République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

Université des **S**ciences et de la **T**echnologie d'**O**ran **M**ohamed **B**oudiaf

Faculté des Mathématiques et Informatique **D**épartement d'Informatique

THÈSE

En vue de l'obtention du

Diplôme de Doctorat

Présentée et Soutenue par :

ZERKOUK Meriem

Intitulée

Modèles de contrôle d'accès dynamiques

Soutenue le : 22 Novembre 2015

Domaine	*: Mathématiques et Informatique*
Spécialité	*: Systèmes Informatiques et Réseaux*
Intitulé de la Formation	*: Informatique*

Le jury est composé de :

Grade, Nom &Prénom	*Statut*	*Domiciliation*
Professeur, FIZAZI Hadria	*Président*	*U.S.T.O MB*
Professeur, CHOUARFIA Abdallah	*Rapporteur*	*U.S.T.O MB*
Professeur, M'HAMED Abdallah	*Co-Rapporteur*	*Ecole Télécom SudParis*
Professeur, Feham Mohamed	*Examinateur*	*Univ Tlemcen*
Professeur, Hadj Said Naïma	*Examinateur*	*U.S.T.O MB*

Année Universitaire 2015 / 2016

Thèse réalisée au Département d'informatique
Faculté des Mathématiques et Informatique
Université des Sciences et de la Technologie d'Oran
- Mohamed Boudiaf (U.S.T.O-MB)

BP 1505 El M'Naouar Bir el Djir 31000
Oran, 31000, Algérie

`http://www.univ-usto.dz/mathinfo/presentation.php`

Présentée par ZERKOUK Meriem meriem.zerkouk@univ-usto.dz

Sous la direction de : MESSABIH Belhadri messabih@univ-usto.dz
MHAMED Abdallah abdallah.mhamed@telecom-sudparis.eu
CHOUARFIA Abdallah chouarfia@univ-usto.dz

Étude de cas réalisée dans Département RST (Réseaux et Services de Télécommunications)
et Département EPH (Electronique et PHysique)
Ecole Télécom SudParis - France

Travaux scientifiques

Conférences internationales avec acte et comité de lecture

1. Zerkouk, M., M'hamed, A., Messabih, B., User Behavior and Capability Based Access Control Model and Architecture in Proc (Springer) of the Fourth International Conference on Networks & Communications, Volume 131, 2013, pp 291-299.

2. Mhamed, A., Zerkouk, M., El Husseini, A., Messabih., B., El Hassan, B., Towards a Context Aware Modeling of Trust and Access Control Based on the User Behavior and Capabilities, in Proc ICOST 2013, LNCS 7910, pp. 69–76, 2013.

Journaux internationaux avec acte de lecture

1. Zerkouk, M., M'hamed, A., Messabih, B., A User Profile Based Access Control Model and Architecture. In : I. J. Computer Networks & Communications, Vol 5, N° 1, pp. 171—181 (2013).

2. Zerkouk, M., Cavalcante, P., M'hamed, A. Boudy, J., Messabih, B., Behavior and Capability based Access Control Model for Personalized TeleHealthCare Assistance, J. Mobile Networks & Application, DOI : 10.1007/s11036-014-0516-9, (2014).

Remerciements

Louange à Dieu Tout Puissant de m'avoir donné courage et patience pour mener à bien cette thèse.

Mes tous premiers remerciements vont à mes encadreurs, Mrs. MESSABIH Belhadri, M'HAMED Abdallah et CHOUARFIA Abdellah pour m'avoir initiée à la recherche, conseillée et orientée le long de ce travail. Je leur exprime ici toute ma gratitude et ma reconnaissance.

Je remercie également les membres du jury : Mme. FIZAZI Hadria pour l'honneur d'avoir accepté de présider le jury ; Mme. HADJ SAID Naima et Mr. FEHAM Mohamed pour l'honneur d'avoir accepté d'examiner ma thèse.

Mes remerciements vont également à :

- L'équipe du Laboratoire SIR de l'USTO au sein duquel j'ai évolué.
- L'équipe du Département EPH (Université Télécom SudParis), pour leur très bon accueil durant mon stage et leur fructueuse collaboration.

Je tiens à exprimer à tous mes enseignants, chacun en son nom, toute ma reconnaissnce, vénération et respect pour leur contribution inéstimable à ma formation.

Je termine par un chaleureux remerciement à mes parents, ma soeur et mes frères pour leur amour, leur soutien inconditionnel et avec qui j'ai partagé toutes mes peines et joies.

Résumé

L'émergence de l'intelligence ambiante et de la sensibilité au contexte ont favorisé le déploiement des services dans les environnements dédiés aux personnes dépendantes (âgées ou déficientes). Les applications sensibles au contexte contribuent significativement à l'amélioration de la qualité de vie de ces personnes en termes d'autonomie et de sécurité. Néanmoins, l'accessibilité à ces services reste assez limitée et ne peut se concevoir sans la prise en considération des capacités de ces personnes. Par conséquent, la modélisation des politiques de sécurité constitue un défi majeur dans la conception de modèles de contrôle d'accès pour une gestion dynamique et personnalisable des services selon le profil utilisateur. La mise en place d'une politique de sécurité au niveau des systèmes intelligents a eu toujours recours aux modèles de contrôle d'accès dynamiques où l'assignation des droits d'accès est liée à la validité du rôle et du contexte. Cependant, les données contextuelles utilisées ne permettent pas de résoudre tous les verrous liés aux exigences de la sécurité. Les modèles existants sont inadaptés en raison du manque de flexibilité, de personnalisation et d'adaptabilité à la capacité et au comportement de l'utilisateur. Pour remédier à ces insuffisances, l'incorporation de données contextuelles riches et complexes est nécessaire. D'où, le besoin d'exploiter une architecture sensible au contexte munie des modules d'acquisition, de modélisation, de raisonnement et d'adaptation.

Le travail effectué dans cette thèse porte sur la conception d'une politique de sécurité mise en place par un modèle de contrôle d'accès basé sur le comportement et les capacités des utilisateurs dans les environnements intelligents UBC-ACM (User Behavior Capability based Access Control Model) et développée au moyen de l'architecture UBC-ACA (User Behavior Capability based Access Control Architecture). L'assignation des droits d'accès est basée sur l'analyse et le suivi du comportement ainsi que l'extraction des profils et les situations critiques vécues par l"utilisateur. Le processus de contrôle d'accès est composé de les phases suivantes:

- L'extraction des comportements selon le degré de la sensibilité des situations au moyen d'un processus d'apprentissage.
- La génération d' un modèle de contrôle d'accès dynamique basé sur les comportements, les profils et les capacités.
- Le raisonnement intelligent basé sur l'intégration des résultats d'apprentissage afin d'extraire les droits d'accès les plus appropriés vis à vis des besoins des personnes agées dépendantes.
- La prise de décision effectuée par l'exploitation des résultats inférés.

Finalement, notre politique de sécurité a été validée avec des données acquises d'une plate forme de télé-vigilance munie de capteurs ubiquitaires et portables.

Mots clés : Modèles de contrôle d'accès, sensibilité au contexte, comporte-

ment, capacité d'utilisateur, modélisation, raisonnement.

Dynamic access control models for pervasive systems

Abstract

The emergence of ambient intelligence and context awareness favored the deployment of services in dedicated environments for the dependents people (elderly or deficient). The context-aware applications contribute significantly to improve the life quality of these people in terms of autonomy and safety. However, the access to these services remains limited enough and can not be understood without consideration of the capacity of these people. Consequently, the security policy modeling is a major challenge in the design of access control models for dynamic and personalized service management according to the user profile. The implementation of the security policy into intelligent systems had always used dynamic access control models where the access rights assignment rely on the validity of the role and the context. However, contextual data used do not solve all the locks associated with the security requirements. The existing models are inadequate because of the lack of the flexibility, the personalization and the adaptability to the capacity and the user behavior. To remedy these shortcomings, the incorporation of rich and complex contextual data is needed. Hence, the need to operate a context aware architecture provided with the acquisition modules, modeling, reasoning and adaptation.

The work done in this thesis focuses on the design of a security policy implemented by an access control model based on the behavior and user capabilities in smart environments UBC-ACM (User Behavior based Access Control Capability Model) and developed by UBC-ACA architecture (User Behavior based Access Control Architecture Capability). The assignment of access rights is based on the analysis and monitoring of the behavior and the extraction profiles and critical situations experienced by the user. The access control process is composed of the following phases:

- The extraction of behaviors depending on the degree of sensitivity situations through a learning process.

- The generation of dynamic access control model based on the user behavior, profiles and capabilities.

- The intelligent reasoning based on the integration of learning outcomes in order to extract the most appropriate access rights with respect to the needs of dependent elderly.

- The decision made by the use of the inferred knowledge.

Finally, our security policy has been validated with the data acquired from a tele-vigilance platform equipped with ubiquitous and wearable sensors.

Keywords : Tele-healthcare, tele-monitoring, assistive living, access control, classification, context awareness, user behavior , user capability, user profile, modeling, reasoning, querying.

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Problématique

Les travaux de recherche dans le domaine de télé-médecine, au cours de la dernière décennie, une grande importance a été consacrée au développement des applications orientées santé et bien être des personnes dépendantes (âgées, déficientes).

