du message génère sa paire de clés (publique, privée). Il diffuse sa clé publique te maintient sa clé privée secrète. Pour signer un document l'émetteur commence par calculer le code hashage du document puis signe ce code de hashage avec sa clé privée. Le résultat est la signature digitale qui accompagnera le document.

Quand le récepteur reçoit le message et la signature digitale, il recalcule le code de hashage, déchiffre la signature avec la clé publique de l'émetteur et compare les deux codes de hashages. Si les deux codes sont similaires alors la signature est valide.

L'émetteur ne pourra pas nier dans le futur avoir émis le message puisque y a que lui qui peut générer la signature digitale avec sa clé privée secrète.

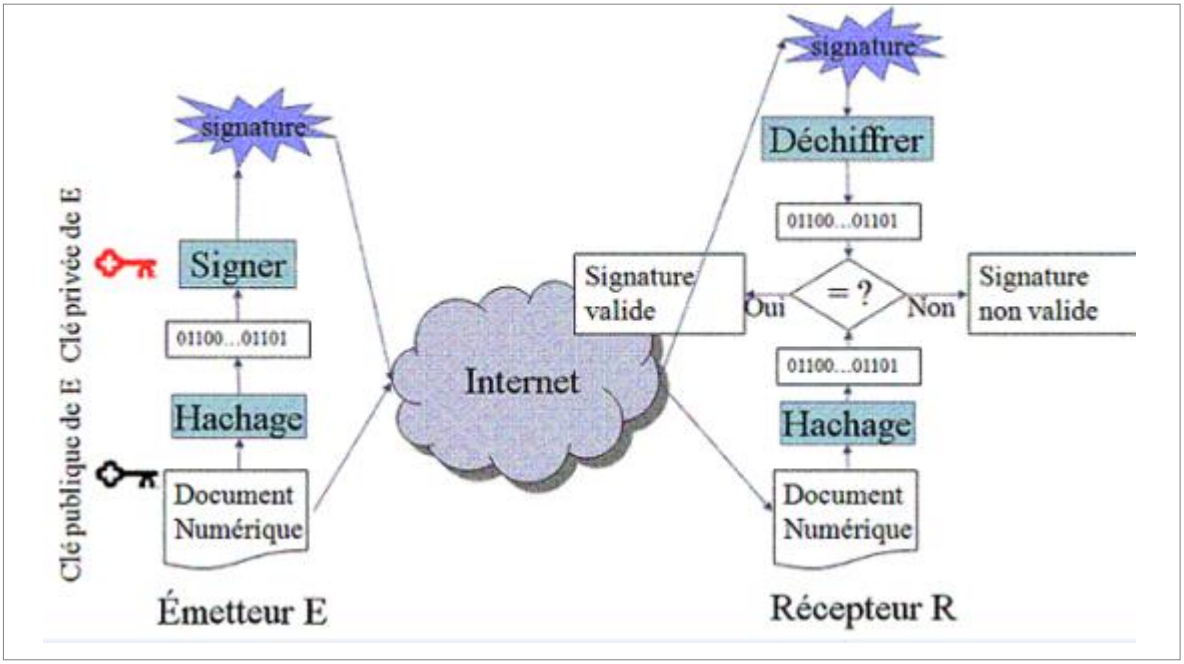

Figure 3 : Signature digitale et non-répudiation [28]

6.1.5 L'authentification

Le service d'authentification consiste à assurer l'identité d'un utilisateur, cela est effectué par un contrôle d'accès par exemple des techniques traditionnelles:

– *Some Thing you Know* : mot de passe
– *Some Thing you Have* : carte à puce
– *Some Thing you Are* : empreinte digitale

Ces techniques permettent de vérifier l'identité annoncée et à s'assurer la non usurpation de l'identité d'une entité.

D'autres caractéristiques sont également utilisées peuvent s'ajouter à celles précitées, tels que :

6.1.6 La traçabilité :

elle consiste à garder trace de l'heure d'accès, des informations divulguées, du nom et de l'adresse de l'utilisateur, de l'objectif etc.

Par exemple, dans le domaine médical, l'accès au dossier médical peut être forcé en cas d'urgence pour sauver la vie de patient. Par contre, les circonstances des accès doivent être sauvegardées pour justifier par la suite les raisons de ces accès.

En Effet, Toute information circulant sur Internet peut être capturée, enregistrée ou modifiée : Problème de confidentialité et d'intégrité.

Toute personne peut falsifier son adresse IP (spoofing) ce qui engendre une fausse identification : Problème d'authentification.

Aucune preuve n'est fournie par l'application sur l'accès au dossier médical: Problème d'absence de traçabilité.

D'une manière générale, la sécurité d'un système d'information consiste à assurer l'unique utilisation des ressources systèmes d'une organisation dans le cadre prévu. Elle est évaluée par ces propriétés, ce sont des caractéristiques critiques des ressources.

Ces critères sont généralement assurés par des techniques et mécanismes qui portent essentiellement sur divers aspects, tels que :

6.2 La sécurité des réseaux :

L'une des tendances de croissance les plus rapides de la technologie est la connectivité de tous les supports de communication sur un réseau unique homogène. Cette conversion permet à de nombreuses fonctions disparates de se réunir pour incorporer dans les limites d'un seul réseau d'information. Ce progrès est déjà apparent au sein du réseau de l'hôpital avec l'intégration des systèmes d'information de radiologie et les systèmes d'information de l'hôpital dans un système d'archivage et de transmission d'images. Cette intégration peut introduit une nouvelle vulnérabilité sur le réseau d'information de l'hôpital.

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs possèdent uniquement les droits qui leur ont été accordés.

Il peut s'agir :

- d'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- d'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système
- de sécuriser les données en prévoyant les pannes
- de garantir la non-interruption d'un service

La clé pour une bonne sécurité réseau réside dans la mise en place de mécanismes d'isolation entre les différentes composantes de réseau, l'outil de base pour cela est le filtreur de trafic pare-feu (firewalls en anglais) qui permettent de surveiller et de restreindre les accès de l'extérieur (par exemple, l'Internet) vers l'intérieur (une machine, un réseau local, les réseaux de l'hôpital), et aussi les accès de l'intérieur vers l'extérieur grâce à un ensemble de règles. Les pare-feu comportent des fonctions de filtrage qui ne laissent passer que les paquets en provenance des adresses (IP+numéro de port) autorisées, et se

préoccupent le plus souvent de la résolution des problèmes de confidentialité et d'intégrité des données qui transitent.

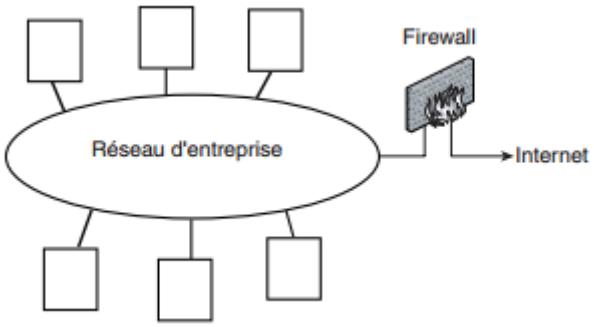

Figure 4 : un pare-feu qui sépare physiquement le réseau d'hôpital du réseau internet [31]

Le pare-feu à séparation de réseaux est illustré à la figure 4 C'est un routeur qui possède deux cartes réseaux et sépare physiquement le réseau de l'hôpital d'Internet : tout le trafic inter réseau passe par le pare-feu qui peut exécuter son filtrage sur chaque requête entrante ou sortante…

6.3 La détection d'intrusions :

Nous appellerons intrusion toute utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'acquisition de privilèges de façon illégitime. Le système de détection d'intrusion (SDI) est un outil qui se charge de surveiller le réseau et alerte l'administrateur en cas de comportement anormal.

On distingue deux grands types d'approches pour détecter des intrusions. La première consiste à rechercher des signatures connues d'attaques tandis que la seconde consiste à définir un comportement normal du système et à rechercher ce qui ne rentre pas dans ce comportement. Un système de détection d'intrusions par recherche de signatures connaît ce qui est mal, alors qu'un système de détection d'intrusions par analyse de comportement connaît ce qui est bien. On parle de détection de malveillances et de détection d'anomalies...

6.3.1 La détection de malveillances :

La détection de malveillances fonctionne essentiellement par la recherche d'activités abusives, par comparaison avec des descriptions abstraites de ce qui est considéré comme malveillant.

Cette approche tente de mettre en forme des règles qui décrivent les usages non désirés, en s'appuyant sur des intrusions passées ou des faiblesses théoriques connues.

Les inconvénients de ce type sont :

- Base de signatures difficile à construire.
- pas de détection d'attaques non connues.

6.3.2 La détection d'anomalies

Cette approche se base sur l'hypothèse que l'exploitation d'une faille du système nécessite une utilisation anormale de ce système, et donc un comportement inhabituel de l'utilisateur. Elle cherche donc à répondre à la question « le comportement actuel de l'utilisateur ou du système est-il cohérent avec son comportement passé ? ».

Les inconvénients de ce type sont :

- Pour un utilisateur au comportement Instable, toute activité est normale.
- En cas de profonde modification de l'environnement du système cible, déclenchement d'un flot continu d'alarmes.

7. Conclusion

L'information médicale est très sensible et confidentiel, donc chaque établissement de santé doit respecter les lois de la sécurité des données et garantir au patient le respect de sa vie privée. Au cours de ce chapitre nous avons abordé la notion du dossier médical informatisé et ces avantages. Ainsi qu'on a parlé sur les différents aspects liés à la sécurisation de ses ressources précieuse et les concepts de sécurité avec des exemples des solutions retenues actuellement pour faire face aux différents risques. À titre d'exemple, nous avons décrit le chiffrement, la signature numérique, les pare-feu, etc.

Etat de l'art sur la sécurité du dossier médical informatisé

Introduction

Le XXe siècle fut marqué par la révolution des technologies de l'information et des communications.

Avec l'ère du numérique, toute une variété de nouveaux défis techniques, scientifiques et sociaux est apparue. L'un d'entre eux est la sécurité des systèmes d'information.

Il éveille utilisateurs, industriels et scientifiques. Les grandes entreprises redoutent la mise hors d'usage de leurs systèmes de production et la fuite d'informations confidentielles.

Les principes d'authentification et d'autorisation sont incontournables lorsqu'on envisage de garantir la sécurité d'un système. L'authentification concerne la preuve de l'identité, l'autorisation c'est le synonyme de contrôle d'accès et elle définit et impose ce qu'il est permis et interdit de faire.

Les recherches dans le domaine du contrôle d'accès furent initiées par le Departement of Defense américain (DOD) dans les années 70. Des modèles théoriques furent élaborés et très largement implantés, pour faire face aux besoins de sécurité, militaires à l'époque. Avec la démocratisation de l'informatique et son usage incontournable dans presque toutes les organisations, tous les acteurs de l'informatique prêtent désormais attention à la sécurité de leurs systèmes d'information, pour des raisons juridiques, éthiques (respect de la vie privée), techniques (interconnexion de réseaux locaux, régionaux et nationaux) et déontologiques (secret médical, par exemple).

Beaucoup des travaux sont réalisé dans le domaine médicale, des modèles sont proposé et d'autre sont réutilisé. Le modèle DAC (Contrôle d'Accès Discrétionnaire), est le plus ancien de ces modèles, c'est un mécanisme décentralisé basé sur l'utilisateur dans lequel le créateur d'une donnée possède la pleine discrétion de définir les autorisations. MAC (Contrôle d'Accès Mandataire) est un mécanisme de contrôle d'accès basé sur l'étiquetage (exemple : Top Secret, Secret..) des différentes entités (sujets et objets) du système. D'autres politiques de sécurité, fondés sur le concept de rôle, sont une première étape pour répondre à tels besoins sectoriels. La famille des modèles RBAC (Contrôle d'Accès à Base de Rôle) présente une nouvelle organisation des droits centrée sur le concept de rôle pour simplifier l'administration des droits des grands systèmes.

Plus récemment, les modèles TBAC (Contrôle d'Accès A base de Tache) et TMAC (Team based Accès Control) ont également été proposés. Ces modèles raffinent le modèle RBAC en introduisant respectivement les notions de tâches et d'équipes.

Ainsi, des modèles et politiques, reposant sur les notions de contextes C-TMAC (Context Team based Accès Control) et O-RBAC (Contrôle d'accès a base d'organisation).

1. Description des modèles de contrôle d'accès

1.1 Les politiques discrétionnaires (ou DAC pour Discretionary Access Control).

Dans le cas d'une politique discrétionnaire, les droits d'accès à chaque information sont manipulés librement par le responsable de l'information (généralement le propriétaire), chaque objet à un propriétaire qui décide quels sont les sujets qui ont accès à cet objet.

Plusieurs modèles sont associés à DAC :

1.1.1 Modèle de Lampson

La notion de matrice de contrôle d'accès, dédiée à la représentation des droits d'accès (autorisations), a été introduite par Lampson dès 1971.

Ce modèle peut être représenté par un triplet (S, O, Mso) où S désigne les sujets, O les objets et Mso la matrice de contrôle d'accès qui associe à chaque couple (sujet s, objet o) un ensemble de droits d'accès.

Sujet/Objet	o_1	…	o_j	…	o_N
s_1	*Lecture Écriture Exécution*	…		…	*Pas d'accès*
s_2	*Lecture*	…		…	*Lecture*
⋮	…	…		…	…
s_i		…	***Lecture***	…	…
⋮	…	…	…	…	…
s_M	*Pas d'accès*	…		…	*Écriture*

Tableau 2- Matrice de contrôle d'accès [29]

La matrice représentée dans le tableau 3 nous montre que le droit d'accès r est associé au sujet S_i et l'objet O_j. Les droits correspondent généralement à des actions élémentaires telles que « lire » ou « écrire ». La matrice des droits d'accès n'est pas figée. En effet, si de nouveaux objets, de nouveaux sujets ou de nouvelles actions sont ajoutées dans le système, il devient alors nécessaire d'enregistrer toutes les permissions accordées pour ces nouvelles entités. Par conséquent, si la matrice est de taille petite, on n'a aucun problème, mais si cette matrice est de grande taille cela pose une difficulté de la mise à jour

du politique de sécurité exprimée par ce modèle. Enfin, ce modèle ne permet pas d'exprimer directement des interdictions ou des obligations.

Le règlement (politique d'autorisations) correspond à un ensemble d'autorisations positives (permissions) du type : "le sujet s a la permission de réaliser l'action a sur l'objet o". La politique d'autorisation par défaut est fermée, par défaut tous les accès sont interdits "tout ce qui n'est pas explicitement autorisé est interdit"

Le modèle de Lampson a été progressivement amélioré pour donner naissance à d'autres modèles tels que le modèle de Harrison-Ruzzo-Ullman (HRU).

1.1.2 Modèle de Harrison-Ruzzo-Ullman

Ce modèle de control d'accès fournit des commandes pour attribuer les droits d'accès, ainsi que pour créer et supprimer les sujets et les objets.

La politique de sécurité est réduite à l'expression des permissions ; ces dernières étant des relations entre les sujets, les objets et les actions. Elles sont représentées dans la matrice A des permissions.

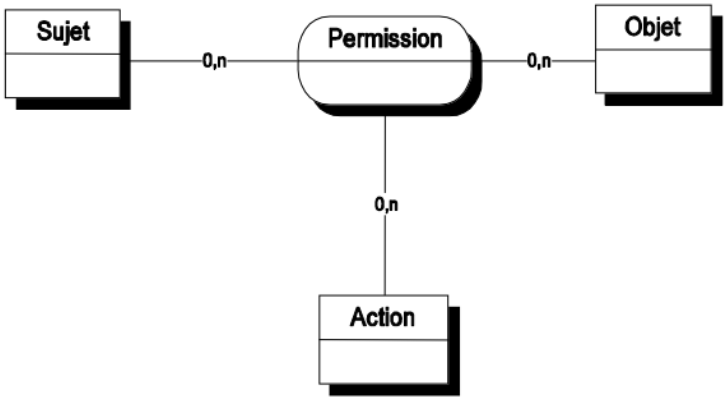

Figure 5 : le modèle HRU. [3]

Si s est un sujet et o est un objet alors, A(s, o) définit l'ensemble des actions α que le sujet s est autorisé à faire sur l'objet o.