Le développement rapide des technologies de communication, des réseaux mobiles et des dispositifs ubiquitaires, a favorisé l'émergence des technologies de détection, ce qui a favorisé le déploiement d'applications sensibles au contexte. Les systèmes de santé ont largement exploité le concept de « context aware computing (informatique contextuelle)» pour surveiller, de façon préventive, les conditions de santé et les activités physiques afin de détecter toute situation indésirable portant atteinte à la santé et la sécurité de ces personnes. Ces systèmes ont acquis un degré élevé d'intelligence grâce à l'intégration du paramètre contextuel lors des procédures de surveillance et d'assistance. La fourniture de services (gestion de confort et de sécurité) répond aux exigences des personnes dépendantes (âgées, déficientes) sans être limitée par le temps ou l'emplacement « any where, any time » car le taux de cette population augmente rapidement et ce flux émergeant a attiré l'attention des développeurs pour rendre leurs espaces de vie plus intelligents, confortables et sécurisés. Grâce à l'hétérogénéité, la dynamicité et l'interopérabilité des dispositifs embarqués dans l'environnement, l'évolution des systèmes pervasifs et la fourniture de services ont ouvert de nouveaux horizons lors de la mise en place du service de sécurité. La gestion des services est basée sur les techniques d'intelligence artificielle dans le but d'extraire puis d'identifier les situations et les besoins des personnes en termes de sécurité.

Malgré les efforts consentis dans ce domaine, nous avons constaté que des contributions importantes peuvent être apportées notamment en matière de mise en place de systèmes de santé installés dans des habitats intelligents, adaptatifs et personnalisés aux besoins des personnes dépendantes. Dans cette thèse, on s'intéresse à la sécurité comme élément clé au niveau d'un système de santé sensible au contexte où les données manipulées sont de plus en plus hétérogènes et dynamiques. Plus précisément, une étude particulière est consa-

crée au contrôle d'accès comme service de sécurité ; celui-ci revêt un aspect clé dans un système intelligent dans la mesure où il sert à contrôler tout accès aux services et/ou aux ressources pour garantir le confort et la sécurité aux personnes. Afin de remédier aux insuffisances constatées, on a choisi de résoudre cette problématique via la mise en place d'un modèle de contrôle d'accès dynamique. La conception d'un nouveau modèle de contrôle d'accès nécessite l'identification des exigences des patients utilisant les systèmes de surveillance et assistance. Par ailleurs, il est nécessaire de distinguer les exigences des systèmes de santé spécifiquement en termes de sécurité (Authentification et/ou Autorisation). Dans la littérature, les modèles de contrôle d'accès existants sont généralement destinés à contrôler l'accès aux informations des personnes. Traditionnellement, la sécurité est assurée par les modèles de contrôle d'accès et plus particulièrement le modèle RBAC et ses extensions. Ce modèle gère l'attribution des droits d'accès suivant les rôles que l'utilisateur exerce et la validité du contexte. Divers travaux de recherche ont proposé l'extension du modèle RBAC en tenant compte des changements détectés dans l'environnement selon les aspects temporels, géographiques et ambiants (température et bruit). Néanmoins, ces extensions ne peuvent répondre que partiellement à nos exigences en raison de leurs insuffisances liées aux aspects suivants : politique, modèle et architecture.

Politique : La politique de RBAC est à la base de toutes les approches de gestion des nouveaux besoins de sécurité introduits par la forte dynamicité et l'hétérogénéité des dispositifs mobiles qui caractérisent les environnements pervasifs et dynamiques. Cependant, la gestion des droits d'accès en rôles ne permet pas d'assurer une meilleure attribution des droits d'accès dans les différents types d'environnements pervasifs (maison intelligente, hôpital, entreprise).

La conception d'une politique de sécurité personnalisée exige la manipulation des données personnelles d'où la nécessité de préserver la vie privée des utilisateurs en intégrant cette caractéristique dans les différentes extensions du modèle RBAC.

Parmi les insuffisances au niveau de la conception d'une politique de sécurité, on peut citer :

- La détection d'une faiblesse au niveau de la conception des politiques de sécurité qui ne tiennent pas compte des différents aspects : la préservation de la vie privée, la gestion de la confiance et la sensibilité au contexte liée aux données issues de sources multiples.

- Le manque de meilleure identification de la personne en prenant en compte son historique qui peut servir à la gestion de l'anonymat et de la confiance des utilisateurs.

- Le manque de personnalisation et de d'adaptabilité spécialement lors de l'assurance de la sécurité aux personnes ayant une capacité limitée.

- Le manque de modèle gérant la sécurité et la sûreté des personnes dépendantes situées dans un espace intelligent.

Modèle : Actuellement, la sécurité est fondée sur les extensions du modèle RBAC ; celles-ci sont développées suivant les besoins des systèmes auxquels elles sont destinées. Lors de l'application de ces modèles au niveau d'un système de santé, différentes insuffisances sont identifiées car les données contextuelles sur lesquelles on raisonne sont limitées à l'environnement (localisation, temps, ..). Par conséquent, la modélisation de la politique de sécurité dans un format standardisé est essentielle et la prise en compte de l'aspect sémantique est obligatoire pour gérer l'hétérogénéité des données.

Architecture : La gestion de personnalisation et d'adaptation dans un modèle de contrôle d'accès exige la prise en compte des données contextuelles multi sources issues de capteurs portés par l'utilisateur et/ou embarqués dans l'environnement. Pour cela, on note qu'une architecture propre aux modèles de contrôle d'accès dynamiques est nécessaire pour assurer l'acquisition, la modélisation, le raisonnement et l'adaptation. Dans cette thèse, on cherche à remédier aux problèmes identifiés et d'introduire une politique de sécurité adaptative et personnalisée aux personnes âgées dépendantes. Les défis majeurs rencontrés lors de la conception d'un modèle de contrôle d'accès dynamique, sont principalement liés aux types de dispositifs exploités pour capturer toutes sortes de données contextuelles qui servent à suivre l'utilisateur dans sa vie quotidienne. Notre objectif est de développer un modèle de contrôle d'accès basé sur le comportement et le profil (capacité) de l'utilisateur générés par l'application d'un processus d'extraction de connaissances à partir de l'enregistrement de traces (historique). Afin de gérer toute cette diversité de connaissances, on a eu recours aux technologies du web sémantique en termes de modélisation et de raisonnement.

Dans ce travail, on s'intéresse à l'adaptation des services demandés aux besoins des patients (âgés, déficients). Cependant, on a ciblé les Objets de Recherche (OR) suivants :

OR 1 : La gestion d'un système sensible au contexte doit exploiter une variété de capteurs pour raisonner sur des données complexes (comportement, profil, habitudes, situations, activité).

OR 2 : La création d'un modèle de contrôle d'accès doit tenir en compte le profil et le comportement des patients afin d'assurer la fourniture de services d'assistance d'une façon adaptative et personnalisée.

OR 3 : La gestion des données contextuelles est caractérisée par une forte hétérogénéité, ce qui exige l'utilisation des technologies du web sémantique pour construire un modèle unifié sur lequel on peut appliquer un raisonnement intelligent par l'intégration de l'identification des comportements et situations critiques.

Contexte de la thèse

Le paradigme de l'informatique personnelle à favorisé la relation d'interaction "one to one" où chaque utilisateur a son propre ordinateur. L'arrivée du paradigme de l'informatique ubiquitaire et pervasive a étendu cette relation au "many to many" où chaque utilisateur a accès aux différents dispositifs « personnal computing devices ». L'objectif de cette nouvelle génération d'informatique est d'assister les utilisateurs dans leur vie quotidienne lorsqu'ils effectuent leurs tâches. De plus, l'intégration importante des dispositifs mobiles (téléphones, capteurs, etc) a rendu les espaces de vie davantage intelligents. La notion de contexte est développée via l'interaction entre les utilisateurs et les dispositifs situés dans un environnement physique et opérationnel. Selon [Dey 2001], le contexte est défini comme une information caractérisant une situation liée à l'interaction entre les utilisateurs, les applications et leur environnement. Dans le but d'apporter une aide précieuse à l'utilisateur, les technologies et les protocoles d'interaction entre l'utilisateur et son environnement doivent être améliorés afin d'assurer un accès facile et transparent aux services. Un point de vue différent a été introduit par Dey, qui a proposé l'utilisation de modèles et d'outils conceptuels pour soutenir le développement rapide d'applications sensibles au contexte qui, grâce à l'intégration de l'informatique contextuelle pourrait apporter de nouveaux aspects (intelligence, adaptation et personnalisation) dans différents espaces de vie. Par ailleurs, [Weiser 1993] a constaté que les services doivent être fournis d'une façon semi-automatique au moyen de la capture d'environnement, l'analyse de situation et la prise de décision.

Les activités de recherche émergentes dans le domaine de l'informatique ubiquitaire traitent des défis de la sensibilité au contexte. Bien que la notion de contexte peut entrainer des interprétations très subtiles et des situations complexes .

Dans cette thèse, l'accent est mis principalement sur la compréhension et la manipulation de contexte qui peut être détecté automatiquement dans l'envi-

ronnement physique et traité comme entrée implicite pour fournir des services d'une façon adaptative et personnalisée. Dans la conception des systèmes intélligents, les approches d'acquisition, de traitement et de gestion de contextes gagnent une grande applicabilité dans les différents domaines de la vie quotidienne (environnements assistés et systèmes de santé).

Motivations et challenges

L'assurance d'une meilleure sécurité et confort au niveau d'un espace de vie est devenu le défi majeur de beaucoup de chercheurs. Les travaux récents portent principalement sur l'intégration de l'intelligence dans les différents espaces de vie grâce aux avancées en intelligence artificielle, à la miniaturisation des dispositifs électroniques pour l'intelligence ambiante et au développement des réseaux de communication. Ce progrès vise à améliorer la qualité de vie des personnes dépendantes en leur permettant de vivre en toute autonomie et liberté. An niveau des maisons intelligentes, on distingue l'aspect d'intelligence qui porte sur l'environnement (gestion des dispositifs de températures, énergétiques ....) et l'autre aspect qui porte sur l'utilisateur et les différents dispositifs de capture des caractéristiques de l'utilisateur.

Dans notre thèse, on s'intéresse à la protection, la gestion de la sécurité et de la sûreté associées aux technologies de communication dans le domaine de la télé-surveillance et la télé-assistance. Notre contribution a été motivée par un ensemble de défis identifiés ci-dessous :

1. Sensibilité au contexte : c'est une caractéristique principale pour rendre le modèle plus dynamique afin d'assurer la personnalisation et l'adaptabilité lors de la fourniture des droits d'accès suivant la situation qui se présente. Grâce à la diversité des dispositifs environnementaux ou corporels introduits dans l'environnement, différentes connaissances sur l'utilisateur peuvent être extraites. C'est la perception de l'environnement pour interagir plus « naturellement » avec l'utilisateur (capteurs de l'environnement physique, matériels auto-descriptifs, description des personnes).
2. Réactivité : cette caractéristique est le résultat de la prise en compte des données contextuelles et le suivi de comportement.
3. Personnalisation : c'est notre défi principal ; cet aspect dépend des données contextuelles exploitées (profil, capacité, préférences, état de santé). Afin d'assurer cette caractéristique, il est nécessaire d'avoir différents types de capteurs pour extraire ces connaissances.
4. Adaptabilité : c'est notre second défi, il sert à mettre en place la personnalisation en adaptant les services demandés aux profils identifiés.

5. Confiance : les systèmes pervasifs fournissent des services aux personnes anonymes d'où la nécessité de gérer et d'identifier les paramètres permettant d'avoir une certaine confiance sur l'utilisateur.
6. Préservation de la vie privée : l'assurance de la sécurité dans un environnement intelligent exige un suivi de comportement par la mise en place de différents types de capteurs et caméras. Étant donné que différentes informations personnelles sont communiquées aux couches applicatives, l'exclusion des caméras est nécessaire.
7. Intelligence : tout système doté d'adaptabilité, de personnalisation, de réactivité et sensible aux changements détectés dans l'environnement est considéré comme système intelligent. Elle sert à utiliser efficacement les informations du contexte, par exemple : maison intelligente.
8. Scalabilité : c'est le passage à l'échelle et la gestion des volumes de plus en plus grands des utilisateurs, applications et appareils connectés.
9. Invisibilité : cette caractéristique nécessite un minimum d'intervention humaine et lui permet de s'adapter aux changements, par exemple : reconfiguration dynamique des caractéristiques réseaux d'un appareil.
10. Pro-action « all the time every where » : proposer des actions correctives à l'utilisateur.

Objectifs de la thèse

Dans cette thèse nous nous intéressons à la résolution des verrous liés à la sécurité des personnes dépendantes qui résident dans un environnement intelligent doté d'une technologie assistive favorisant leur autonomie. D'où le grand besoin de solutions plus automatiques, réactives et dynamiques aux changements détectés dans leur comportement et ces changements sont strictement nécessaires pour être identifiés.

En effet, l'assurance de la sécurité et de l'assistance ouvrent de nouvelles directions de recherche dans le domaine des systèmes pervasifs. L'objectif de notre thèse est de remédier à cette problématique par le développement d'un modèle de contrôle d'accès personnalisé et adaptatif aux profils et comportements des utilisateurs. Grâce aux technologies d'acquisition, un enregistrement de l'historique du comportement est mis en place dans l'environnement par le biais des dispositifs portables et déployés dans une plateforme de télé-vigilance. Les technologies de la fouille de données sert à l'analyse et l'identification des différents états critiques à partir du corpus obtenu, au fil du temp et contenant les activités quotidiennes. Les technologies du web sémantique ont été largement utilisées pour la conception du modèle et le processus de raisonnement afin d'extraire les droits d'accès à partir des différentes données collectées. Notre politique de sécurité est alimentée par les données contextuelles multi-sources fournies par la plateforme de Télé-vigilance qui est formée de trois sous

systèmes (RFPAT, GARDIEN, ANASON) [Cavalcante 2012][Medjahed 2010]. Ces données contextuelles relatives à l'utilisateur et son environnement, sont une base importante dans la constitution des historiques et dans l'extraction des connaissances implicites pour la mise en place des aspects de personnalisation et d'adaptation. Lors de l'assignation des droits d'accès la politique de sécurité tient en compte l'interaction entre les différentes entités : utilisateur, environnement, dispositif et service demandé.

Afin de gérer la diversité de ces entités (utilisateur, environnement, dispositif, service), une modélisation dans un format standard est nécessaire tout en ayant les avantages de partage, d'interopérabilité de la politique et de raisonnement en tenant compte de l'aspect sémantique. Le modèle proposé est mis en place au moyen d'une ontologie qui gère la spécification des différentes entités de la politique ainsi que la définition des règles responsables sur l'attribution des droits d'accès.

L'architecture qui supporte notre politique de contrôle d'accès est développée suivant quatre couches principales : acquisition, modélisation, raisonnement et application du contrôle d'accès. La contribution de notre travail est caractérisé par les points forts suivants :

- Meilleure identification des utilisateurs, ceci est assuré grâce au suivi du comportement, en analysant l'historique.
- Analyse et extraction des situations sensibles ou d'urgences à travers le comportement surveillé.
- Assignation des droits d'accès suivant la validité du contexte et de la situation
- Validation de la politique de sécurité par la plateforme de télé vigilance.

Organisation du mémoire

Le mémoire est organisé en cinq chapitres répartis en deux parties principales : Etat de l'art et Développement et Validation de la politique de sécurité.

- **Première partie : Etat de l'art**

  Cette partie consiste à faire un état de l'art sur les éléments clés (pour) la résolution de notre problématique, en étudiant et analysant les insuffisances en termes d'assurance de la sécurité des personnes âgées dépendantes. Une étude sur la gestion des données contextuelles ainsi que les différentes phases nécessaires pour leur exploitation est présentée. Elle regroupe les chapitres 1 et 2.

  Le chapitre 1 a pour objectif de décrire l'évolution de l'informatique et l'impact de la technologie de communication aboutissant à l'intelligence ambiante. On cite les domaines d'application de cette technologie au niveau des habitats, des hôpitaux,plus généralement les espaces de vie devenus intelligents grâce à l'intelligence ambiante. Il présente l'étude et

l'analyse des différentes phases en termes d'acquisition, de modélisation, de raisonnement et d'adaptation pour bien concevoir et développer une application sensible au contexte ainsi que les différents verrous rencontrés lors de sa conception.

Le chapitre 2 consiste à présenter un état de l'art sur les modèles de contrôle d'accès dynamiques basés sur la sensibilité au contexte, la préservation de la vie privée et la confiance.

- **Deuxième partie : Développement et validation de la politique de sécurité**
  Cette partie consiste à présenter l'approche développée dans notre thèse, les entités principales du modèle définissant notre politique de sécurité ainsi que l'architecture ayant servi à la mise en œuvre du modèle.

  Le chapitre 3 : Modèle de contrôle d'accès (UBC-ACM)
  Il consiste à présenter l'approche basée sur le suivi du comportement où l'assignation des droits d'accès est liée à la validité de la situation ainsi qu'a l'adéquation du profil au service demandé. L'approche est mise en place grâce à un modèle conçu et élaboré à partir d'une ontologie puis alimenté avec une architecture servant à acquérir et traiter les données contextuelles.

  Le chapitre 4 : **Développement et Mise en place de l'architecture (UBC-ACA)**
  Il présente l'architecture et ses différents modules : l'apprentissage sert à l'extraction des comportements d'utilisateurs, la modélisation définit dans une structure standard la politique de sécurité et ses différentes entités (utilisateur, environnement, service , dispositifs), le raisonnement traduit un ensemble de règles pour inférer des connaissances plus complexes sur l'utilisateur et la prise de décision définit la nature de l'action accordée à l'utilisateur (permission, interdiction, recommandation et obligation).

  Le chapitre 5 : **Validation**
  Il présente la plateforme de télé-vigilance d'acquisition de données contextuelles, le schéma de la maison intelligente ainsi que les différents capteurs exploités pour assurer un meilleur suivi du comportement de l'utilisateur. Les scénarii simulés avec la plateforme nous ont servi comme cas d'étude où les données capturées ont été injectés comme des instances dans le modèle conçu.

- **Conclusion** : cette partie résume le travail effectué dans cette thèse et donne des perspectives qui ouvrent de nouvelles voies de recherche sur différents niveaux (acquisition, modélisation, raisonnement et application de contrôle d'accès).

Partie 1 : État de l'Art, Cadre et Contexte de la thèse

Chapitre 1

L'Ubiquité, la Sensibilité au Contexte et L'Intelligence dans nos Environnements

Grâce à l'évolution des technologies de l'information et de communication. La nouvelle tendance de la recherche tient à fusionner l'aspect physique et digital et les intégrer dans les environnements de nos jours. Cette intégration a fait la naissance de nouvelles ères d'informatique ubiquitaire, pervasive, sensible au contexte et ambiante. L'informatique ambiante a conduit au déploiement des environnements intelligents qui servent d'interface entre les applications et les utilisateurs. Il est nécessaire de prendre en compte le contexte dans lequel les utilisateurs exercent leurs rôles pour adapter les services aux besoins identifiés. Cependant, le service fonctionnel sensibilité au contexte permet d'assurer la personnalisation et l'aptabilité grâce à la mise en pratique des techniques d'acquisition, de modélisation, de raisonnement et d'adaptation aux utilisateurs.