La politique de sécurité s'exprime à travers l'énumération dans la matrice des permissions de tous les triplets <s, o, α>. Si de nouveaux objets, de nouveaux sujets ou de nouvelles actions sont ajoutés au système d'information, il est alors nécessaire d'enregistrer toutes les permissions accordées à ces nouvelles entités. Ce modèle offre la possibilité de vérifier qu'il n'y a pas d'ajout aléatoire de droits dans la matrice d'accès.

Exemple de politique d'accès discrétionnaire, gestion des droits d'accès aux fichiers sous UNIX : Trois types d'accès : « read » « write » « execute »

Le propriétaire du fichier peut librement définir des droits pour :

- Lui-même
- Son groupe
- Les autres utilisateurs

Le modèle de contrôle d'accès discrétionnaire limite l'accès aux objets uniquement en se basant sur l'identité de l'utilisateur, pour cela ils ont une faiblesse importante. On ne peut plus contrôler ce qui est fait de l'information une fois que celle-ci a été accédée par un utilisateur légitime. Si un utilisateur a le droit de lire une information, en générale il a le droit de la transmettre à n'importe qui. Ce problème peut être une source de diffusion de chevaux de Troie.

Afin de comprendre comment le cheval de Troie peut amener à une fuite d'information vers des utilisateurs non autorisés, nous prenons un exemple :

Supposons dans un hôpital, Bob, directeur, crée un fichier *antécédent* (*diagnostic*) contenant des informations très sensibles sur le patient. Ces informations sensibles, d'après la politique de l'organisation, ne devraient être accessibles que par Bob. Supposons maintenant qu'un utilisateur malveillant *David*, un adjoint de Bob, veuille récupérer cette information sensible, Pour cela, David crée un fichier *observation* et donne l'autorisation à Bob d'écrire dans ce fichier. David, ensuite, introduit deux opérations cachées dans l'application utilisée par Bob. Ces opérations sont *lire* dans le fichier *diagnostic* et *écrire* dans le fichier observation. Une fois que Bob exécute l'application, les opérations lire et écrire vont être permises. Puisque, l'utilisateur malveillant David est le propriétaire du fichier *observation* il pourra accéder à ce fichier et récupérer les informations désirées. [4]

En plus, les modèles DAC sont assez statiques car une fois que la matrice d'accès est en place, sa modification peut être complexe si elle est grande.

1.2 Les politiques obligatoires (ou MAC pour Mandatory Access Control).

Dans ce type de contrôle d'accès les sujets ne peuvent pas intervenir dans l'attribution des droits d'accès, Ces politiques sont généralement des politiques multi-niveaux basées sur une classification des sujets et des objets. A chaque sujet et objet on attribue une classe dans l'ensemble (Confidentiel, Secret, Top Secret, etc). La classe de l'objet indique la sensibilité de l'information, alors que la classe du sujet indique le degré de confiance accordé au sujet en termes de divulgation d'information.

Prenons l'exemple d'un système d'administration du personnel : le nom et l'adresse d'un employé peuvent ne pas être considérés comme des informations sensibles de sorte que tous les sujets peuvent accéder à ces informations. Toutefois, leurs salaires peuvent être

considérés comme confidentiels de sorte que seulement un employé, ses directeurs et le personnel du département peuvent avoir accès à cette information.

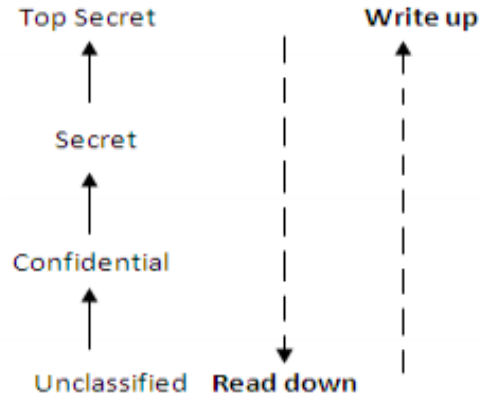

Figure 6 : Sécurité multi-niveaux [5]

La figure 6 représente un modèle de contrôle d'accès qui autorise 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.

Ce modèle résoudre le problème de fuite d'information (voir l'exemple dans le modèle précèdent) c'est-à-dire la divulgation des données dans un système de règles de contrôle d'accès. Mais il reste un modèle rigide qui impose des contraintes fortes sur les organisations et qui ne permet pas la gestion des exceptions.

L'utilisation du modèle MAC dans le domaine de la santé implique que l'autorité de santé est la seule instance à pouvoir définir la politique de sécurité.

1.3 Modèle de Contrôle de Flux

Depuis 1975 on sait que le modèle de contrôle d'accès ne permet pas de prendre en compte les applications piégées par un cheval de Troie opérant par recopie de fichiers. Le modèle de contrôle des flux constitue une alternative au modèle de contrôle d'accès.

Les politiques de contrôles de flux proposent des solutions pour l'identification et l'élimination des canaux cachés. Un canal caché est un chemin de communication pouvant être exploité par un processus de transfert d'information de telle sorte qu'il contourne les mécanismes de contrôle d'accès, et qu'ainsi il viole la politique de sécurité «une fuite d'information vers un utilisateur qui n'est pas autorisé à accéder à cette information ».

De nombreux modèles de politiques de flux d'information ont été proposés dans la littérature. Nous présenterons successivement dans cette section le modèle en treillis inspiré par les travaux de Bell et LaPadula.

1.3.1 Politiques en treillis

Ce type de modèle a été associé aux politiques multiniveaux, Afin de contrôler les flux d'information entre les objets, chaque objet est associer à une classe de sécurité, la comparaison entre les classes de sécurité des objets permettant de spécifier si le flux est légal ou non.

Un exemple de politique de flux d'information le plus courant est celui utilisé dans le milieu militaire. Il est composé de 4 niveaux de confidentialité (non classifié, diffusion restreinte, confidentiel, secret) totalement ordonnés.

1.3.2 Modèle de Bell et LaPadula

Le modèle de contrôle proposé par Bell et LaPadula vise à contrôler la confidentialité des données utilisées dans un système. Ce modèle est une première approche du contrôle de flux d'information au niveau d'un système.

Le système de Bell et LaPadula est composé des éléments suivants :

- S un ensemble de sujets ;
- un ensemble d'objets ;
- A les opérations d'accès sur les objets {execute, read, write, append}
- L un ensemble de classes de sécurité avec un ordre partiel ≤ ;
- un état est une matrice ($S \times O \rightarrow A$) qui pour chaque sujet $s \in S$, chaque objet $o \in O$, décrit tous les accès autorisés $a \in A$.

A chaque sujet est attribué une habilitation $h(s) \in L$ et à chaque objet est associé une classification $c(o) \in L$. Ces habilitations et classifications sont fixes et n'évoluent pas lors des modifications de l'état du système.

Un état est considéré comme sûr s'il respecte les deux propriétés suivantes : [6]

- (Propriété simple). Si (si, oj, lecture) $\in (S \times O \times A)$ alors $c(oj) \leq h(si)$.
- (Propriété ⊛). Si (si, oj, lecture) $\in (S \times O \times A)$ et (si , ok, écriture) $\in (S \times O \times A)$, alors $c(oj) \leq c(ok)$.

La propriété simple permet d'assurer qu'un sujet n'accède en lecture qu'à des objets dont le niveau de classification est inférieur à son niveau d'habilitation. Cette propriété permet d'assurer le contrôle d'accès à l'information.

La propriété ⊛ permet de contrôler le flux d'information en empêchant un sujet pouvant accéder à un objet d'un niveau de classification d'écrire le contenu de celui-ci dans un objet de classification inférieure.

Figure 7: Vulnérabilité aux chevaux de Troie. [7]

Bell–LaPadula empêche certains chevaux de Troie, On considère deux classes de sécurité : Secret et Non-classifié. On place Alice et Bob dans la classe Secret et Charlie dans Non- classifié.

Le cheval de Troie de Bob va travailler en tant que sujet Secret, car créé par un sujet Secret par la propriété ⊛. En conséquence, le cheval de Troie ne pourra pas créer de fichier de classe Non-classifié, par la même propriété ⊛. Finalement, Charlie ne pourra lire aucun fichier créé par Alice, Bob ou le cheval de Troie par la propriété de sécurité simple. [8]

Ces types des modèles sont généralement réservés à des usages militaires qui traitent de la confidentialité, a cause de ces règlements rigide et ils sont plus complexe a implémenté.

1.4 Politiques et modèles de sécurité par rôles (RBAC)

La politique basée sur les rôles (RBAC, pour Role-Based Access Control) a été proposé pour la première fois selon Amal HADDAD [1] en 1992 par David Ferrailo et Richard Kuhn dans l'article [9], attachés au département de commerce des Etats-Unis. Ce modèle propose de structurer l'expression de la politique d'autorisation autour du concept de rôle.

Un rôle représente de façon abstraite une fonction identifiée dans l'organisation (par exemple, chef de service, ingénieur d'étude, etc.). À chaque rôle, on associe des permissions, ensemble de droits correspondant aux tâches qui peuvent être réalisées par chaque rôle.

Contrairement aux modèles qui ont précédé RBAC (HRU, par exemple), les permissions ne sont plus associées d'une façon directe aux sujets, mais à travers des rôles. Ensuite, les sujets peuvent être attribués aux rôles qui découlent généralement de la structure d'une organisation.

RBAC est considéré comme un système « idéal » pour les entreprises dont la fréquence de changement du personnel est élevée (c'est un modèle dynamique). En effet quand un sujet X est remplacé par le sujet Y, il n'est pas nécessaire d'affecter à Y individuellement toutes les permissions de X mais il suffit d'affecter à Y le même rôle de X.

Un rôle peut avoir plusieurs permissions et une permission peut être associée à plusieurs rôles. De même qu'un sujet peut être membre de plusieurs rôles et inversement, un rôle peut être exécuté par plusieurs sujets. Ainsi, si le docteur X est à la fois chirurgien et directeur de l'hôpital, en tant que chirurgien, il aura le droit d'accès aux dossiers médicaux, alors qu'en tant que directeur, il pourra accéder aux informations administratives.

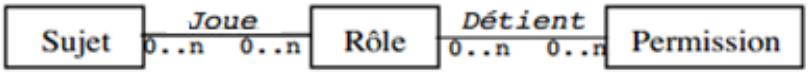

Figure 8 ; Attribution des permissions aux sujets à travers des rôles. [11]

Le côté dynamique du modèle est matérialisé par la notion de session et de hiérarchie de rôles. Une session est attribuée à un utilisateur, ce dernier a la possibilité d'ouvrir plusieurs sessions en même temps, ou uniquement le sous-ensemble de ses rôles nécessaires à la réalisation de la tâche à accomplir.

Cependant à un instant donné, un utilisateur exerce un seul rôle. C'est la notion de rôle actif. Le contrôle d'accès se déroule au cours d'une session. Un utilisateur a le droit d'exécuter sur les objets les seules opérations que son rôle activé lui autorise.

Ce modèle contribue également à maîtriser la complexité de la gestion des droits d'accès, grâce au mécanisme d'héritage entre les rôles : les rôles peuvent être structurés de façon hiérarchique, un (sous-)rôle héritant des permissions du rôle dont il dépend hiérarchiquement.

Par exemple, le rôle chirurgien possède toutes les permissions du rôle médecin.

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

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

1.5 Modèles de contrôle d'accès à base des tâches TBAC

Le modèle TBAC (Task Based Access Control) a été conçu afin d'activer une permission par rapport aux tâches effectuées par l'utilisateur. L'idée essentielle de ce modèle à ajouter la notion de tâche dans des règles d'autorisation. Cela permet de définir les permissions qu'un sujet peut activer selon la tâche qui est en cours.

Le modèle TBAC fut le premier modèle à introduire le concept de tâche [10]. Cette notion permet de contrôler les activités exercées par les utilisateurs d'un système d'information au sein de l'organisation. TBAC n'intègre pas la notion de rôle. Le modèle TR-BAC (Task and Rôle BAC) a été défini pour l'adaptation et l'intégration de cette notion. Dans ce cas, les droits sont activés en fonction d'un rôle et portent sur la réalisation des tâches.

TBAC est bien adapté pour le calcul distribué et les activités de traitement de l'information avec de multiples points d'accès, c'est un modèle de sécurité "actifs". Dans une approche active de la gestion de sécurité, les autorisations sont constamment surveillés et activés et désactivés en conformité avec des contextes émergeants associé à des tâches progressant.

TBAC présente l'inconvénient de ne pas prendre en compte des contraintes sur les horaires ou périodes d'accès pendant lesquels les utilisateurs sont en charge de la réalisation de leurs activités. Le manque constaté est couvert par d'autres modèles formels de contrôle d'accès.

1.6 Politiques et modèles de sécurité par équipes (C-TMAC)

Le modèle TMAC (pour Team-based Access Control en anglais) a été formulé pour la première fois selon Anas ABOU EL KALAM [11] en 1997 par Thomas dans son article TMAC: A primitive for Applying RBAC in Collaborative Environment.

Le but était de fournir un contrôle d'accès pour les systèmes d'information ayant des activités nécessitant la collaboration de plusieurs personnes. L'entité de base, l'équipe, est une abstraction qui encapsule un ensemble d'utilisateurs ayant des rôles différents et qui collaborent dans le but d'accomplir une tâche commune. Les utilisateurs appartenant à une équipe donnée devront avoir accès à l'ensemble des ressources utilisées par l'équipe, et ces permissions dépendent des variables environnementales (lieu, temps, le patient traité, etc.), elles peuvent donc changer selon le contexte.

C-TMAC (Context-based Team Access Control) est une adaptation de TMAC aux domaines dépendant du contexte tels que celui de la santé, par exemple, un patient est traité dans le service de médecine générale. Suite à une attaque cardiaque, il est transféré

d'urgence à l'unité de soins cardiologiques. Donc la tâche de l'équipe de cardiologie est exécutée durant un intervalle de temps donné et dans un endroit spécifique. Les variables contextuelles sont le temps, le lieu et le patient.

C-TMAC utilise un mélange de RBAC et TMAC, et consiste en cinq entités : utilisateurs, rôles, permissions, équipes et contextes.

La déduction des privilèges se fait selon les deux règles suivantes : [12]

- privilège-rôle = Combinaison [privilège-rôle-session, privilège-équipe]
- privilège-contexte = Filtrage [privilège-rôle, contexte-équipe]

Privilège-rôle est une combinaison (union, maximum ou minimum) des permissions associées au rôle de l'utilisateur avec les permissions de l'équipe à laquelle il appartient.

Si la combinaison est l'union, privilège-rôle correspond à l'ensemble des permissions de tous les membres de l'équipe.

Si la combinaison est un maximum (respectivement le minimum) : privilège-rôle est égal à l'ensemble maximal (respectivement minimal) des permissions des membres de l'équipe.

L'ensemble des permissions finales, réduit privilège-rôle en tenant compte du contexte des équipes de l'utilisateur.