Le but de ce chapitre est de présenter un état de l'art sur l'évolution des ères informatiques. En outre, on fait un tour d'horizon sur les différents verrous liés à la sensibilité au contexte ainsi que les principaux champs d'application en matière de reconnaissance, de personnalisation et d'adaptation à l'utilisateur et son environnement. Ensuite, on montre l'apport de cette intelligence au niveau des différents espaces de vie. En particulier, on présente les maisons intelligentes et le healthcare qui se considèrent comme domaine d'application de l'intelligence ambiante et un cadre applicatif de cette thèse. Entre autres, on a mis l'accent sur l'aspect de la sécurité au niveau de ces systèmes intelligents et plus particulièrement la surveillance et l'assistance des personnes âgées dépendantes.

1.1 De l'Ubiquité à l'Intelligence Ambiante

D'après l'analyse de l'histoire du développement de l'informatique de [Reignier 2010], trois ères ont fait son émergence.

Dans les années (1960-1980), les utilisateurs partagent un seul ordinateur en même temps où la machine est très grosse, couteuse et difficile à utiliser. Cette époque est désignée par l'ère des mainframes.

En suite, nous sommes passés à une nouvelle ère (1980-1990) qui est l'ère des ordinateurs personnels où un utilisateur possède et utilise un ordinateur personnel. Cette ère s'est orientée vers la prise en compte du facteur humain (aspect utilisateur), les ordinateurs ne sont plus destinés seulement aux chercheurs scientifiques et ingénieurs mais ils sont devenus exploitables par une large frange de personnes. La migration à l'ère des ordinateurs personnels est due à la progression technologique matérielle et logicielle en termes de miniaturisation, réduction des prix des ordinateurs et d'augmentation de la puissance de traitement.

Dans les années 1990, encore une évolution très rapide constatée des capacités de traitement, des technologies de communication de l'information et de la miniaturisation des dispositifs, robustes, connectés en réseau et installés dans nos environnements, de nombreux ordinateurs servent une personne. Ces ordinateurs sont spéciaux en forme et fonctionnalité comme les smart phones, PDA, lecteurs mp3 etc. Ce développement important a conduit à la naissance de l'informatique ubiquitaire qui est considérée comme troisième ère.

De nos jours, s'appuyant sur cette évolution technologique, quatre axes de recherche ont fait l'objet de différents domaines d'application. La figure 1.1.1 montre la relation en termes de contribution au développement d'une nouvelle ère partant de l'informatique distribuée à l'intelligence ambiante.

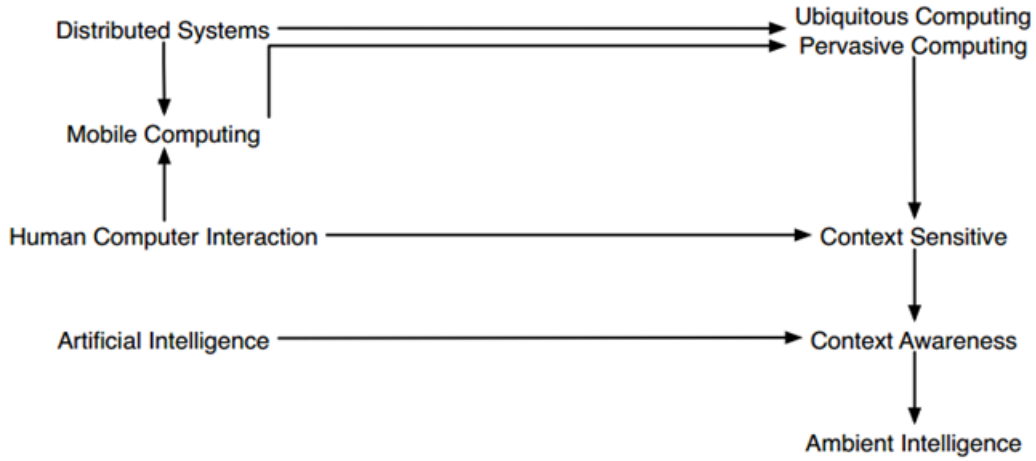

FIGURE 1.1.1 – Relation entre les nouvelles ères d'Informatique [Kofod-Petersen 2007] .

Dans cette thèse, on s'intéresse à la troisième ère d'informatique (ubiquitaire) et sa contribution pour la naissance de nouveaux axes de recherche :

- Informatique Ubiquitaire.
- Informatique Pervasive.
- Informatique Sensible au Contexte.
- Informatique d'Intelligence Ambiante.

Une analyse effectuée sur les ères d'informatique, selon [Dibitonto 2012] a constaté quatre dimensions de changement sur lesquelles eu ce passage entre les ères :

- Dimension physique : En termes d'occupation d'espace, il a eu un passage des mainframes qui prennent une salle entière aux microprocesseurs qui peuvent s'insérer dans les objets de nos environnements.
- Dimension mobilité : Grâce à la dimension physique, cela a conduit à la possibilité d'utiliser l'ordinateur dans n'importe quelle place dans l'environnement. En outre, la mobilité dépend aussi du facteur capacité de mise en réseau et d'énergie (efficacité des batteries).
- Puissance de traitement : l'augmentation des capacités de traitement ont apporté des changements au niveau des applications complexes et plus particulièrement aux interfaces homme machine en termes de réactivité et d'interfaces graphique.

- Relation entre l'homme et l'utilisabilité : Ce changement est évalué sur la base du rapport entre l'utilisateur et l'ordinateur. Auparavant, l'ère des mainframes est caractérisée par l'utilisation d'une machine par plusieurs utilisateurs mais avec la troisième ère ce rapport est inversé où un utilisateur exploite plusieurs ordinateurs avec une personnalisation selon ses besoins sans nécessite de connaitre les détails techniques.

Les nouvelles avancées de l'informatique du 21ème siècle ont été imaginées par Mark Weiser dans ses articles [Weiser 1993] [Weiser 1999], il propose les concepts de l'informatique ubiquitaire et pervasive où les nouvelles ères d'informatique ont été développées au cours des années 90 à Xerox Parc. Ces derniers termes s'intègrent dans la troisième ère d'informatique. Dans la littérature, il y a une confusion entre l'ubiquité et pervasive, où le terme « Informatique Ubiquitaire » a été proposé par Mark Weiser à Xerox Parc et le terme « Informatique Pervasive » a été proposé par IBM. Dans les sections ci-dessous, on aborde les deux concepts tout exposant leur spécificité [Dibitonto 2012] .

1.1.1 Informatique Ubiquitaire

« Les technologies les plus profondes sont celles qui sont devenues invisibles. Celles qui, nouées ensemble, forment le tissu de notre vie quotidienne au point d'en devenir indissociables » [Weiser 1999]

D'aprés [Ronzani 2009], indique que le terme « Informatique Ubiquitaire » est apparu dans les journaux en 1987, mais pas avec le sens envisagé par mark Weiser. Ce terme a été utilisé par Steve Jobs lorsqu'il a décidé de construire des ordinateurs sophistiqués et peu couteux. Cette technologie a été dédiée spécialement à l'enseignement supérieur. Steve a noté qu' avec Appel 2 que "a ubiquitous computing resource that is powerful, reliable and flexible enough to be used everywhere on campus".

Dans la période, 1990-1994, le terme de l'ubiquité se rapportait principalement sur la miniaturisation du matériel où les ordinateurs deviennent de plus en plus petits, l'informatique est devenue embarquer dans tout type d'objet de la vie quotidienne.

De nos jours, l'informatique ubiquitaire [Friedewald et al. 2011] [Schmidt 2002] est devenue un axe de recherche majeur et un paradigme qui réfère au concept "every-where" où l'informatique est intégrée dans l'environnement par l'installation de plus en plus de dispositifs au lieu d'avoir les ordinateurs comme des objets distincts (voitures, meubles, PDA, smart phones) dans notre vie quotidienne, l'accès est transparent et invisible aux ressources vis-à-vis des utilisateurs [Krumm 2009]. Dans [Weiser 1999] l'informatique ubiquitaire est

définie comme un modèle d'interaction homme-machine dans lequel le traitement de l'information est relatif aux activités de la vie quotidienne. Une autre vision de Mark weiser, considère l'informatique ubiquitaire comme un environnement saturé de dispositifs informatiques susceptibles de coopérer de façon autonome et transparente afin d'améliorer l'interactivité et/ou l'expérience de l'utilisateur. Weiser cite dans son rapport que l'informatique ubiquitaire peut être vue comme l'opposé de la réalité virtuelle. La réalité virtuelle met une personne à l'intérieur d'un monde créé par l'ordinateur.

L'informatique ubiquitaire a pour but de permettre à l'ordinateur de "vivre" dans le monde des hommes et de s'y intégrer au point de disparaitre. Dans [Krumm 2009] ce paradigme est caractérisé principalement par :

- La décentralisation ou modularité des systèmes et leur mise en place en réseau.
- l'embarquement des aspects matériels et logiciels des équipements à utilisation quotidienne.
- Le support mobile des utilisateurs à travers la disponibilité des services dans n'importe quel lieu et à n'importe quel moment.
- La sensibilité au contexte et l'adaptation du système aux informations courantes exigées.
- La reconnaissance automatique et le traitement autonome des tâches répétitives sans l'intervention de l'utilisateur.