Le contexte du rôle précise les valeurs que doivent prendre certaines variables pour autoriser l'utilisateur à jouer le rôle. Il est parfois possible d'associer des contraintes aux rôles, par exemple : la cardinalité, pour désigner le nombre maximal d'utilisateurs autorisés à jouer le rôle ; l'exclusion mutuelle statique, pour spécifier qu'un utilisateur ne peut jamais jouer deux rôles (dans le même établissement, être personnel soignant et comptable) ; l'exclusion mutuelle dynamique pour obliger l'utilisateur à ne pas jouer deux rôles simultanément (médecin à l'hôpital et médecin travaillant pour une société d'assurance), etc.

Le contrôle d'accès basé sur les équipes, C-TMAC considère deux relations binaires (utilisateur, rôle) et (utilisateur, équipe). Un utilisateur peut donc activer n'importe lequel de ses rôles dans n'importe laquelle de ses équipes. Dans la pratique, même si un utilisateur a le droit de jouer plusieurs rôles, il n'a pas forcément le droit de les jouer dans n'importe laquelle de ces équipes. Le modèle Or-BAC traite ce problème en ajoutant la notion de « rôle dans organisation ».

1.7 Modèle de contrôle d'accès à base d'organisation (Or-BAC)

Or-BAC, (Organization Based Acces Control) présenté pour la première fois en2003 par [13] selon BELLAL Toufik [2]. Ce modèle propose de structuré l'ensemble des objets et des actions et non pas seulement les sujets. Une notion d'organisation tient un rôle central.

Le but principal du modèle est de permettre de définir une politique de sécurité indépendamment de son implémentation. Cette politique est modélisée à deux niveaux différents: un niveau abstrait qui spécifie les permissions et les interdictions entre les rôles, les activités et les vues, et un niveau concret qui permet de dériver les permissions et les interdictions entre les sujets, les actions et les objets (voir figure 9).

Ces deux niveaux sont reliés de la façon suivante. Dans une organisation org, un sujet s a la permission d'exécuter une action α sur un objet o si :

(1) : s est habilité dans un certain rôle r dans org.
(2) : α implante une certaine activité a dans org.
(3) : o est utilisé dans une certaine vue v dans org.

Si ces trois conditions sont satisfaites et si :

(4) : org accorde au rôle r la permission de réaliser l'activité a sur la vue v dans le contexte c, et dans org; le contexte c est satisfait entre le sujet s, l'action α et l'objet o.

Alors une requête par le sujet s de réaliser l'action α portant sur l'objet o est acceptée.

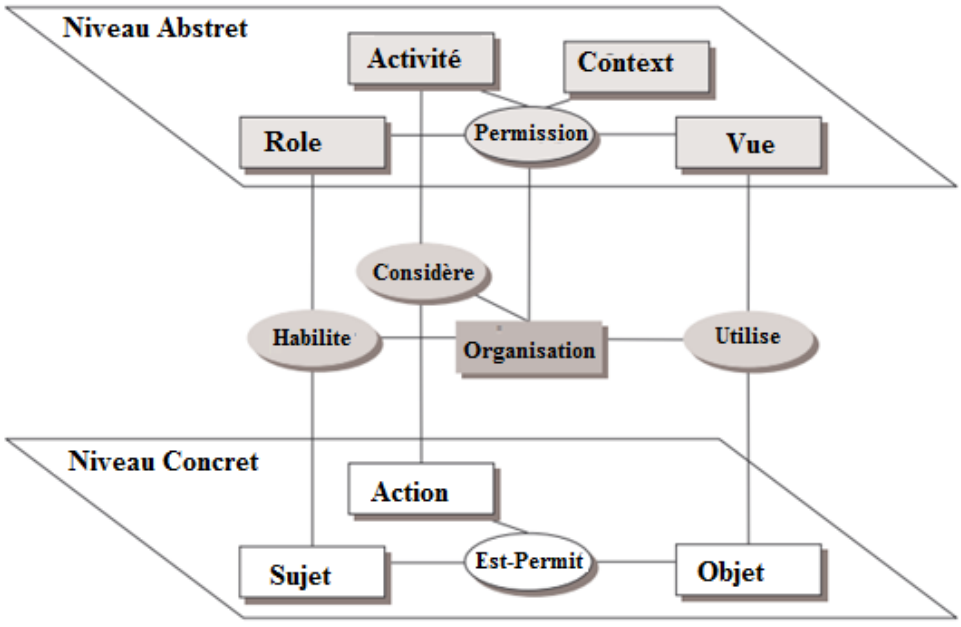

Figure 9: le modèle Or-BAC [14]

On remarquera également la position centrale de l'organisation. Une organisation peut être vue comme un groupe organisé d'entités actives. C'est t'a dire de sujets jouant certains rôles. Notons qu'un groupe de sujets n'est pas nécessairement considérer comme une organisation.

1.7.1 Les sujets et les rôles

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

La relation Habilite (figure 10). Si org est une organisation, s est un sujet et r est un rôle, alors Habilite(org, s, r) signifie que org habilite le sujet s à jouer le rôle r.

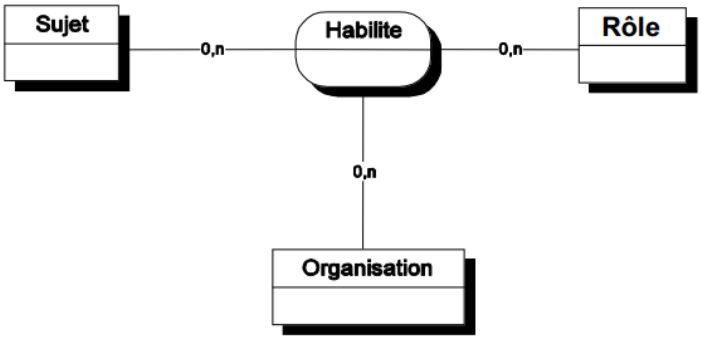

Figure 10: la relation Habilite [3]

Un sujet est soit un utilisateur, soit une organisation. Par exemple {Habilite (H1, Dr.Mohamed, cardiologue) : « l'hôpital H1 habilite Dr.Mohamed dans le rôle cardiologue »} ou {Habilite (H2, ICU31, unité_des_soins_intensifs) : « l'hôpital H2 habilite l'unité ICU31 dans le rôle d'unité des soins intensifs »} [15]

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

1.7.2 Les objets et les vues

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

Dans la mesure où il est également nécessaire de structurer les objets et d'ajouter de nouveaux objets au système, Nous l'appelons : entité Vue. Une vue correspond, comme dans les bases de données relationnelles, à un ensemble d'objets qui satisfait une propriété commune. Par exemple, la vue « dossiers médicaux » correspond aux dossiers médicaux des patients.

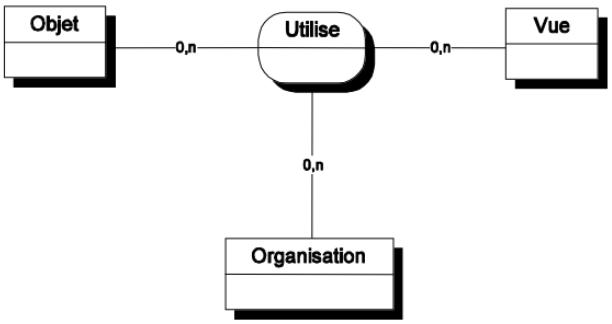

Figure 11 : relation Utilise. [3]

Dans la mesure où les vues caractérisent la manière dont les objets sont utilisés dans l'organisation, nous avons besoin d'une relation qui lie ces trois entités : la relation Utilise (figure 11), Utilise (org, o, v) signifie que org utilise l'objet o dans la vue v.

1.7.3 Les actions et les activités

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

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

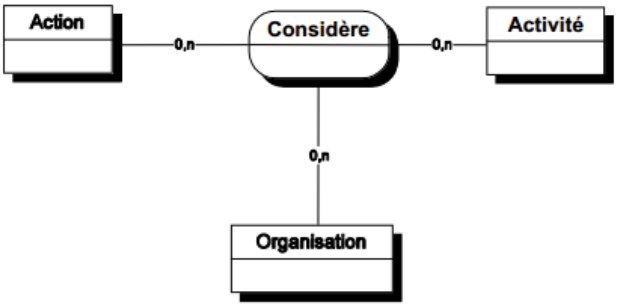

Figure 12 : la relation Considère. [3]

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

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

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

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

1.7.4 Les Contextes

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

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

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

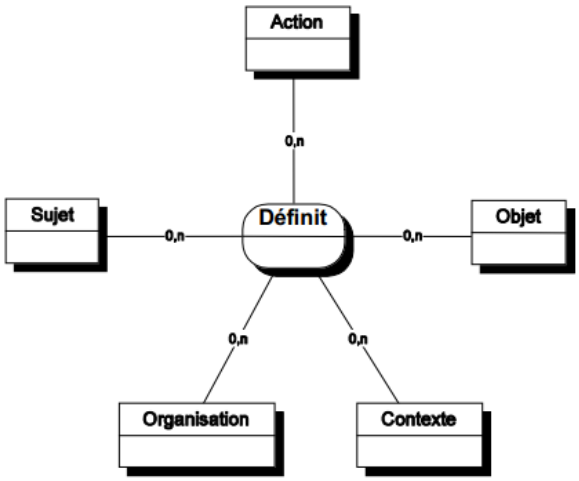

Figure 13 : la relation Définit [3]

Par exemple,

(1) Définit(hôpital1, Mohamed, lire, F31.doc, urgence) et,
(2) Définit(hôpital2, Ali, lire, F32.tex, médecin_traitant).

Si le premier fait est vrai, alors Mohamed n'a pas besoin d'être le médecin traitant du patient correspondant au dossier médical F31.doc pour consulter son dossier. En effet, il est raisonnable de considérer que dans un contexte d'urgence, les médecins ont un accès immédiat à tous les dossiers médicaux. Si le second fait est vrai, alors Ali doit être le médecin traitant du patient dont le dossier médical est F32.tex : dans un contexte normal comme « médecin traitant ».

Or-BAC permet d'exprimer aussi bien les autorisations, que les interdictions ainsi que les obligations/recommandations. On pourra ainsi, grâce aux obligations, autoriser un infirmier à accéder à un dossier médical en cas d'urgence sous condition qu'il rédige par la suite un rapport. Cette condition est exprimée grâce aux obligations.

2. Résumé

Le contrôle d'accès, c'est le mécanisme qui définit et impose ce qu'il est permis et interdit de faire, c'est un outil technique et organisationnel incontournable lorsqu'on envisage de garantir la sécurité d'un système. Le tableau suivant représente un résumé de chaque modèle de sécurité détaillé dans ce chapitre

modèle	principe
Dans les modèles discrétionnaires DAC	les utilisateurs sont autorisés à définir leur propre règlement de sécurité sur les informations dont ils sont propriétaires, en attribuant et en retirant des droits aux autres membres de l'organisation.
Les modèles obligatoires MAC	s'appuient sur le niveau de confiance accordé aux sujets. Ainsi, si un sujet est habilité à un certain niveau de confiance, alors il pourra accéder aux ressources ayant un besoin de sécurité équivalent ou inférieur.
Politiques et modèles de sécurité par équipes **C-TMAC**	l'équipe est utilisée pour représenter un groupe d'utilisateurs, ayant des rôles spécifiques, et qui collaborent pour réaliser une activité. L'ensemble des droits de l'utilisateur est combiné avec l'ensemble des droits de l'équipe, et les droits finaux sont dérivés à partir du contexte.
Le modèle de contrôle d'accès basé sur les rôles RBAC	des permissions sont attribuées à un sujet en fonction des rôles.
Contrôle d'accès basé sur les organisations ORBAC	Dans une organisation org, un sujet s a la permission d'effectuer une action α sur un objet o si dans cette org:

	• s est habilité dans un certain rôle r. • α implante une certaine activité a. • o est utilisé dans une certaine vue v. et si : • org accorde au rôle r la permission de réaliser l'activité a sur la vue v dans le contexte c. • et le contexte c est satisfait entre le sujet s, l'action α et l'objet o.
Modèle de Contrôle de Flux	ces modèles proposent des solutions pour l'identification et l'élimination des canaux cachés, elles se base sur les niveaux de confidentialité et permettent de contrôler le flux d'information en empêchant un sujet pouvant accéder à un objet d'un niveau de classification différent.
Contrôle d'accès à base des tâches TBAC	La famille des modèles TBAC propose de structurer les droits selon les tâches que les acteurs du système d'information doivent effectuer, mais sans concept de rôle.

Tableau 3 : Résumé sur les modèles de contrôle d'accès

Ces modèles de sécurité sont proposées pour organiser les droits d'accès dans un système. Mais le problème reste toujours, comment choisir le bon modèle qui garantit une meilleure sécurité des données de santé informatisées ?

Le tableau si dessous représente une brève définition d'un ensemble des propriétés respecté par les politiques de contrôle d'accès :

Propriétés	définition
Rôles	Un rôle c'est ne fonction identifiée dans l'organisation (par exemple, médecin, infirmière, ingénieur d'étude, etc.). l'accès aux données est effectué par l'association des permissions à chaque rôle.
niveau de confiance	Cette propriété prend en considération la sensibilité de l'information, et le degré de confiance accordé au sujet en termes de divulgation d'information.
Contrôle de flux	Transfert d'information illégal entre deux acteurs du système d'information.
équipe	Groupe de personnes qui partagent une activité.

contexte	exprime des règles de sécurité spécifiques à certain circonstances concrètes qui entourent un fait.
permission	l'autorisation d'un sujet d'effectué une action
Interdiction	Action d'interdire quelque chose ; par exemple, les médecins n'ont pas le droit d'effacer des diagnostics déjà établis.
obligation	Ce sont des actions automatiques obligatoires dans un système, comme par exemple : Chaque fois qu'un médecin consulte un dossier d'un patient qui n'est pas à lui, un message est automatiquement envoyé à son chef de rayon.
confidentialité	Sorte de garantie de protection d'un secret lors d'une étude de dossier [18], l'information ne doit être accessible qu'aux ayants droits
Intégrité	" empêcher une modification non autorisée", c'est-à-dire empêcher toute modification (suppression, ajout, mise à jour) d'une donnée par un utilisateur non légitime [4].
Modèle dynamique	les droits d'accès sont facilement modifiables
Mise A jour	l'action qui consiste à mettre « à niveau », un outil informatique.

Tableau 4 : propriété des modèles de contrôle d'accès

Chaque modèle répond aux besoins spécifiques qui surviennent au long du cycle de vie du contrôle d'accès, Pour cela on a essai de synthétiser ces modèles par rapport a l'ensemble de ces propriétés :

PROPRIETES/ MODELE	DAC	MAC	C-TMAC	RBAC	ORBAC	MODELE DE CONTROLE DE FLUX	TBAC
ROLES			*	*	*		
NIVEAU DE CONFIANCE		*				*	
CONTROLE DE FLUX		*				*	*
EQUIPE			*				
CONTEXTE			*		*		
PERMISSION	*	*	*	*	*	*	*

INTERDICTIONS					*	*		
OBLIGATION					*			
CONFIDENTIALITE		*			*	*		
INTEGRITE	*	*	*	*	*	*		*
MODELE DYNAMIQUE			*	*	*			
FACILITE DE LA MISE A JOUR			*	*	*			

Tableau 5 : Synthèse des modèles de contrôle d'accès

3. Implémentation réel et les solutions pratiques

3.1 Sécurité Unix : Contrôle d'accès discrétionnaire

Le modèle de sécurité DAC reste la base de la sécurité Linux, Le DAC Unix est un modèle de sécurité relativement simple, toutefois, conçu en 1969. En résumé, Le DAC Unix permet au propriétaire d'un objet (un fichier par exemple) de décider de la politique de sécurité en ce qui concerne cet objet. En tant qu'utilisateur, vous pouvez, par exemple, créer un nouveau fichier dans votre répertoire personnel et décider de qui peut lire ou écrire ce fichier. Les permissions d'accès au fichier, comme la lecture et l'écriture, peuvent être positionnées séparément pour le propriétaire, C'est une forme relativement simple de liste de contrôle d'accès. [15]

Voici un exemple de définition des droits sous LINUX :

```
benaissa@benaissa-HP-630-Notebook-PC:~$ mkdir jahida
benaissa@benaissa-HP-630-Notebook-PC:~$ cd jahida
benaissa@benaissa-HP-630-Notebook-PC:~/jahida$ touch fich.txt
benaissa@benaissa-HP-630-Notebook-PC:~/jahida$ chmod -wr fich.txt
benaissa@benaissa-HP-630-Notebook-PC:~/jahida$ chmod +wr fich.txt
```

3.2 Trusted Extensions: fournit des contrôles d'accès discrétionnaire et obligatoire

Trusted Extensions offre des fonctionnalités qui permettent à une organisation de définir et de mettre en œuvre une stratégie de sécurités qui correspond à l'ensemble de règles qui vous aident à protéger et gérer les autorisations d'accès de chacun aux différents types

d'informations pour votre système Oracle Solaris, en proposant à la fois un contrôle d'accès discrétionnaire et un contrôle d'accès obligatoire.