1.1.2 Informatique Pervasive

L'Informatique Pervasive est une nouvelle tendance vers l'informatisation, la miniaturisation des dispositifs électroniques, leur intégration à n'importe quel objet du quotidien, l'intégration des technologies de la connexion en réseau et l'informatique mobile [Najar 2014] . Le but de cette nouvelle ère d'informatique est de créer un environnement complètement connecté dans lequel les utilisateurs peuvent communiquer des informations et les objets font profit l'aspect de disponibilité de service. Cette connectivité augmente très rapidement comme le montre la figure 1.1.2. Cette souplesse permet de fournir les services suivants : « ce que tu veux, quand tu veux, où tu veux, comme tu veux ».

Dans la littérature, différents chercheurs ont proposé les définitions suivantes [Rouse 2015] :

1. Mark Weiser pense que l'évolution exponentielle des données, des logiciels, du matériel et de la connectivité est susceptible degénérer de nouveaux environnements riches d'éléments qui manquent d'interaction.

2. En conséquence, il a présenté un paradigme où les éléments de calcul ne seront plus prisent en considération par l'utilisateur tout en fonctionnant de manière homogène dans son environnement. L'objectif final est

de fournir aux utilisateurs des services homogènes et omniprésents disponibles à n'importe quel endroit, à n'importe quel moment et à n'importe comment que nécessaire

3. L'informatique pervasive permet le couplage du monde physique au monde de l'information, et fournit une multitude de services et applications qui permettent aux utilisateurs, des machines, des données, des applications et des espaces physiques d'interagir.
4. L'informatique pervasive fusionne les infrastructures physiques et informatiques dans un environnement intégré, où les différents dispositifs informatiques et les capteurs sont réunis pour offrir de nouvelles fonctionnalités et des services spécialisés et de stimuler la productivité.
5. L'accent sur l'informatique pervasive est plus sur les propriétésde logiciel des services que sur les propriétés de l'appareil comme dans le cas de l'informatique mobile, qui résultent de poids, la taille, et d'autres contraintes physiques [Dibitonto 2012]
6. L'informatique pervasive est définie par IBM comme «l'accès pratique, grâce à une nouvelle classe d'appareils, à l'information pertinente avec la possibilité de prendre facilement des mesures à ce sujet quand vous en avez besoin et n'importe où" [Hansmann et al. 2001] .
7. Les environnements de l'informatique pervasive, l'informatique est répandu dans l'environnement, les utilisateurs sont mobiles, les appareils d'information sont de plus en plus disponibles, et la communication est facilitée - entre les individus, entre les individus et les choses, et entre les choses.[Ark et al. 1999]

Dans [Perera et al. 2014] ont décrit les principales caractéristiques de l'Informatique Pervasive :

- Scalabilité : exprime le passage à l'échelle et la gestion des volumes de plus en plus grands des utilisateurs, des applications et des appareils connectés.

- Invisibilité : exprime la nécessite d'un minimum d'intervention humaine et d'auto-adaptation aux changements, comme par exemple : la re-configuration dynamique des caractéristiques réseaux d'un appareil.

- Sensibilité au contexte : exprime la perception de l'environnement pour interagir plus « naturellement » avec l'utilisateur grâce aux capteurs de l'environnement physique, aux matériels auto-descriptifs et a description des personnes).

- Intelligence : exprime l'utilisation efficace des informations contextuelles (maison intelligente).

- Pro-action « all the time every where » : exprime la capacité de proposer des actions correctives à l'utilisateur en fonction du contexte présent ou prédit.

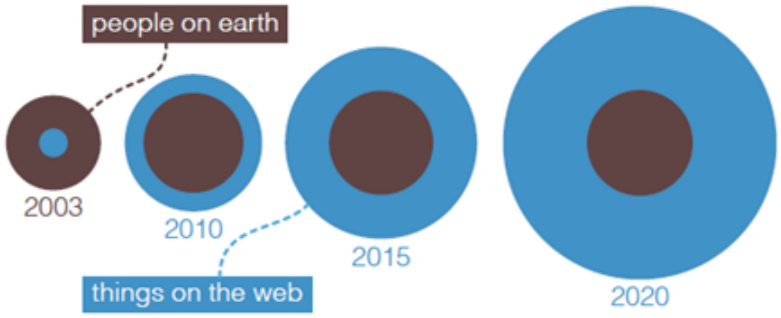

FIGURE 1.1.2 – Connectivité des utilisateurs au fil du temps [Tiberghien 2013].

1.1.3 Informatique Sensible au Contexte

La sensibilité au contexte est considérée comme un service fonctionnel de l'Informatique Ubiquitaire et gagne de plus en plus en applicabilité dans les systèmes Intelligents [Coutaz et al. 2005] . Elle est caractérisée par la manipulation de l'information à n'importe quel moment, à n'importe quelle place via les dispositifs connectés à internet. La sensibilité au contexte joue un rôle de plus en plus important dans le domaine de l'informatique ubiquitaire. Le développement de la sensibilité au contexte à introduit une forme d'intelligence dans les différents espaces de vie (habitats, hôpitaux, espaces de travail) et ainsi, contribué à l'amélioration de la qualité de vie et l'autonomie des personnes occupants. Les tâches liées à la conception d'un système sensible au contexte ont ouvert différents axes de recherches au niveau d'acquisition, de modélisation, de raisonnement et d'adaptation suivant l'exploration et la gestion des données contextuelles qui sont de nature très complexe.

Le terme "contexte" a été défini par plusieurs chercheurs spécialement dans le domaine de l'Informatique Pervasive et Ubiquitaire, la notion de contexte a pris beaucoup d'ampleur et a attiré l'attention de plusieurs chercheurs. Ainsi, on trouve dans la littérature de nombreuses définitions. On présente dans cette

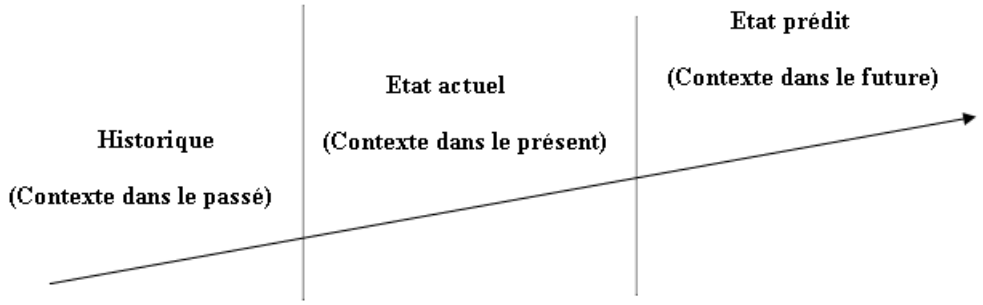

FIGURE 1.1.3 – Le contexte au fil du temps.

section un aperçu des définitions les plus citées : au niveau littéraire, on peut citer :

- Larousse : (latin contextus, assemblage), ensemble des conditions naturelles, sociales, culturelles dans lesquelles se situe un énoncé, un discours.

- Robert : ensemble du texte qui entoure un élément de la langue : un mot, une phrase ou un fragment d'énoncé ou bien un ensemble des circonstances dans lesquelles s'insère un fait.

- Oxford : "The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood."

Au niveau des articles de recherche, on a choisi de revoir les définitions les plus citées sur le terme « contexte ».

- Le contexte est la localisation de l'utilisateur, les identités et les états des personnes et des objets qui l'entourent [Schilit et al. 1994].

- Le contexte est défini en tant que l'identité de l'utilisateur, des personnes et des objets qui l'entourent, sa localisation géographique, son orientation, la saison et la température où il évolue [Brown et al. 1997].

- Le contexte représente la localisation, l'environnement physique, l'identité et le temps de l'utilisateur [Ryan et al. 1997] .

- Le contexte regroupe toutes les informations sur l'environnement courant d'exécution (d'un agent mobile). Ces informations sont distribuées selon trois

niveaux de contexte : physique, social et utilisateur [Amara-Hachimi et al. 2006] .

- Le contexte est défini en tant que : toute information dont le changement de sa valeur déclenche un service ou change la qualité (la forme) d'un service [Miraoui et al. 2008].

- Le contexte représente ce qui l'entoure, et donne un sens à, quelque chose d'autre [Foldoc 2015].

- Le contexte est défini comme une situation, évènements, ou des informations qui sont liées à quelque chose et qui vous aide à le comprendre [Longman 2015].

- Le contexte peut avoir d'autres synonymes : circonstance, situation, phase, position, posture, attitude, lieu, le point ; termes ; régime ; pied, debout, état, occasion, environnement, emplacement, dépendance. [Dictionary 2015]

- Le contexte est défini comme l'ensemble des paramètres externes à l'application pouvant influer sur le comportement d'une application en définissant de nouvelles vues sur ses données et ses services [Chaari 2007] .

Finalement, selon [Dey 2000] résume et généralise la définition du contexte comme suit : « couvre toute information qui peut être utilisée pour caractériser la situation d'une entité. Une entité est une personne, un endroit ou un objet qui peut être considéré significatif à l'interaction entre l'utilisateur et l'application, incluant l'utilisateur et l'application eux-mêmes » (traduction française de la définition de Dey).