Le DAC laisse à la discrétion du propriétaire la définition de la protection des fichiers. Les deux formes de DAC sont les bits d'autorisation UNIX et les listes de contrôle d'accès (ACL).

Les bits d'autorisation permettent au propriétaire de définir la protection en lecture, écriture et exécution en fonction du statut de l'utilisateur : propriétaire, groupe et autres utilisateurs.

La stratégie MAC utilise les étiquettes de sensibilité à tous les processus créés pour exécuter des programmes. [16]

3.2.1 Processus de connexion à Trusted Extensions

a) Identification : tapez votre nom d'utilisateur dans le champ Username.

b) Authentification : tapez votre mot de passe dans le champ Password.
Votre mot de passe est stocké sous forme cryptée et n'est pas accessible par d'autres utilisateurs sur le système.
La réussite de l'identification et de l'authentification confirme que vous êtes autorisé à utiliser le système.

c) Vérification des messages et sélection du type de session : examinez les informations dans la boîte de dialogue Message du jour (Message Of The Day). Cette boîte de dialogue affiche l'heure de votre dernière connexion, les éventuels messages de l'administrateur et les attributs de sécurité de votre session.

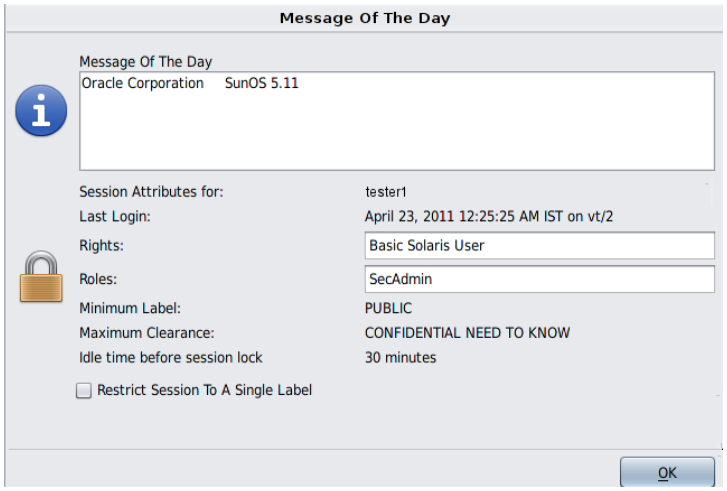

Figure 14 : la boite de dialogue (message du jour)

d) Sélection d'étiquette : dans le générateur d'étiquettes (label builder), choisissez le niveau de sécurité le plus élevé auquel vous avez l'intention de travailler pendant votre session.

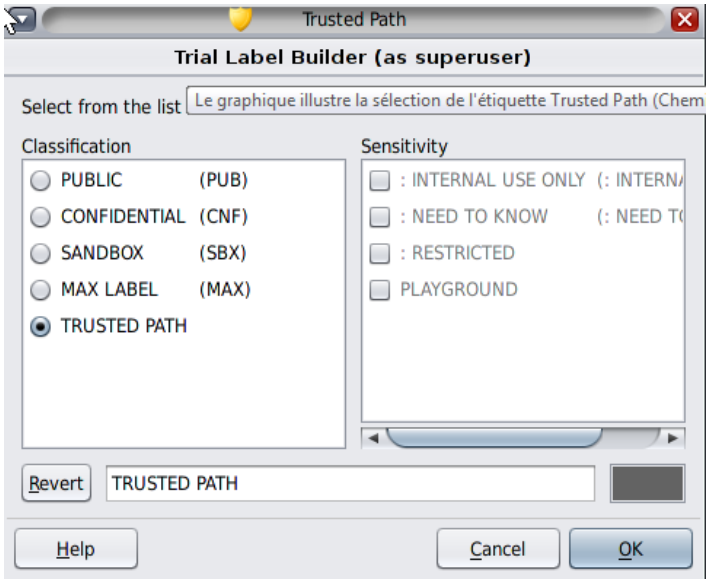

Figure 15 : générateur d'étiquettes

Une fois vous êtes connecté vous pouvez travailler dans Trusted Extensions.

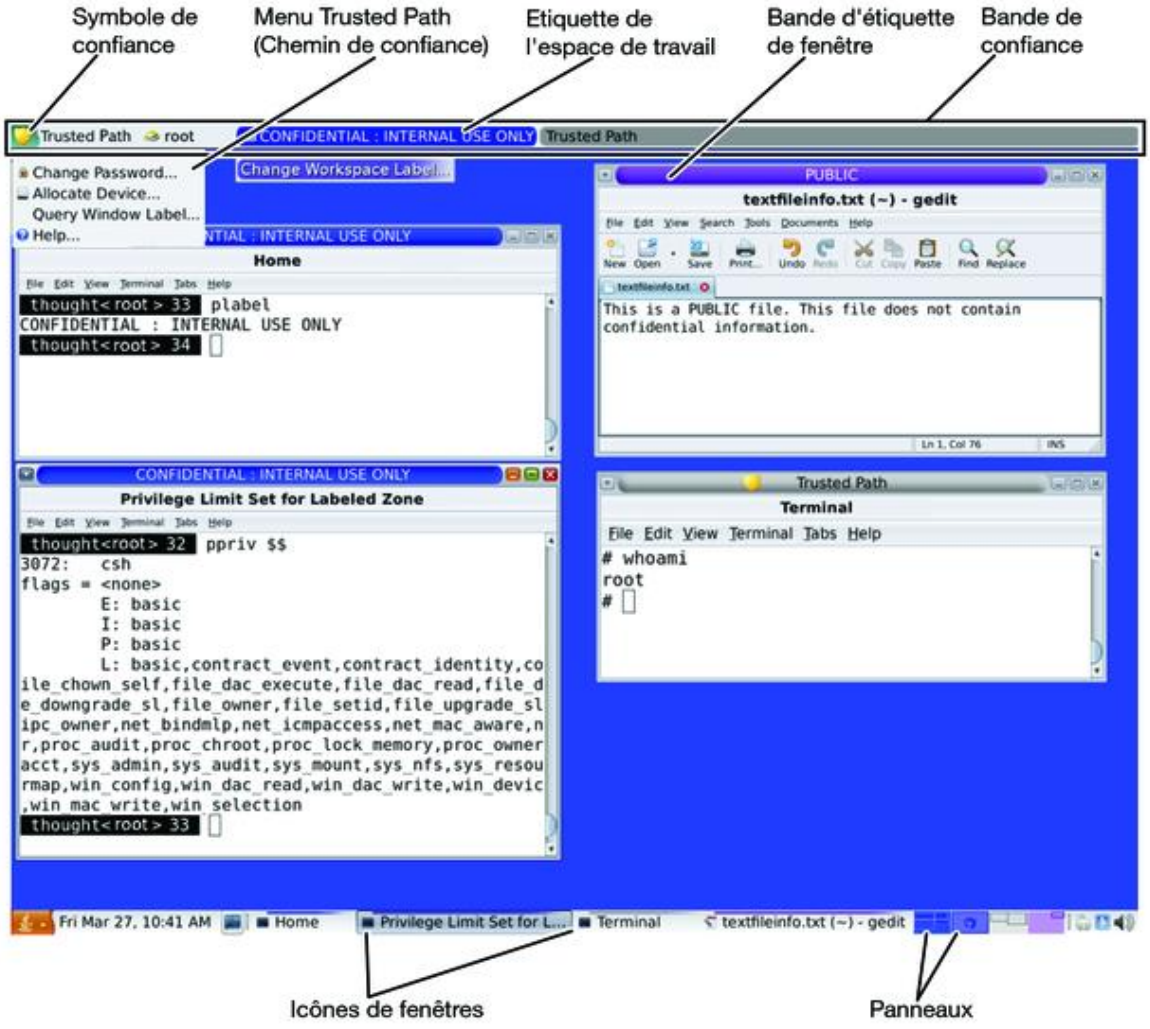

Figure 16 : une session multiniveau classique de Trusted Extensions.

Trusted Extensions utilise des conteneurs pour l'étiquetage. Les conteneurs sont également appelés zones. La zone globale est une zone d'administration et n'est pas disponible pour les utilisateurs. Les zones non globales sont appelées zones étiquetées. Les zones étiquetées sont disponibles pour les utilisateurs.

La communication réseau est limitée par étiquette. Par défaut, les zones ne peuvent pas communiquer les unes avec les autres car leurs étiquettes sont différentes.

L'administrateur peut configurer des zones spécifiques afin qu'elles puissent lire des répertoires spécifiques d'autres zones. Par exemple, le répertoire personnel d'un utilisateur situé dans une zone de niveau inférieur peut être monté à l'aide du service de montage automatique.

MAC est automatiquement appliqué par le système. Si vous êtes autorisé à augmenter ou réduire le niveau de sécurité d'informations étiquetées, il vous incombe de vous assurer que le besoin de modifier le niveau de sécurité des informations est légitime.

3.3. MotOrBAC

L'éditeur de politique de sécurité MotOrBAC, un outil permettant de spécifier des politiques de sécurité utilisant le modèle Or-BAC.

L'interface de programmation permet d'implémenter cette politique.

- Création d'une politique abstraite

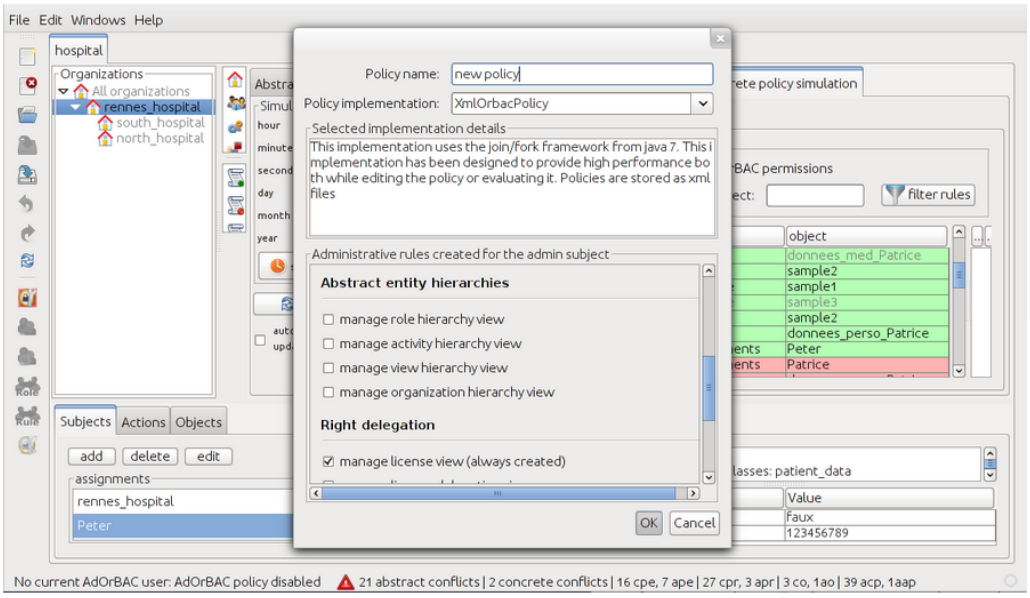

Figure 17 : création de la politique abstraite [17]

- Edition de la politique abstraire

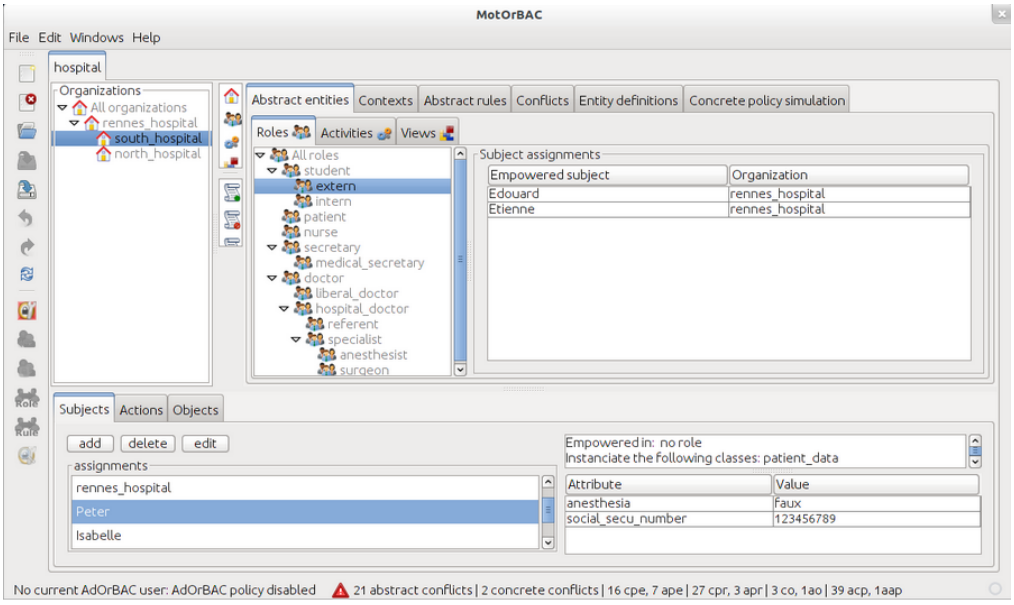

Figure 18 : Edition de la politique abstraite [17]

Editer une politique Or-BAC consiste en la définition d'une hiérarchie d'organisations ainsi que les hiérarchies de rôles, activités et vues.

Et d'autre capture qui permet de,

- spécifier les contextes, qui expriment les règles dynamiques.
- Spécification des règles abstraites, les rôles les activités et les vues.
- la gestion des conflits, MotOrBAC peut détecter les conflits abstraits et concrets, et identifier les couples de règles conflictuelles avec les couleurs. Et il peut aussi proposées des solutions à l'utilisateur pour éliminer un conflit.

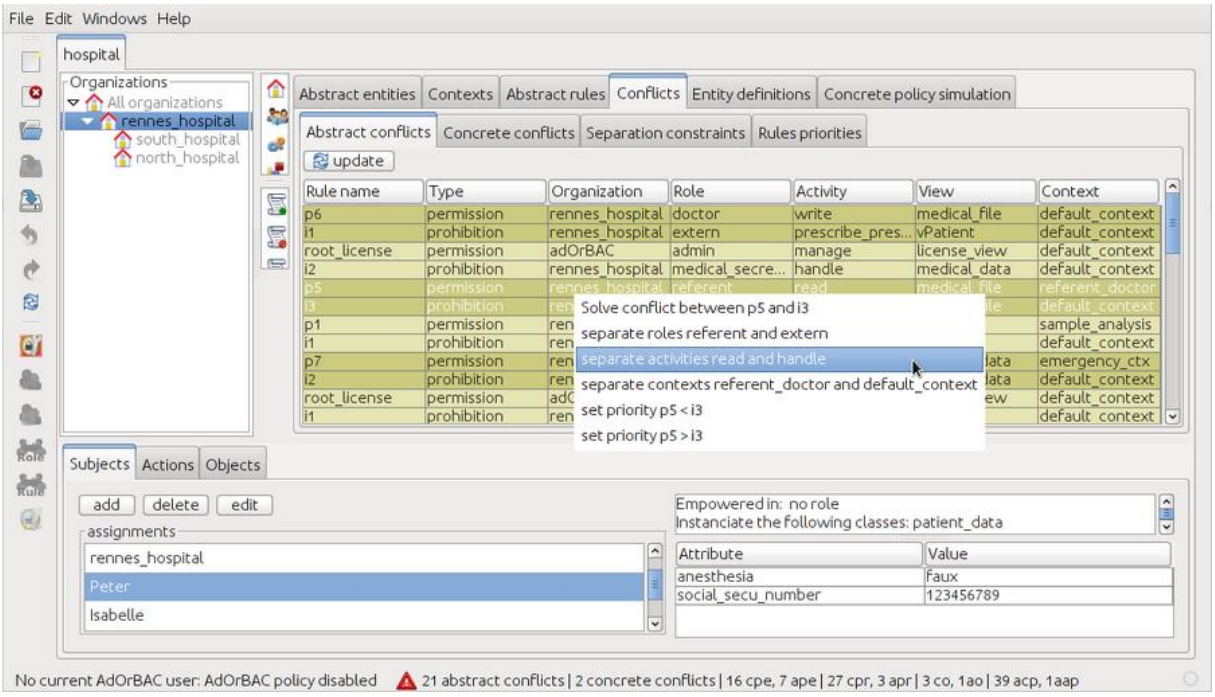

Figure 19: gestions des conflits [17]

- Définition d'entités, les entités sont utilisées pour définir des contraintes que la politique doit respecter. Par exemple, un sujet ne peut être affecté au rôle "extern" dans l'organisation "x" seulement s'il possède un attribut nommé "internat" qui a la valeur "obtenu".
- Simulation de la politique concrète, sujets, actions et objets. MotOrBAC peut afficher la politique concrète dérivée d'une politique abstraite et pour chaque règle concrète montre son état d'activation.

4. Conclusion

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

Dans ce chapitre, nous avons présenté le maximum des modèles de contrôle d'accès connus dans la littérature. Ces différents modèles permettent de spécifier si un sujet à l'autorisation de réaliser une action sur un objet du Système d'information.

Eventuellement, une condition contextuelle peut être associée à l'autorisation ; cette condition doit être satisfaite avant que l'action puisse être réalisée.

Et finalement, on a présenté quelques exemples d'implémentation réelle de ces politiques de sécurité.

Modélisation, implémentation et contribution

Partie I Modélisation et implémentation du modèle Or-BAC

1. Modélisation :

Le modèle Or-BAC est le plus utilisé dans le domaine médicale, néanmoins il répond à la pluparts des besoins de sécurité (voir tableau 5 ; chapitre 3) et il est simple à réaliser.

La notion de rôle permet de simplifier l'administration de la politique de sécurité (l'intégration des utilisateurs et la gestion des permissions), il a aussi des avantages comme l'abstraction des sujets, des actions et des objets et la prise en compte des contextes.

Dans la construction de nos politiques de sécurité, Il s'agit de déterminer précisément ce qui est permis, interdit et obligatoire dans le système. Ceci peut conduire à définir qu'une certaine catégorie d'information doit être inaccessible pour une certaine catégorie d'utilisateurs, par exemple : autoriser les agents des services payeurs à accéder aux données financières, interdire au pharmacien de créer des ordonnances... etc.

L'entité centrale dans le cas de la modélisation de la politique de sécurité liée au dossier patient est une organisation au sens Or-BAC réunissant un ensemble de professionnels de santé et de patients. Par exemple on peut considérer un hôpital comme une organisation supérieur, et chaque hôpital est organisé en services.

Le concept de rôle est indispensable dans les systèmes d'information médicale. En effet, on trouve les professionnels de santé, des personnes administratives, des patients, Pharmacien etc.

Un utilisateur peut avoir plusieurs rôles, mais il n'a pas forcément le droit de les jouer dans n'importe quelle organisation.

Dans une organisation, les sujets sont structurés en rôle. Pour cela nous avons définie « Role » comme association (figure 20).

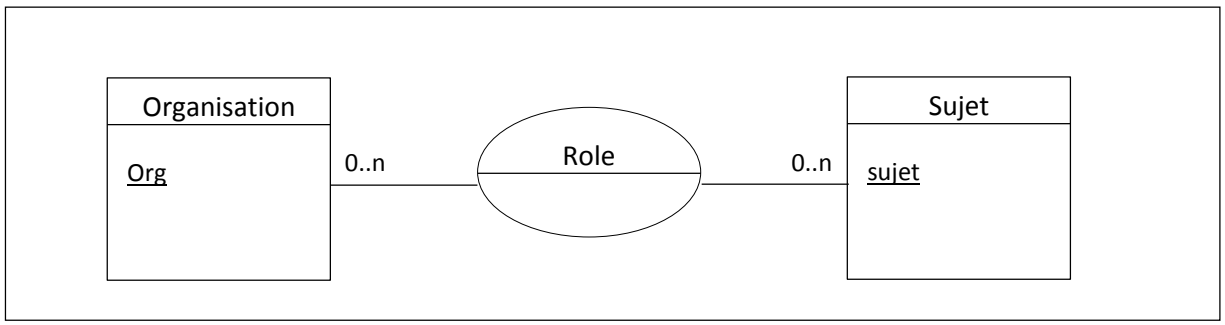

Figure 20 : Diagramme entité/association représentant l'association Rôle dans une organisation

L'attribution des droits d'accès aux documents patient se fait par le biais de la structuration en rôles qui correspond à un profil de règles de contrôle d'accès et n'a de sens que dans l'organisation où il été défini.

La gestion de la politique de sécurité est simplifiée lorsqu'on structure les éléments que l'on manipule en les abstrayant. Dans Or-BAC, les documents sont modélisés sous forme d'objets qui sont regroupés dans des vues. Cette abstraction des objets en vues permet de diminuer le nombre de règle à définir dans la politique de sécurité.

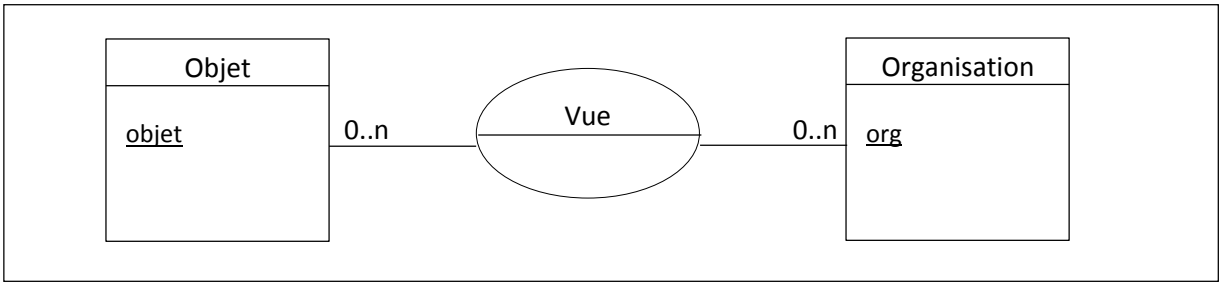

Figure 21 : Diagramme entité/association représentant les objets et les vues dans une organisation

La figure ci-dessus montre que dans une organisation ; les objets sont structurés en vues. Cette manière de structuration permet d'exprimer qu'une même vue peut être définie différemment suivant l'organisation considérée. Par exemple un hôpital X utilise un système de fichiers, et que l'hôpital Y utilise une base de données ; la vue « dossier médical » peut être définie à X comme un ensemble de documents textes, tandis qu'à Y, cette même vue correspond à des attributs ou à des tables de la base [11].

Les actions sont aussi regroupées en activité qui correspond aux divers services offerts aux utilisateurs, à titre d'exemple on cite :

- Ajouter des documents au dossier patient (Act. Ajout),
- Consulté des informations liés à un patient (Act.lecture et Act.Recherche),
- Archiver des informations (Act.Archive)
- Modifier des informations (Act.Modifier)
- Supprimer des documents (Act.Suppression)
- Imprimer des documents (Act.Impression)

On peut dire : les actions « modifier ou supprimer » un document corresponds a une activité commun « écriture »

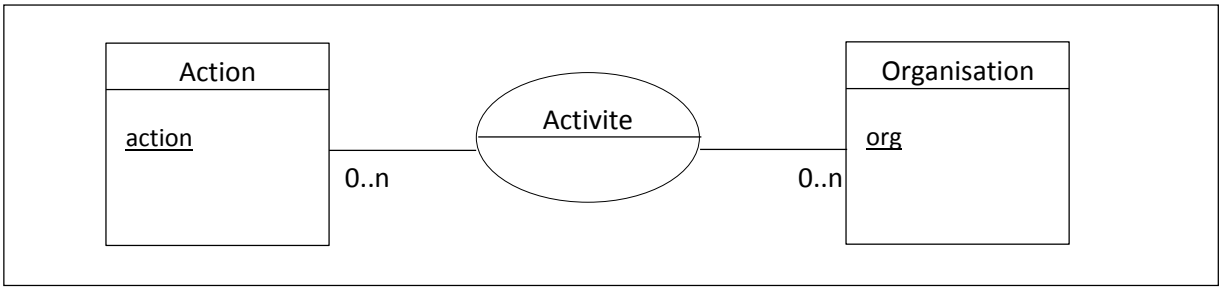

Figure 22 : diagramme entité/association représentant l'association Activité Dans une Organisation

Si nous considérons l'activité « lecture », celle-ci peut correspondre, dans une organisation X, à l'action « lire » un fichier, mais peut tout aussi bien correspondre à l'action « select » dans Y.

En plus des rôles et des groupes d'objets, nous tenons compte le contexte dans lequel la requête d'accès est faite. Pour chaque document du dossier médical, il existe des contraintes qui sont exprimées à l'aide des contextes.

- Contextes Médecin Traitant :

Dans le domaine médical, la modélisation de la notion de « traiter un patient donné » met en relation un ensemble d'utilisateurs avec un ensemble de patients. Tous les utilisateurs ayant le même rôle ne traitent pas forcément les mêmes patients, et par conséquent, ils n'ont pas les mêmes privilèges.

Par exemple, le seul fait d'être un médecin (avoir le rôle médecin) ne donne pas le droit d'accéder aux données privées des patients qu'il ne traite pas. (Médecin X traitant un patient M) et (Médecin Y traitant un patient N). Dans ce cas, l'instance X du rôle médecin possède des privilèges sur le patient M (et aucun privilège sur N), alors que l'instance Y du même rôle médecin possède des privilèges sur le patient N (et aucun privilège sur M).

- Contexte Personne Confiance Patient :

Son utilisation permet de contraindre les sujets concernés par les permissions ou les interdictions dépendant de ces contextes et qui vient réduire ou étendre les droits d'accès hérités du rôle associé.

- Contextes de type temporel :

Ce sont des contextes régissant la durée de validité des droits d'accès au dossier médical

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

- la durée pendant laquelle on peut endosser un rôle.

- Contexte Objet :

Ce contexte permet de poser des contraintes sur les documents par exemple, la durée de conservation des données doit être supérieur à 20 ans.

- Urgence :

Ce type de contexte est activé, par exemple, par le médecin chef du service des urgences dans le cas où un patient dans un état grave y est transféré. En effet, aucun traitement ne peut lui être appliqué sans consultation au préalable du dossier médical. Dans ce cas, le médecin chef de ce service est habilité à activer ce contexte pour récupérer les droits d'accès appropriés.

Anas Abou El Kalam [11] a été représenté le modèle Or-Bac par des classes associations RdO (rôle dans organisation), VdO (vue dans organisation), AdO (action dans organisation) et CdO (contexte dans organisation). La figure 24 montre qu'un utilisateur ne peut activer son rôle que dans l'organisation ou il appartient.

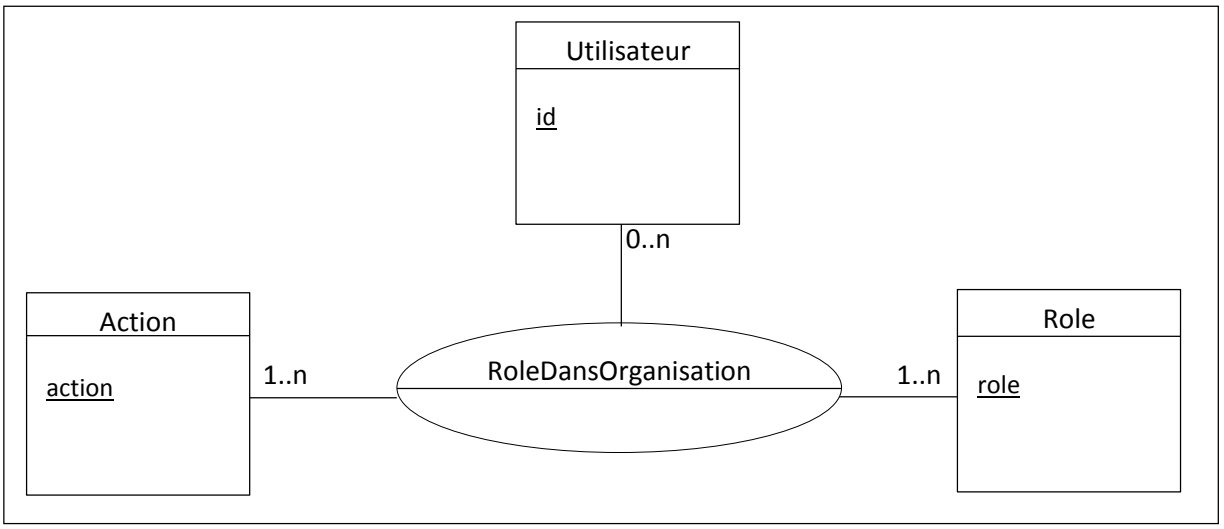

Figure 24 : l'association Rôle Dans une Organisation

Et pour les autres classes il a utilisé le même principe, Ce sont des classes associations entre l'organisation d'une part, et le rôle, la vue, l'activité et le contexte.

Selon le besoin et les niveaux d'abstraction, ces concepts peuvent servir à [11] :

- structurer les sujets, les objets et les actions par des entités abstraites ;
- identifier les rôles, vues et activités présents dans chacune des organisations du système ;

- spécifier qu'un utilisateur peut jouer différents rôles dans différentes organisations, mais pas forcément les mêmes rôles dans chacune de ces organisations ; montrer qu'une même vue peut correspondre à des objets différents selon les organisations ; montrer qu'une même activité peut être implémentée différemment dans des organisations différentes ; etc.

Le diagramme Entité/association dans la figure 25 résume notre modèle de sécurité et montre les entités et les relations utilisé dans notre base de données. Les rôles, activités, vues et le type d'accès qui correspond à une permission, obligation, interdiction sont modélisé par des classes-associations, les relations exprimé ne concerne qu'une seule organisation.