Les challenges rencontrés avec les nouvelles ères d'informatique en termes de reconnaissance, de personnalisation et d'adaptation réside dans le fait de faire face aux besoins des personnes déficientes (âgées, dépendantes) ayant pour but de rendre les espaces intelligets. En revanche, l'exploitation des données contextuelles jouent un rôle primordial pour mettre en place ces nouveaux défis. Les dispositifs portables et les capteurs embarqués sont de plus en plus en progrès très rapide pour fournir les informations les plus significatives. De nombreuses données contextuelles sont introduites dans les travaux de recherche.

On distingue deux catégories principales de contextes : Utilisateur et Environnement. Les données contextuelles peuvent être de nature statique ou

dynamique et d' autres informations sont de haut ou de bas niveau comme illustré dans la figure 1.1.3.

* Contexte Utilisateur : représente toute information de nature liée à l'utilisateur qui peut être acquise à travers des dispositifs portables et de capteurs omniprésents. Le contexte utilisateur peut inclure :
  - Identité ou des renseignements personnels : désigne tout type d'information qui peut être statique ou dynamique (nom, âge, sexe, numéro de téléphone, fonction).
  - Contexte Activité représente l'activité exercée par l'utilisateur comme (dormir, marcher, tâches domestiques).
  - Contexte Comportementale : représente les habitudes sur le déplacement, dormir, cuisiner et sortir.
  - Contexte Profil : Ce concept regroupe les préférences, habitudes.
  - Contexte Physiologique : Correspond aux données émises à partir de capteurs corporels (rythme cardiaque, ...).

* Contexte Environnement : représente toute information collectée par le biais des différents capteurs embarqués dans les environnements intérieurs et extérieurs. Dans cette thèse, l'environnement intérieur est pris en compte en utilisant les données contextuelles suivantes :
  - Contexte géographique : correspond à la localisation intérieure ou extérieure.
  - Contexte Temporel : se réfère à l'heure ou le moment auquel la tâche est accomplie.

La notion de sensibilité au contexte concerne l'utilisation du contexte dans les applications intelligentes. Cette notion est une traduction de l'expression anglaise "context awareness".

La sensibilité au contexte (Context-Awareness) est la capacité de réagir proprement en prenant en compte l'information de contexte [Weiser et al. 1997] . Le terme "Context-Awareness" est introduit pour la première fois en 1994 par [Schilit et al. 1994] . Ils considèrent que les applications sensibles au contexte sont des applications ayant des mécanismes leur permettant de changer dynamiquement ou d'adapter leurs comportements en se basant sur le contexte de l'application ou de l'utilisateur.

La sensibilité au contexte étant l'aptitude de capturer, interpréter et répondre aux aspects de l'environnement local de l'utilisateur et de terminal [Ryan et al. 1997] .

Un système est dit sensible au contexte s'il peut changer automatiquement ses formes de services ou déclencher un service comme réponse au changement de la valeur d'une information ou d'un ensemble d'informations qui caractérisent le service [Miraoui 2009].

Un système est sensible au contexte s'il utilise le contexte pour fournir une information pertinente à l'utilisateur, la pertinence dépend de la tâche de l'utilisateur [Dey 2000].

"A system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task." Cette dernière définition d'un système sensible au contexte a été adoptée par tous les chercheurs dans ce domaine.

La définition précise que la sensibilité au contexte est une méthode efficace pour identifier si une demande est sensible au contexte ou non, et a fourni aux chercheurs un moyen utile pour déterminer quels types d'applications

1.1.4 Informatique Ambiante

L'Intelligence Ambiante est un nouveau domaine multi disciplinaire, elle s'appuie sur les avancées de l'informatique ubiquitaire, l'informatique pervasive, les techniques d'interaction centrées homme-machine et d'intelligence artificielle [Balbo et al. 2009] [Reignier 2010]. L'interaction et l'intégration de ces technologies permettent de fournir des services d'une manière plus adaptative, personnalisée ou bien intelligente pour l'utilisateur. Cette technologie gère globalement l'interaction entre l'utilisateur, la technologie et l'environnement. L'acceptabilité de l'intelligence ambiante est due à la combinaison équilibrée de la technologie opérationnelle et de l'intelligence artificielle. Selon [Chahuara Quispe 2013], les termes « Intelligence » et « Ambiante » signifient :

Intelligence : Le test de turing définit l'intelligence comme le fait d'arriver à distinguer entre une personne ou une machine lorsqu'une personne communique avec.

Ambiante : Entourant, se trouve par tout, omniprésent.

Cette ère est caractérisée par le fait que l'informatique est intégrée au cœurs des différents objets de la vie quotidienne au moyen des dispositifs communicants et intelligents. D'où la possibilité de fournir les services aux utilisateurs en réagissant d'une façon réactive et adaptative grâce à la prise en compte de leurs besoins afin d'améliorer leur qualité de vie. Cependant, on se dirige vers l'offre d'un espace quotidien « intelligent » : télémédecine, maison communicante, ...

Le paradigme de l'informatique ambiante a eu une grande importance dans

le domaine de recherche. Chaque chercheur a sa propre vision envers cette évolution technologique. Ces définitions mettent en évidence les caractéristiques qui caractérisent la technologie d'intelligence ambiante :

- Développer la technologie qui va rendre, de plus en plus, notre environnement quotidien sensible et réceptif à notre présence
- Un potentiel futur dans lequel nous serons entourés par des objets intelligents et dans lequel l'environnement va reconnaître la présence de personnes et nous allons y répondre d'une manière indétectable.
- Une vision de l'avenir la vie quotidienne . . . contient l'hypothèse que la technologie intelligente devrait disparaître dans notre environnement pour apporter aux humains une vie facile et divertissant.
- Dans un environnement AmI les gens sont entourés avec des réseaux de dispositifs intelligents embarqués capables de détecter leur état, anticiper, et peut-être adapter à leurs besoins.

[Cook et al. 2007] ont collecté ces définitions et ils ont mis en évidence les points clés de l'intelligence ambiante :

- Sensibilité : Capacité de percevoir les données contextuelles.
- Réactivité : Réagir en fonction de la présence de l'utilisateur dans son environnement ;
- Adaptabilité : Capacité de répondre de manière dynamique aux différentes situations qui se présentent ;
- Transparence : invisibilité pour l'utilisateur ;
- Ubiquité : Présence à n'importe quel endroit.
- Intelligence : Capacité de répondre et de s'adapter de manière intelligente, cette notion est liée à l'utilisation des techniques de l'intelligence artificielle.

Pour la mise en place d'un système ambiant intelligent, il est nécessaire de répondre aux "5Whs" (Qui, Où, Quoi, Quand et Pourquoi) :

Qui : Identification de l'utilisateur et plus spécifiquement de son profil et de son rôle qu'il joue au sein de son environnement par rapport aux autres utilisateurs.

Où : Suivi ou identification de localisation géographique de l'utilisateur ou d'un objet lors du fonctionnement du système. Ils sont fournis à l'aide de la combinaison de différents capteurs installés dans l'environnement.

Quoi : Reconnaissance des activités et des tâches que les utilisateurs exercent où la prise en compte du temps et l'emplacement sont nécessaires afin de fournir l'assistance la plus appropriée à l'utilisateur.

Quand : Identification du temps ou du moment auquel se réalisent les tâches ou activités. Elle représente une caractéristique importante pour l'aspect dynamique.

Pourquoi : Identification et déduction des intentions et des buts des utilisateurs qui sont derrière les activités accomplis par les utilisateurs. Une des solutions utiles est de se baser sur les techniques d'inférence. Cet axe de recherche est considéré comme un défi majeur lors de la conception d'un système ambiant intelligent.

Les (WHs) permettent à un système ambiant intelligent l'acquisition des cinq propriétés suivantes [Augusto 2008] :

- **Non-obtrusivité** : Le système ne doit pas interférer à la vie privée de l'utilisateur à travers des dispositifs invisibles, embarqués et distribués dans l'environnement.
- **Sensiblité au contexte** : Le système doit être capable de reconnaitre et d'anticiper le contexte utilisateur qui évolue dans l'environnement ainsi de réagir aux besoins et aux exigences d'utilisateurs.
- **Personnalisation** : Les profils des utilisateurs et les environnements sont hétérogènes. Le système devrait être personnalisable afin de s'adapter dans des environnements différents et être utilisé par différents utilisateurs.
- **Adaptabilité** : Le comportement du système peut changer en réponse aux actions et besoins d'une personne. De nouveaux services et fonctions peuvent être ajoutés par rapport aux besoins des utilisateurs.
- **Anticipation** : il anticipe les désirs de la personne et de l'état de l'environnement ; il est cadre prédictive et proactive facilitateur.

1.2 Cycle de vie d'un système ambiant intelligent

La sensibilité au contexte est une nouvelle discipline importante qui porte sur la gestion des connaissances se rapportant à l'utilisateur et son environnement. D'après les analystes, la conception d'un système ambiant intelligent exige de suivre un cycle de vie composé de quatre phases comme le montre la figure 1.2 [Xu 2013] [Wang 2014]. Premièrement, le contexte est recueilli auprès de diverses sources. Ces sources peuvent être des capteurs physiques, virtuels ou logiques (acquisition de contexte). Deuxièmement, les données collectées doivent être modélisées et représentées dans un format standard (Modélisation de contexte). Les données modélisées sont ensuite utilisées pour inférer des connaissances de haut niveau (Raisonnement de contexte). Enfin, les connaissances obtenues doivent être exploitées par les applications de reconnaissance, d'adaptation ou de personnalisation afin d'aboutir à un système sensible au contexte et intelligent.