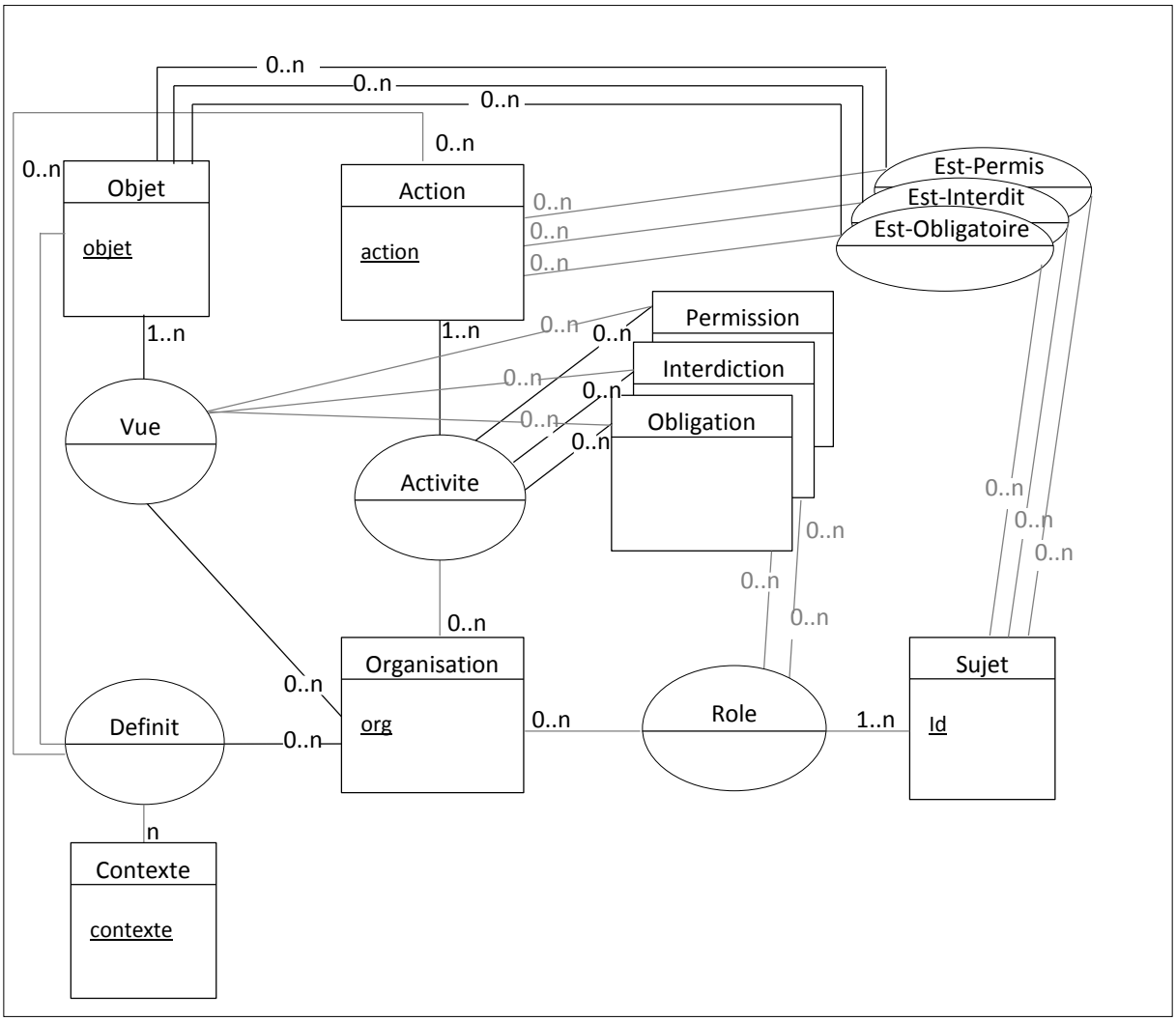

Figure 25 : Diagramme Entité/association de notre application

La relation Permission permet à une organisation donnée de spécifier les permissions accordées suivant le contexte, et le même principe pour les interdictions.

La spécification d'une politique Or-BAC se fait au niveau organisationnel (dit abstrait). La politique implantée (dite concrète) est d'dérivée de la politique organisationnelle. Cette approche rend toute politique exprimée dans le modèle Or-BAC reproductible et évolutive.

La relation définit signifier que le contexte est vrai entre un sujet une action et un objet, Les relations (Est-Permis, Est-Interdit, Est-Obligatoire) permettent à une organisation donnée de spécifier les permissions accordées Dans le but de modéliser des permissions concrètes, ces relations permettre de décrire les actions concrètes que réalisent les sujets sur les objets.

L'étape suivante est de représenter la structure de notre code orienté objet par un diagramme de classe (figure 26).

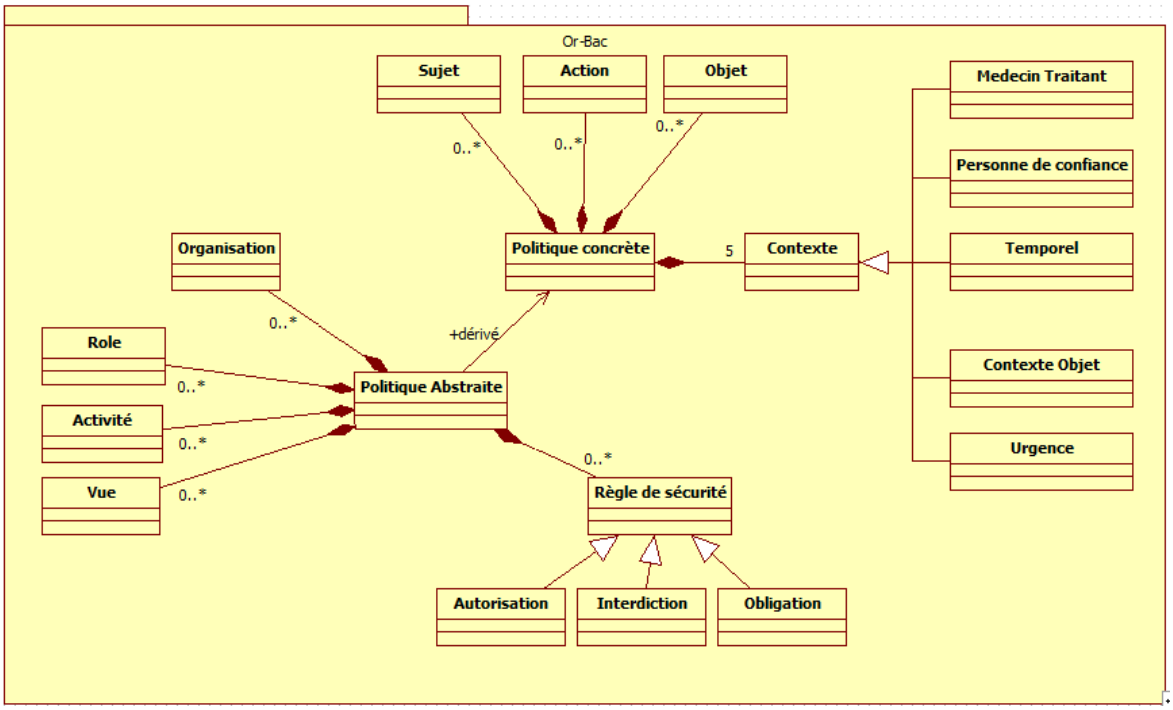

Figure 26 : Diagramme de classe de notre application

Notre modélisation montre que les éléments de politique de sécurité sont repartis en deux parties ; une politique abstraite et une politique concrète. Une politique abstraite est composé de règles de sécurité dans laquelle on donne a un rôle l'autorisation (interdiction) de réaliser une activité dans une vue, ensuite une politique concrète est dérivé de la politique abstraite ; c'est-à-dire : un sujet jouant un rôle peut réaliser une action dans cette activité sur un objet dans une vue.

Notre politique de sécurité a été codée avec le langage de programmation java. Un des principaux atouts de Java est la facilité de programmation, sa possibilité de crées des programmes robustes et surtout sa portabilité qui permet aux utilisateurs de charger dynamiquement des programmes (code mobile).

Voici quelque capture d'écran de l'interface : création de la politique Or-Bac

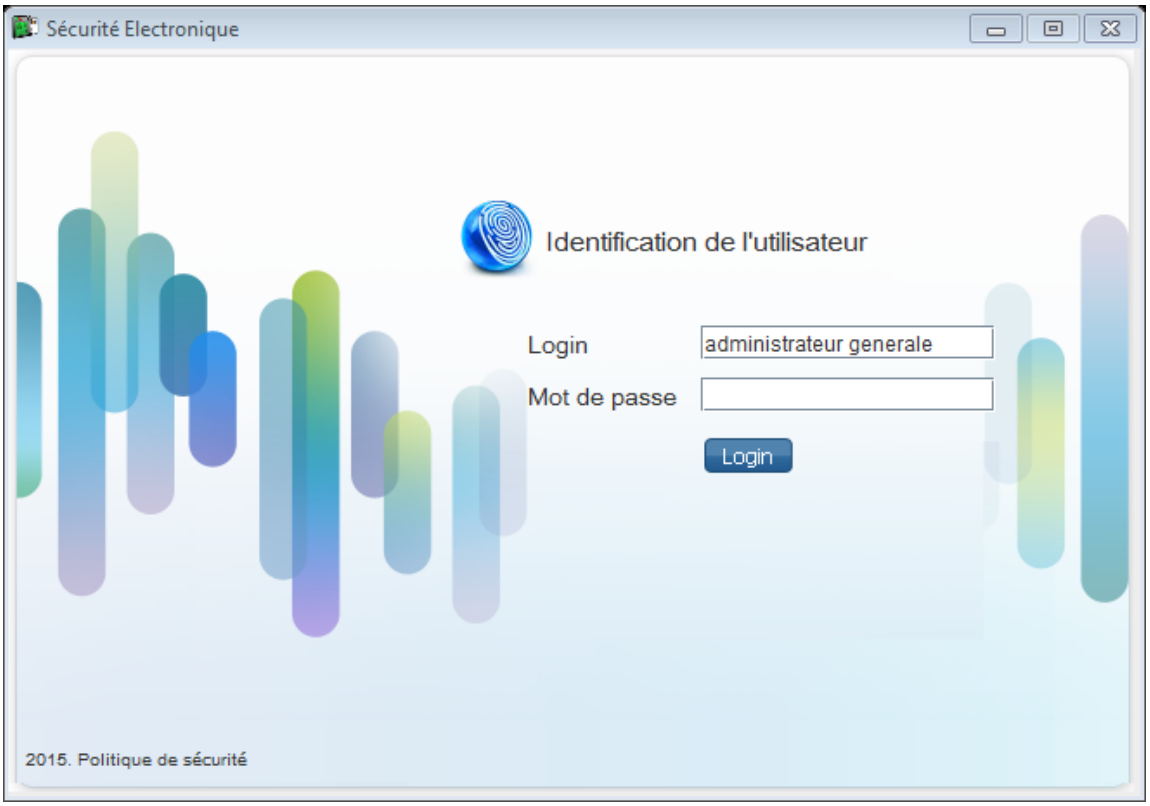

Figure 27 : phase d'identification

La Saisie d'une politique de sécurité se fait par l'administrateur ; qui peut introduire les différentes entités spécifiques au Système d'information dont il gère la sécurité (organisations, rôles, activités, vues et contextes) et les règles de sécurité associées.

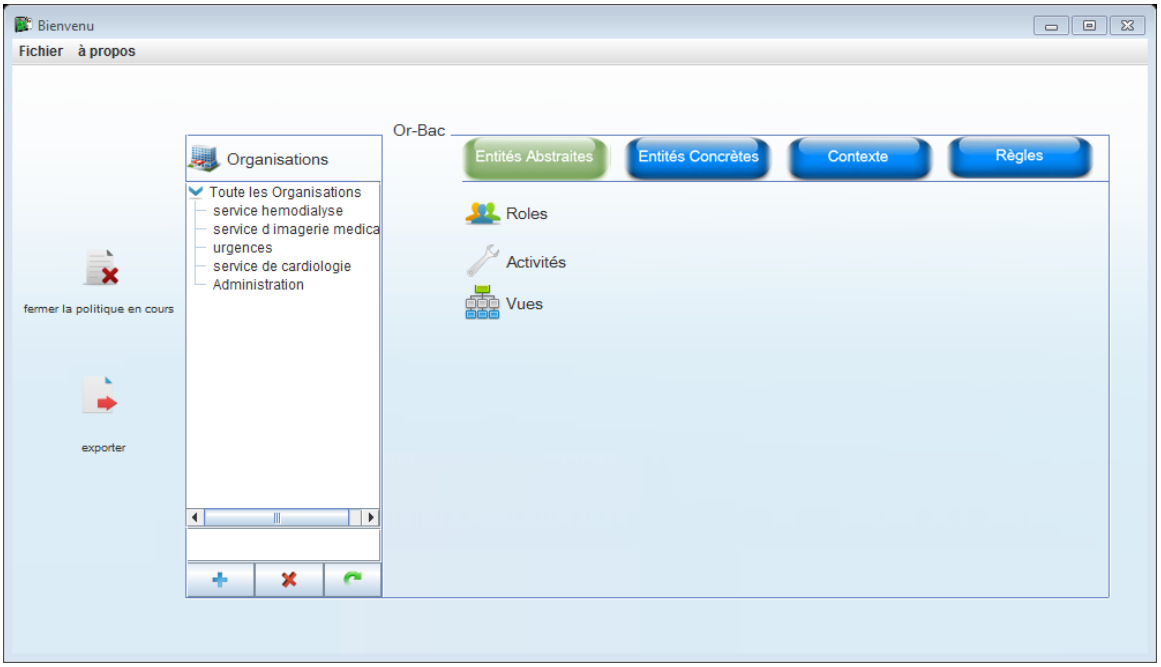

Figure 28 : Edition de la politique Or-BAC

Au moment de la création des sujets, ont associé a chaque utilisateur un rôle

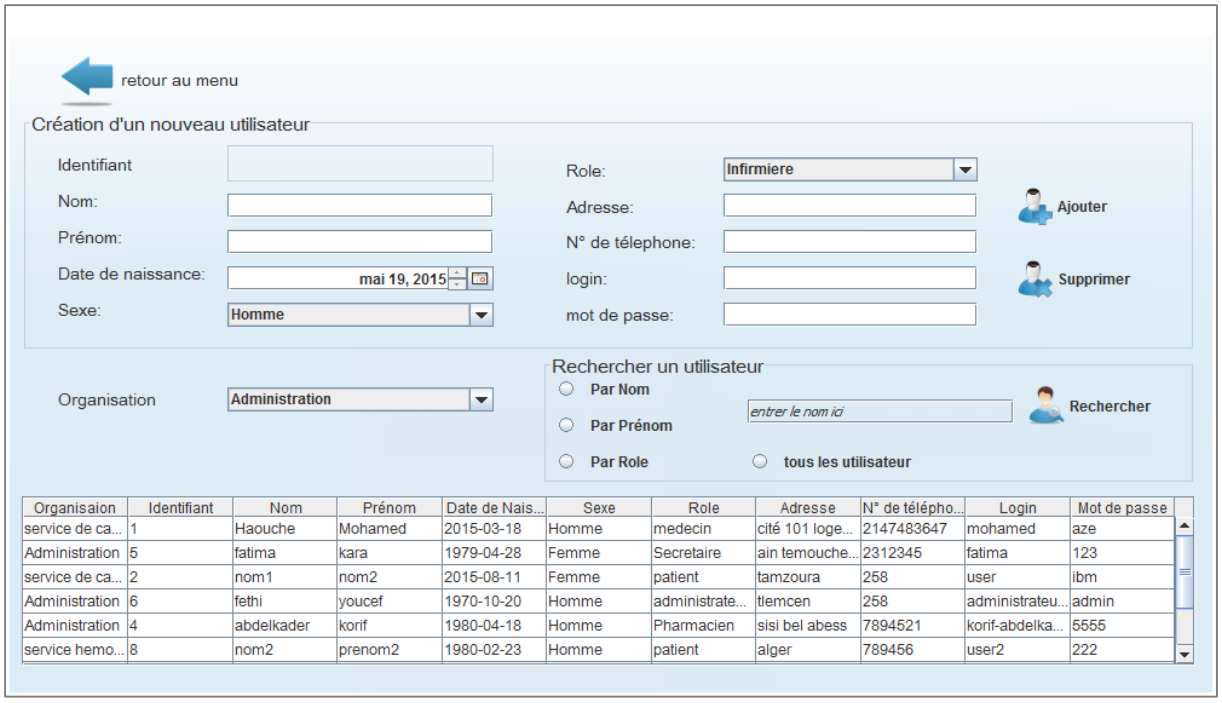

Figure 29 : création des utilisateurs

Ensuite on donne à chaque rôle un ensemble des autorisations, ce qu'est représenté dans la capture ci-dessous.