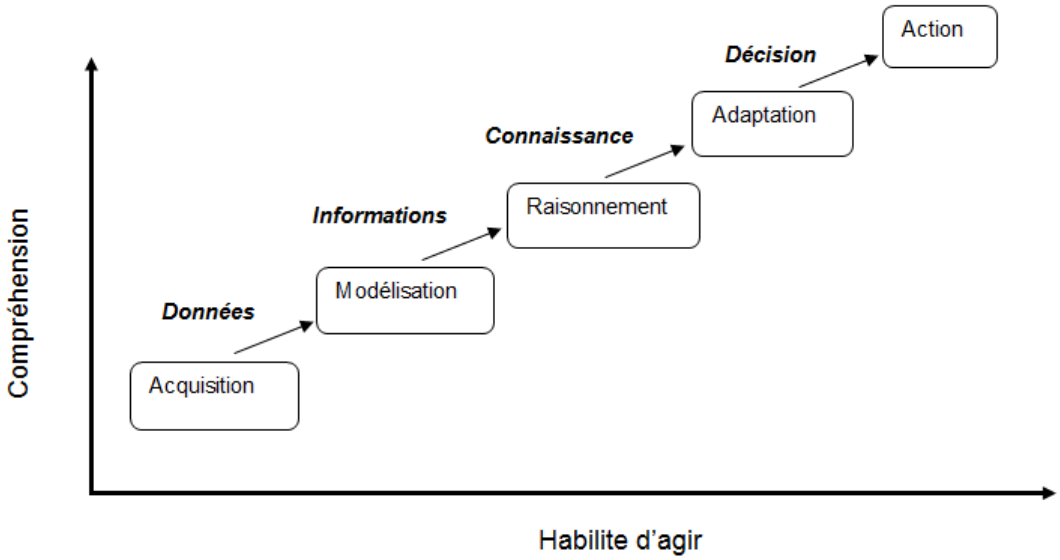

FIGURE 1.2.1 – Cycle de vie d'un système ambiant intelligent.

1.2.1 Acquisition

Le processus d'acquisition est à la base de tout système ambiant intelligent et de toutes applications sensibles au contexte . Cette étape est sensée être à l'écoute des changements survenus lors de l'interaction de l'utilisateur avec son environnement [Perera et al. 2014] [Zhang et al. 2013]. Les informations observées doivent être interprétées dans un format compréhensible par la machine pour qu'il soit exploité comme données contextuelles au niveau des couches supérieures. Ce processus admet deux fonctionnalités majeures :

- La collecte et la détection des informations contextuelles à partir de diverses sources (capteurs embarqués, dispositifs portables et/ou de sources virtuelles). Les données acquises sont considérées comme des données brutes, ensuite elles se transforment en informations contextuelles lorsqu'elles seront associées à un processus de modélisation et d'interprétation. Les capteurs utilisés dans ce processus sont en progrès considérable.

- L'invocation des actionneurs dans l'environnement à base de commandes qui sont envoyées par les couches supérieures.

1.2.1.1 Modes d'acquisition

Le développement des dispositifs a connu une grande importance et progression en termes technologique. Ainsi, différents modes d'acquisition sont devenus possibles pour fournir des données contextuelles plus riches afin de bien cibler l'utilisateur. Dans la littérature, il existe différents modes d'acquisition mais la catégorisation la plus populaire est celle qui distingue l'acquisition par les capteurs, les intergiciels ou les serveurs.

- **Capteurs** : L'acquisition des données directement via les capteurs est assurée par la communication directe avec le matériel et leurs API associées. Ce mode est basé sur deux méthodes principales (pull / push). Le mode Pull se base sur le principe de querying où la requête est envoyée au capteur périodiquement. Le mode Push correspond à l'envoi des informations au composant logiciel du capteur d'une façon périodique. Les capteurs utilisés dans cette phase peuvent être de type physique, virtuel ou logique (logiciel).
  - **o** Physique : Les données sont générées par les capteurs qui peuvent être installés dans l'environnement, portés par l'utilisateur ou dédié à la capture des grandeurs physiques telles que la température, l'humidité, ...
  - **o** Virtuel : Ce type de détection se base sur l'extraction de données par l'utilisation d'autres applications ou services logiciels, tels que : calendrier, email, application de chat.
  - **o** Logique : Ce type exploite la combinaison des serveurs logiques et physique pour fournir des informations plus pertinentes. Un service web dédié à la météo est considéré comme un capteur logique car il est constitué à la base de plusieurs capteurs physiques et virtuels telle que les applications carte, calendrier et les données d'historique. Ainsi, il est considéré comme le résultat d'une transformation de plusieurs informations de contexte capturées séparément à partir des capteurs physiques et logiques.
- **Intergiciels** : les données sont issues via les middlewares et pas directement des capteurs. La caractéristique de ce mode réside dans le fait que la manipulation des capteurs est déléguée aux middlewares. Cette idée a été exploitée par [dey 2000] via le concept des « agrégateurs ». Ces derniers consistent à collecter les différents signaux issus des « wigdets / gadgets ».
- **Serveurs** : Cette méthode a recours à l'utilisation des supports de stockage (base de données) ou service web.

D'autres modes d'acquisition sont possibles[Perera et al. 2014] :

- **Les données dérivées** sont extraites des données détectées (du lieu et du temps) pour reconnaitre l'activité, la situation, le comportement et les autres données complexes liées à des troubles de l'utilisateur. Pour cela, de nombreuses techniques d'intelligence artificielle et des algorithmes d'extraction de données sont nécessaires.

- **Les données déduites** sont fournies à l'aide d'un sondage auprès de soignants pour récupérer les préférences, les habitudes et les loisirs. Pour de nombreuses applications de la vie assistée ambiante, on constate un manque en termes d'acquisition de données contextuelles provenant de sources multiples ou utilisation de capteurs audio pour détecter les situations de bruit, urgence et de détresse.

En raison de l'hétérogénéité de ces données issues de plusieurs sources, il est nécessaire de les représenter, les structurer dans un format unifié et exploitable par n'importe quelle application.

Le tableau 1.1 montre quelques données générées par les capteurs. Notre étude se focalise seulement sur les capteurs non intrusifs qui préservent la confidentialité et la vie privée de l'utilisateur (les dispositifs de caméras sont exclus de notre champs d'exploration).

Nom du capteur	**Données capturées**
Capteurs audios	Bruit, musique, Niveaux décibel
Caméras vidéo	Émotions, présence, comportement
Détecteurs d'émotions	Présence, utilisateurs individuels ou multiples
Capteurs de pressions	Pressé, occupé, geste de la main
Capteurs de lumières	Lumières ambiantes, luminosité intérieure
Accéléromètres	Mouvement, Vibration, état physique
Bluetooth	Localisation
Infrarouge	Localisation
RFID	Localisation, activité, situation
GPS	Location
Capteurs environnementals	Temps, température, humidité
Moniteurs d'évènements	Événement, calendrier, notification, erreur, mise à jour

TABLE 1.1 – Les dispositifs les plus recommandés et le contexte fourni [Perera et al. 2014].

1.2.2 Modélisation

La sensibilité au contexte et la modélisation sont considérées comme les facteurs clés pour manipuler interagir avec un environnement intelligent. La modélisation de contexte est la deuxième phase dans le cycle de vie des données contextuelles. Les systèmes intelligents collectent des données de sources hétérogènes où les données brutes ne peuvent pas être exploitées par les autres couches ou d'autres processus de gestion des connaissances sur l'utilisateur. Cependant, il est nécessaire de passer par un processus qui définit et structure les données en un format compréhensif pour leur bonne exploitation par les applications sensibles au contexte. La conception d'un modèle de contexte doit gérer tous les aspects associés à un système sensible au contexte (partage, interopérabilité et hétérogénéité) [Bettini et al. 2010] [Gross et al. 2003]. Le grand défi que rencontrent les applications sensibles au contexte réside dans le mode de représentation du contexte et bien sûr de fournir un moyen pour pouvoir raisonner sur les données observées de bas niveau. Les modèles contextuels se chargent de présenter et d'organiser les données et fournissent des modèles normalisés ou standards pour faciliter la garantie des services (personnalisation et adaptation) visés par les systèmes sensibles au contexte [Gray et al. 2001] . Ci-dessous, on présente des définitions proposées dans la littérature et portant sur la modélisation de contexte.

« La modélisation de contexte réfère à la définition et le stockage des données contextuelles dans une machine traitable (machine processable processing ». [Baldauf et al. 2007]

« Un modèle contextuel est un motif pour représenter l'objet "contexte"». [Perera et al. 2014]

Modèle contextuel identifie un sous-ensemble concret de contexte où il est réalisables à partir de capteurs, les applications et les utilisateurs peuvent être exploitées lors de l'exécution d'une tâche. Un modèle contextuel est employé par une application sensible au contexte donné est généralement spécifié explicitement par le développeur de l'application, mais peut évoluer de temps.[Zhang et al. 2013]

« Un attribut contextuel est un élément d'un modèle contextuel décrivant un contexte. Un attribut de contexte a un identifiant, un type, et une valeur et optionnellement, une collection de propriétés décrivant des caractéristiques spécifiques. [Zhang et al. 2013]

1.2.2.1 Exigences de modélisation

Les travaux décrits dans [Strang 2004] [Topcu 2011] [Perttunen et al. 2009]définissent des mesures d'exigence en termes de proposition de techniques de

modélisation pour les espaces intelligents ainsi que leur prise en compte lors du choix d'une technique de modélisation des données contextuelles.