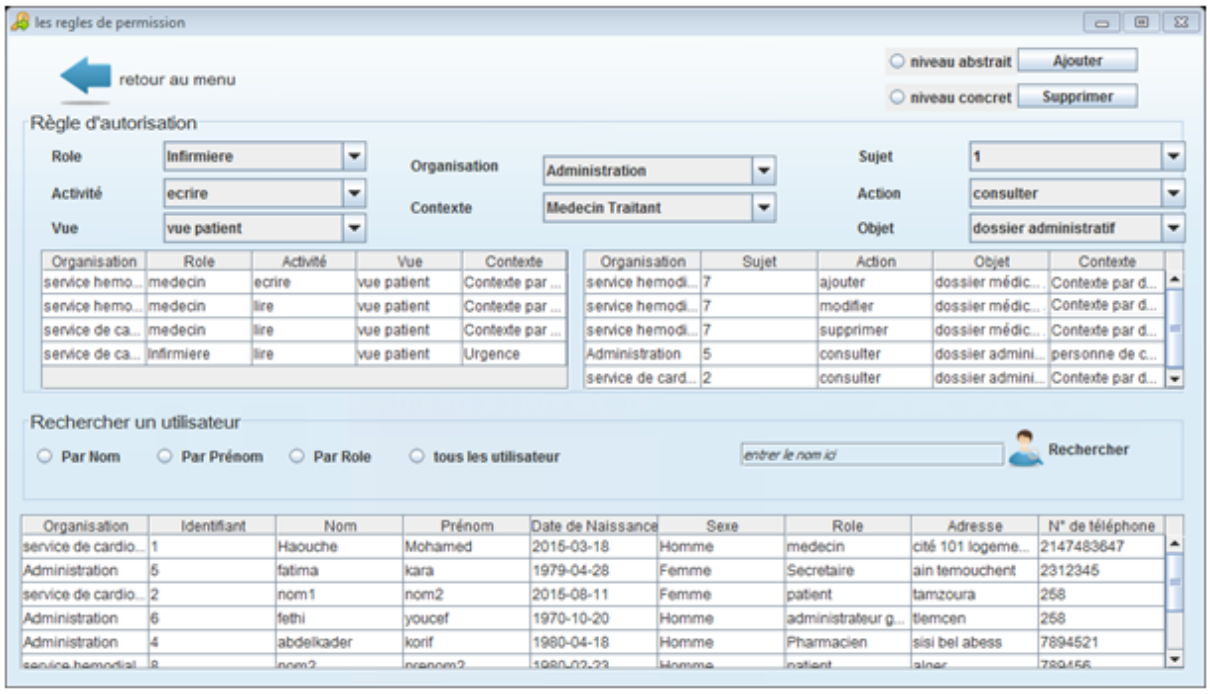

Figure 30 : politique de sécurité « règle d'autorisation »

Une règle autorisation est définit soit au niveau abstrait ; et donc un sujet jouant un rôle dans une organisation a tout le droit de réaliser une action a (dans activité) sur un objet o (dans vue) dans un contexte c. soit on peut donner directement une autorisation a un sujet spécifique.

La politique mise en œuvre considère que tout ce qui n'est pas autorisé est interdit ; dans certains cas, des interdictions sont exprimées pour renforcées par des boîtes de dialogues indiquant à l'utilisateur qu'il n'est pas autorisé à faire l'action demandée.

Les obligations sont implémentées par des actions automatiques comme par exemple : l'enregistrement de données de connexion, la conservation automatique des documents dans les antécédents …

Comme on a déjà décrit, dans le modèle Or-Bac les autorisations sont exprimer dans un contexte, on prend à titre d'exemple le contexte temporel, l'ajout d'un nouveau contexte seras ajouter automatiquement dans la classe autorisation, et après l'expiration de ce contexte il sera supprimer automatiquement par le système.

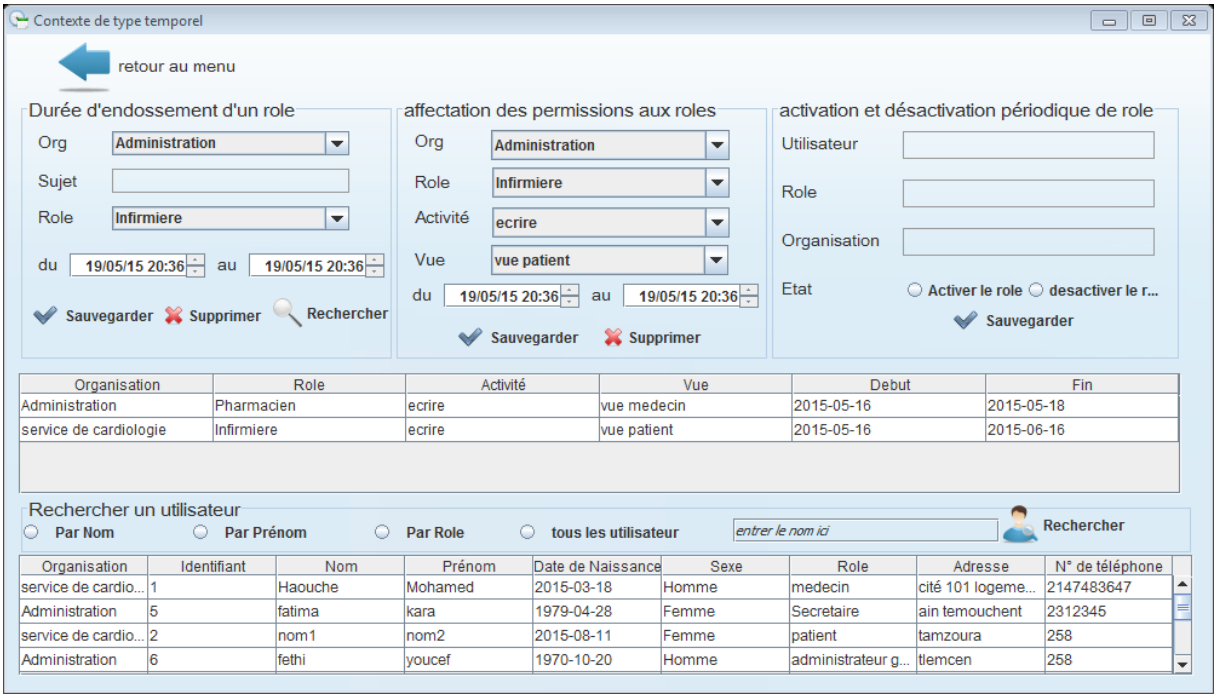

Figure 31 : contexte temporel

Partie II Contribution

1. Intégration de la politique d'accès dans une application :

Cette partie comprend notre contribution proprement dit. Dans la partie précédente, on a présenté l'interface de mise à jour de la politique d'accès. Une fois les droits d'accès définis, alors il reste maintenant comment les intégrés dans une application réelle.

A titre de prototype on va développer une simple application, dans laquelle on a deux vues (vue médecin et vue patient) et sur chaque vue on a quatre actions (voir, ajouter, modifier et supprimer).

Le tableau ci-dessous représente des exemples de droit dans ce système :

Vue	*Rôle*	*Droit*
La vue patient	patient	Peut voir que son dossier
	Médecin	- Peut voir la vue patient - sauf le médecin traitant qui peut modifier dans la vue patient -un médecin peut ajouter un nouveau patient
	Infirmière	- possède les droits de lire
	Secrétaire	- Peut voir la vue patient (sauf la partie « maladie »
	pharmacien	- Peut voir la vue patient (sauf la partie « maladie »
	Administrateur générale	- peut lire
La vue médecin	patient	- peut lire la vue patient
	Médecin	- droit de lire
	infirmière	- droit de lire
	secrétaire	- droit de lire
	pharmacien	- droit de lire
	Administrateur générale	- peut lire et écrire dans la vue médecin.

Tableau 6 : Exemple des droits d'accès

Chaque action doit être contrôlée par les règles de sécurité (permission ou interdiction), autrement, on doit tester si un utilisateur a l'autorisation de réaliser la tache demandée, si non la demande sera refusée. Ces droits sont intégrés (générés) de manière semi-automatique dans l'application source. Pour réaliser cela on a développé un outil permettant la détection automatique des évènements d'accès dans les sources (Java) de l'application en question, ce qui va nous permettre de générer les codes (java) pour le contrôle d'accès dans ces parties de code. La figure suivante (voir figure 32) présente l'interface de cet outil.

Figure 32 : Détection des points d'accès et intégration de la politique de sécurité dans une application

Les étapes de l'intégration de la sécurité sont les suivantes :

- ✓ Ajouter automatiquement les classes de sécurité.
- ✓ Détecter les parties cliquables de l'application.
- ✓ Générer la sécurité par le choix de la partie cliquable et la classe de sécurité nécessaire, une partie de code sera ajouter automatiquement. La procédure est défini par un code orienté objet comme l'indique l'exemple suivant :

```
public class securite {
        public String test="faux";
        public securite () throws Exception {
                if (requête demandée correspond a une règle d'autorisation) {
                        test="vrai";
                }
        }
}
```

```
public class application {
        public String autorisation="faux";
        public application () throws Exception {
                }
        String autorisation ;
        securite s= new securite() ;
        Public String getSecurite() {
                this.autorisation=s.test ;
                return autorisation ;
        }
        if (autorisation est vrai) { la requête demandée est accepté}
 }
```

Le diagramme de séquence ci-dessus résume le scénario de contrôle d'accès et les interactions entre les acteurs du système.

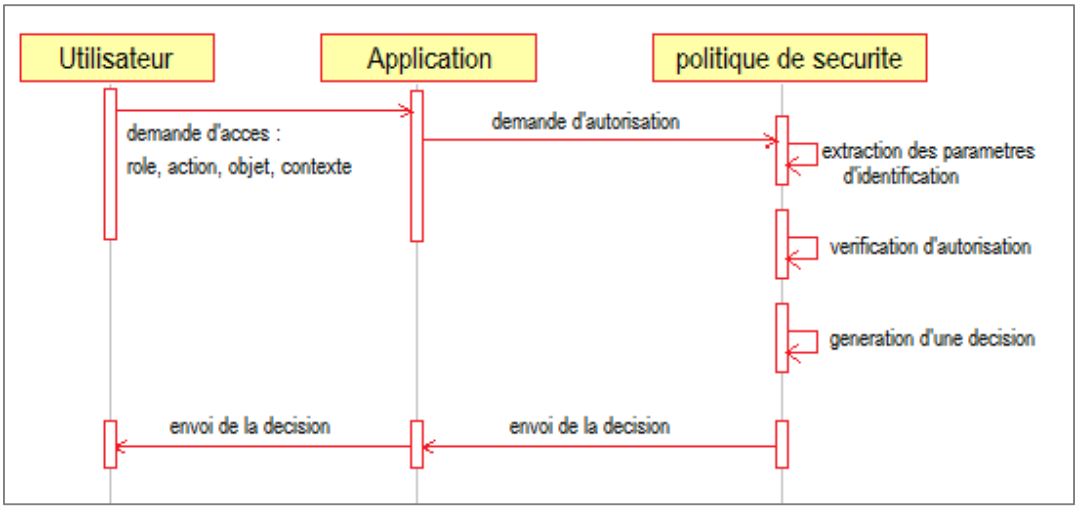

Figure 33 : contrôle d'accès à un objet

Dans cette figure l'utilisateur envoie une requête avec un ensemble de paramètres comme son rôle, l'action, l'objet et le contexte. L'application elle va envoyer une demande d'autorisation, les paramètres de la requête sont évalué dans les règles de sécurité, ensuite ; la politique de sécurité elle va envoyer une décision (est-ce-que l'action est permise ou interdite ?), qui sera envoyer à l'utilisateur. Finalement, un utilisateur ne peut effectuer que les actions qu'il a le droit d'exécuter.

2. Expérimentation :

Les captures d'écran suivantes (voir figures 34, 35 et 36) montrent le scénario en cas de non sécurisation du prototype développé:

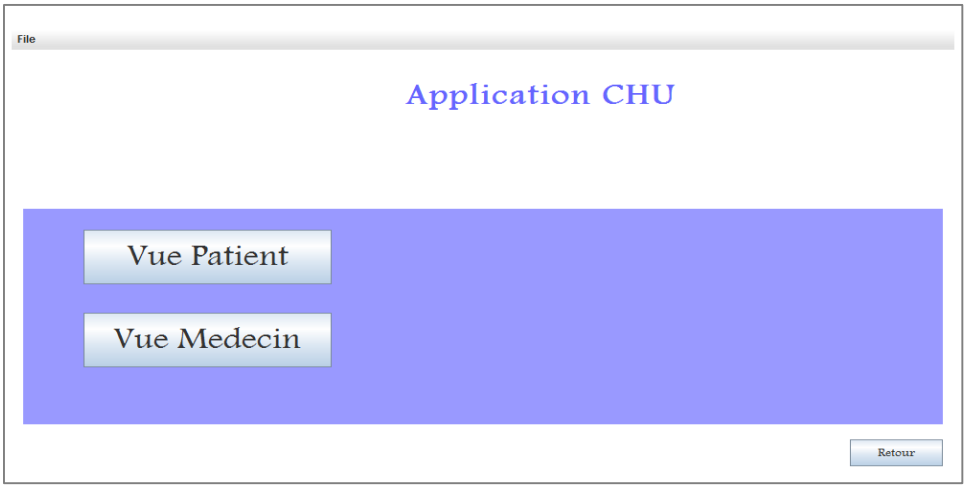

Figure 34 : menu principale

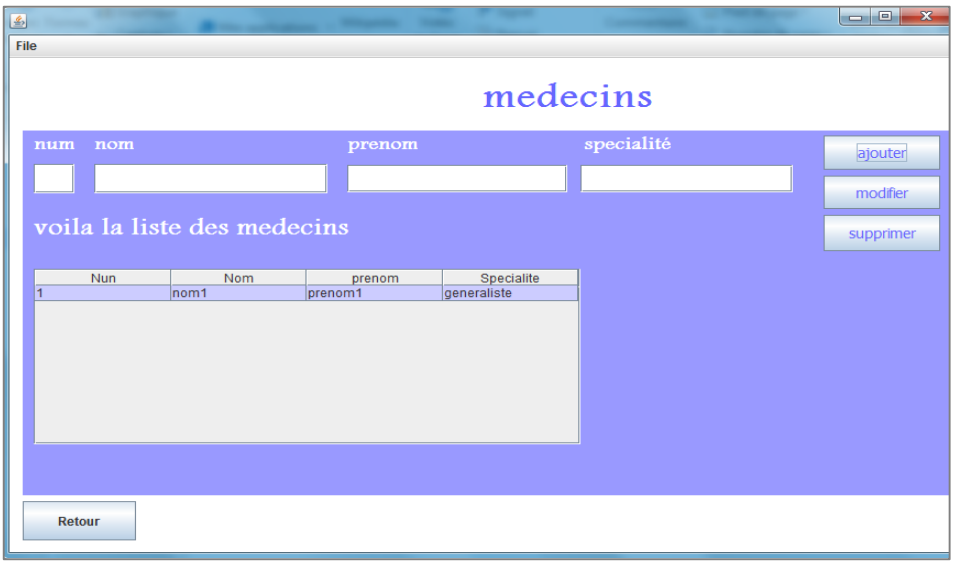

Figure 35 : la vue médecin

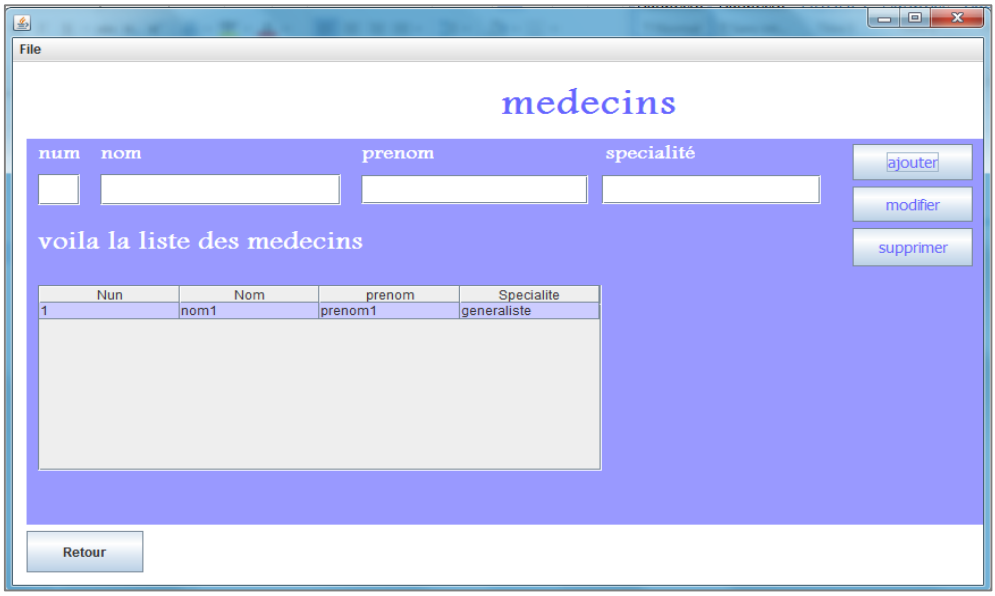

Figure 36 : la vue patient

Apres la génération automatique de la partie sécurisation, on aura tout d'abord une fenêtre d'identification (figure 37), elle permet de contrôlé dans un premier temps l'accès au menu principale de l'application. À chaque « nom de login » correspond un profil ; celui-ci est un numéro qui correspond à un rôle dans une organisation, cela permet de s'identifier, ensuite le nom d'utilisateur est mémoriser pour une prochaine identification dans l'étape de teste.

Figure 37 : Phases d'identification et d'authentification.

Si l'utilisateur connecté possède un droit définis dans la politique de sécurité, l'accès sera autorisé, si non la requête demandé est refusée. La figure 38 interdit un utilisateur de lire la vue médecin :

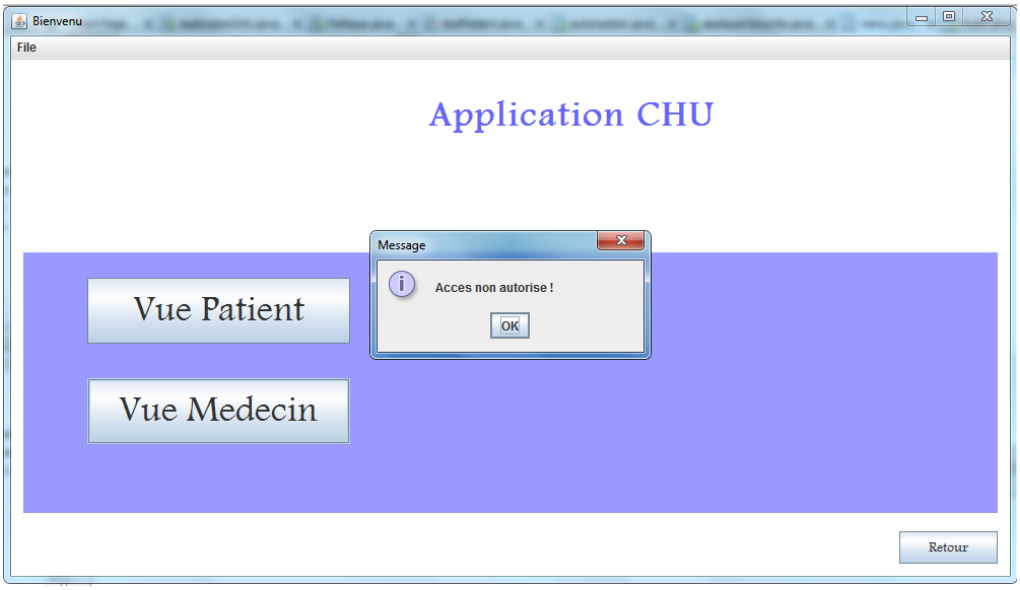

Figure 38 : un exemple d'un cas de refus d'une demande

Chaque accès à la base de données sera mémorisé, on considère cette tache comme une obligation, elle doit être activé par l'administrateur générale. Cela permet de garder une certaine traçabilité sur l'accès au système (figure 41).

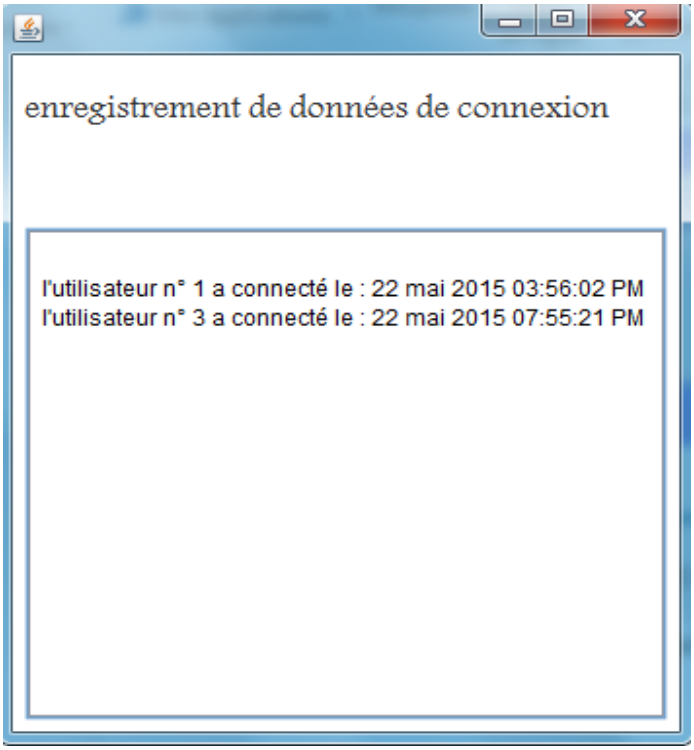

Figure 41 : enregistrement des paramètres d'accès

Conclusion :

Dans ce chapitre, nous avons montré que la définition d'une politique de sécurité est une étape nécessaire pour obtenir des systèmes pouvant satisfaire des exigences de sécurité élevées. Dans la première partie de ce chapitre nous avons choisi de modéliser et développer (implémenter) une politique de sécurité Or-Bac. Cette dernière permet d'exprimer des permissions, des interdictions et des obligations, et elle prend en compte des informations de contexte dans l'expression des règles. Dans la seconde partie de ce chapitre nous avons décrit notre contribution qui consiste à proposer une nouvelle approche automatique pour l'intégration de la politique de sécurité dans une application du domaine médical. L'outil réalisé nous a permet de validé l'approche proposée.

On compte dans l'avenir intégrer l'application sécurité comme un plugin dans les enivrements de développements intégrés comme par exemple l'IDE NetBeans ou Eclipse.

Conclusion Générale

Conclusion générale

L'accessibilité aux ressources d'information dans les systèmes de santé est un aspect très important. Le travail de ce mémoire a porté sur la protection des données médicales et plus spécifiquement sur l'implémentation d'un modèle de contrôle d'accès.

Dans ce projet nous avons dressé un état de l'art exhaustif des modèles de sécurité ce qui nous a permis de choisir objectivement le modèle le plus approprié au domaine médicale.

La concrétisation en terme d'implémentation d'un outil pour la gestion des accès dans le domaine médical nous a permis d'appréhender les concepts liés à la modélisation des systèmes de sécurité des données et plus particulièrement les concepts du modèle de contrôle d'accès à base d'organisation. Ce qui nous a finalement permet de dévoiler l'importance d'un modèle de contrôle d'accès pour sécuriser une application.

La validation de l'approche proposée en termes d'un ensemble de classes Java à intégrer dans une application, constitue notre modeste et propre contribution dans ce domaine.

En fin, même si le travail présenté nous a permis de sécuriser un prototype d'une application du domaine médicale, beaucoup de choses restent à réaliser, et plusieurs perspectives de recherches peuvent être distinguées. On souhaite dans l'avenir :

- travailler sur une application à grandeur réelle,
- proposer une approche pour l'intégration automatique de la politique, au lieu d'une intégration semi-automatique,
- implémenter d'autres modules d'Or-Bac comme les recommandations, la traçabilité de tout utilisateur réalisant une action dans le système et la gestion des conflits.

Référence Bibliographique :

[1] Amal HADDAD « modélisation et vérification de politiques de sécurité », Université Joseph Fourier, Genève. Stage effectué au laboratoire LSR, équipe VASCO du 8 novembre 2004 au 7 Septembre 2005.

[2] BELLAL Toufik «Expression d'une politique de sécurité dans un réseau social » Janvier 2010 : 8

[3] ORBAC : un modèle de contrôle d'accès basé sur les organisations
Anas Abou El Kalam, Yves Deswarte, Rania El Baida, Philippe Balbiani, Frédéric Cuppens, Salem Benferhat, Alexandre Miège , Claire Saurel, Gilles Trouessin.
http://irt.enseeiht.fr/anas/document/03Revue-InfoSyst.pdf (Consulter le 08/06/2015)

[4] Saida Medjdoub ; Modèle de contrôle d'accès pour XML : « Application à la protection des données personnelles » Présentée et soutenue publiquement Le 8 décembre 2005 ;
HAL Id: tel-00340647; https://tel.archives- ouvertes.fr/tel- 00340647; Submitted on 21 Nov 2008 :p10

[5] Sofiene Boulare « Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès » , Université du Québec en Outaouais, Aout 2010 : 15

[6] Thomas DEMONGEOT « Politique de contrôle de flux d'information de définie par les utilisateurs pour les orchestrations de services ». Mise en œuvre dans un orchestrateur BPEL. Soutenue le 19 décembre 2013.HAL Id: tel-00959447 :26-29

[7] Alban Gabillon « Contrôle d'accès – Contrôle de flux – Contrôle d'usage – Le projet ANR FLUOR ». Université de la Polynésie Française. (2007 – 2010)

[8] Catalin Dima. « Introduction à la sécurité » – Cours 11 Modèles de flux d'information: 9, http://lacl.u-pec.fr/dima/securite/secu10.pdf consulté le (05/06/2015)

[9] Ferraiolo, David F. and Kuhn, D. Richard (1992): Role-Based Access Controls. In: 15th National Computer Security Conference October 13-16, 1992

[10] Marwan CHEAITO « Un cadre de spécification et de déploiment de politiques d'autorisation » Le 09/03/2012 ; Délivré par l'Université Toulouse III - Paul Sabatier : 30-31

[11] Anas ABOU EL KALAM Docteur de l'Institut National Polytechnique de Toulouse
Thèse « MODÈLES ET POLITIQUES DE SECURITE POUR LES DOMAINES DE LA SANTE ET DES AFFAIRES SOCIALES » Année 2003, Rapport LAAS N° LAAS ??CNRS 7, avenue du Colonel Roche 31077 Toulouse Cedex 4

[12] (Anas Abou El Kalam — Yves Deswarte), « Modèle de sécurité pour le secteur de la santé » LAAS-CNRS, 7 avenue du Colonel Roche — 31077 Toulouse Cedex 4 — France, page 7.2004

[13] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel et G. Trouessin. Organization Based Access Control. IEEE 4th International Workshop

on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.

[14] Frédéric Cuppens et Alexandre Miège ENST Bretagne « Or-BAC Organisation Based Contrôle » , Campus de Rennes. 2, rue de la Chataigneraie 35576, Cesson Sévigné CEDEX http://www-smis.inria.fr/~bouganim/CASC/Publications/ENST_Druide_2004_Or-BAC.pdf consulter le (08/06/2015)

[15] http://olsc.org/m34-securite-linux/2013/11/26_securite-linux-vue-densemble.html (Consulté le 18/02/2015)

[16] Guide de l'utilisateur Oracle Solaris Trusted Extensions https://docs.oracle.com/cd/E26919_01/html/E25056/docinfo.html#scrolltoc (Consulté le 18/02/2015)

[17] le site de MotOrBAC! http://motorbac.sourceforge.net/index.php?page=home&lang=fr (Consulté le 18/02/2015)

[18] Définition dans le dictionnaire - Linternaute.

www.linternaute.com/encyclopedie/recherche/id-195/?f_libelle=confidentialité

(Consulté le 08/06/2015)

[19] Rapport de séminaire réalisé par un groupe de 10 élèves en formation initale. Animateur Franck LE DUFF « le dossier médicale informatisé : limites éthiques et contraintes professionnelles liées au partage des données médicales ». Thème n°23, année 2001 :4

[20] Comité éditorial pédagogique de l'UVMaF « Le dossier médical ». Support de Cours. Université Médicale Virtuelle Francophone. 2011-1012 : 3

[21] code de la santé public. Article L1110-4.
Modifié par LOI n°2011-940 du 10 août 2011 - art. 2

[22] Code pénal - Article 226-13 : Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

[23] Code de la santé publique - Article L1111-7, Modifié par LOI n°2011-803 du 5 juillet 2011 - art. 9

[24] Dossier médical - Service-public.fr, Mise à jour le 24.11.2014 - Direction de l'information légale et administrative (Premier ministre), http://vosdroits.service-public.fr/particuliers/F12210.xhtml (consulté le 20/02/2015)

[25] http://www.uvp5.univ-paris5.fr/staticmed/e-dosmed/cours/dossier%20patient/references/Avantages.html (consulté le 20/02/2015)

[26] Santé - CNIL - Commission nationale de l'informatique et des libertés
Fiche pratique Sous-traitance : Modèles de clauses de confidentialité, 02 mai 2011

« Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »

[27] Fiche pratique : Le Dossier Médical Personnel et la sécurité – Juin 2011, p : 2-8

[28] Introduction à la sécurité informatique- Non-répudiation de l'origine http://moodle.utc.fr/pluginfile.php/16777/mod_resource/content/0/SupportIntroSecu/co/CoursSecurite_1.html (consulté le 22/02/2015)

[29] Khalid BOURICHE, THÈSE Doctorat: « Gestion de l'incertitude et codage des politiques de sécurité dans les systèmes de contrôle d'accès ». Centre de Recherche en Informatique de Lens – CNRS UMR 8188 Université d'Artois, rue Jean Souvraz, S.P. 18 F-62307 http://www.cril.fr et Faculté des Sciences et Techniques Fès B.P. 2202, Route d'Imouzzer FES www.fst-usmba.ac.ma :18

[30] Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel : livre « Cryptographie et sécurité des systèmes et réseaux » ©LAVOISIER, 2006 ISBN 2-7-462-1260-9 : 103-105

[31] chapitre 10 « La sécurité des réseaux » Reseaux-CH-10 Mercredi, 8. novembre 2006 9:49 09