- **Distribution** : La caractéristique principale des systèmes intelligents est la distribution des traitements. Cependant, une technique de modélisation doit disposer d'une instance centrale de traitement ainsi que de disposer d'un identifiant unique afin d'éviter tout conflit et de pouvoir assurer la réutilisation.

- **Validation** : Une technique de modélisation doit posséder un moyen de validation partielle des données contextuelles et vérifier leur consistance pour éviter des erreurs de modélisation avant de passer à n'importe quel processus de traitement.

- **Richesse et généralité d'information** : Les données sont collectées de sources multiples, ce qui leurs fournit une richesse. Une technique de modélisation doit être capable de représenter tout type d'information dans une structure conceptuelle.

- **Incomplétude, incertitude et ambigüité** : La technique de modélisation doit être capable de manipuler des données incomplètes, imprécises et ambigües car les données sont issues de capteurs avec certaines erreurs de mesure.

- **Formalité** : Les systèmes intelligents exigent le partage et la réutilisation d'information. Pour cela, un niveau de formalité, spécification adéquate et expressivité de données sont nécessaires lors de la modélisation de données.

- **Applicabilité** : L'approche de modélisation conçue doit avoir la possibilité de la mettre en œuvre au sein d'une architecture sensible au contexte.

1.2.2.2 Techniques de modélisation

De nombreuses techniques de modélisation de contexte sont élaborées et discutées dans [Perera et al. 2014] pour représenter les données contextuelles selon différentes formes : paires (attribut, valeur), balisage, graphique, orienté objet, logique de l'ontologie et de modèles de contexte multidisciplinaires.

- **Représentation à base de paire (attribut/valeur)** : Les informations sont représentées sous forme d'attribut valeur dans des fichiers de type texte ou binaires. L'attribut représente une donnée contextuelle. La valeur est la valeur de la donnée. C'est la technique de modélisation la plus simple et flexible et elle est recommandée pour des données de taille limitée. Cette technique ne permet pas la modélisation des structures de données complexes ou des relations entre les attributs. Elle n'admet pas de support de validation et elle ne se base pas sur un langage standard de représentation. La représentation la plus connue illustrant ce modèle est le modèle Context Toolkit de [Dey 2000].

- **Représentation basée sur XML** : Cette technique représente les données sous forme de balise (tags) et elle supporte une structure de données hiérarchique. Plusieurs modèles de description des informations de contexte se découlent à partir de ce langage : UAProf (User Agent Profile), ContextML et CC/PP (Composite Capabilities / Preference Profile). Les modèles basés sur les langages cités précédemment fournissent une description des éléments de contexte (les ressources) en incluant des contraintes élémentaires et des relations entre ces éléments de contexte pour construire un profil. Ces modèles sont plus expressifs et plus structurés relativement aux modèles basés sur Attributs/Valeurs ; cette technique supporte des schémas de validation.

- **Représentation graphique :** Cette technique consiste à modéliser les informations contextuelles ainsi que les relations selon un graphe conceptuel. Elle dispose de différents standards de modélisation, UML (Unified Modeling Language) ou ORM (Object Role Modeling) [Henricksen et al. 2002] ou CML (Context Modeling Language) pour la modélisation des informations contextuelles. Cette extension est plus formelle et plus expressive pour capturer différents types d'informations contextuelles. Elle appuie le raisonnement sur le contexte, décrit les informations imparfaites et résout l'ambiguïté de l'information contextuelle.

- **Représentation orientée objet** : Avec cette approche, les concepts sont modélisés sous forme de classes et relations tout en exploitant les caractéristiques des modèles orientés objet (nommage, d'encapsulation, de réutilisation et d'héritage). Dans leur approche "HYDROGEN ", [Hofer et al. 2002]ont abordé cette méthode où les concepts tels que le temps, le réseau, la localisation, l'utilisateur, la machine sont représentés sous forme de classes et les autres éléments peuvent être ajoutés par héritage. Cette méthode souffre du manque d'un moyen de validation.

- **Représentation basée sur des ontologies :** Cette technique est basée sur des standards du web sémantique. Cette technologie est caractérisée par sa composante principale « Ontologie » permettant de modéliser les données. Une ontologie est un ensemble structuré de concepts. Les concepts sont organisés dans un graphe dont les relations peuvent être des relations sémantiques ou des relations de composition et d'héritage. Les ontologies sont plus utilisées comme moyen de modélisation grâce aux avantages qu'elles procurent : possibilité de partage, réutilisation de structure de données, séparation du domaine de connaissance et du domaine opérationnel, inférence des connaissances de haut niveau et validation. [Chen et al. 2004] ont exploité les ontologies par l'approche proposée basée sur l'idée d'un courtier de contexte (Context Broker Architecture ou CoBrA).

Les travaux actuels se dirigent vers l'utilisation accrue des ontologies en raison de leurs avantages comme la possibilité de partage, l'expression formelle, la modélisation ainsi que le raisonnement. De plus, elle permettent d'avoir un moyen de regrouper les informations en une seule structure de données. Cependant, la modélisation basée sur les ontologies satisfait les exigences de modélisation définies dans la section précédente.

1.2.3 Raisonnement

Le processus de raisonnement représente le noyau d'une architecture sensible au contexte. Ce processus sert à inférer du contexte sur la base d'un contexte existant [Hu et al. 2013] [Riboni et al. 2011]. Le processus de raisonnement est considéré comme une méthode pour la déduction de nouvelles connaissances sur la base des données contextuelles disponibles suivant un modèle contextuel.

Étant donné l'imperfection et l'incertitude des données brutes de bas niveau, les moteurs d'inférences sont nécessaires pour les mettre en place dans une architecture sensible au contexte.

Les fonctionnalités du raisonnement sont :

- **La vérification de la consistance des données** : Cela dépend du modèle contextuel choisi.

- **La déduction des connaissances de haut niveau :** Dans le domaine de la sensibilité au contexte, on distingue deux types de connaissances explicites et implicites : Les connaissances explicites sont celles collectées des capteurs, modélisées et exploitées. Par contre, les connaissances implicites sont inférées par le biais des mécanismes d'inférence et des techniques d'apprentissage. Le processus de raisonnement est basé sur

l'utilisation des données implicites comme entrée aux moteurs d'inférence pour déduire et fournir des connaissances de haut niveau en sortie.

Afin de déduire des connaissances de haut niveau, le processus de raisonnement passe par les phases suivantes [Perera et al. 2014] :

- **Prétraitement du contexte :** Les données capturées directement des capteurs sont généralement entachées d'erreurs. Elles nécessitent un nettoyage. Cette phase a été toujours recommandée dans les domaines de Data Mining et Intelligence Artificielle.

- **Fusion des données capturées :** Le nombre des capteurs croit progressivement, ce qui engendre une quantité d'information importante, et nécessite la fusion de données pour fournir des résultats plus exacts et précis.

- **Inférence du contexte :** Ce processus sert à la génération des données de haut niveau à partir les données de bas niveau.

1.2.3.1 Exigences de raisonnement

Le choix ou la proposition d'un mode de raisonnement doit prendre en considération les conditions suivantes [Hu et al. 2013] :

- **Efficacité, solidité et complétude :** lors de la représentation des données et du raisonnement, il est nécessaire qu'un processus de raisonnement puisse fonctionner avec complétude, efficacité et solidité .

- **Méthodes de raisonnement multiples** : Il est recommandé qu'une méthode doit disposer de différents moyens pour assurer la modélisation.

- **Interopérabilité :** La représentation de données avec l'ajout de l'aspect sémantique assure l'interopérabilité, le partage et la réutilisation. Cependant, le processus de raisonnement doit suivre une certaine standardisation pour produire des résultats exploitables.

1.2.3.2 Modes de raisonnement

Pour mettre en place le processus de raisonnement, de nombreuses techniques ont été proposées dans la littérature, comme le montre la figure 1.2.2. Les techniques de raisonnement sont catégorisées en six classes [Perera et al. 2014] :

Première classe : elle se base sur les algorithmes d'apprentissage supervisé. Ce mode a besoin d'une base d'apprentissage, les algorithmes les plus reconnus sont : les arbres de décision, les réseaux bayesiens , les réseaux de neurones et les séparateurs à vaste marge (SVM). Ces méthodes exigent des fondements mathématiques et il est obligatoire que toutes les données soient numériques.

Deuxième classe : elle est basée sur l'apprentissage non supervisé et une base d'apprentissage non étiquetée. Parmi les méthodes connues, on distingue la clusterisation (k plus proche voisin). Le résultat de ce mode de raisonnement n'est pas prédit.

Troisième classe : elle est considérée comme le mode le plus simple basée sur les règles décrites sous la forme « if-then-else ». Cette approche permet de déduire des connaissances de haut niveau à partir des données de bas niveau mais ce travail est effectué manuellement. Cette approche est intégrée dans le raisonnement ontologique.

Quatrième classe : elle est basée sur la logique floue ; elle est proche du raisonnement probabiliste car elle manipule des données non certaines et la représentation des données est plus naturelle.

Cinquième classe : qualifiée de probabiliste, elle permet de manipuler les données incertaines et des évidences. Elle utilise la théorie de Dempster Shafer ainsi que les méthodes markoviennes (HMM), dans lesquelles les données manipulées sont sous forme numérique.

Sixième classe : elle est basée sur les ontologies, ce mode de raisonnement est très utilisé dans le domaine de la sensibilité au contexte. Ce mode se base sur la logique des prédicats pour dériver de nouvelles connaissances. Il permet un raisonnement sur des données complexes, numériques et textuelles. Il admet un moyen de validation et de vérification de la consistance des résultats.

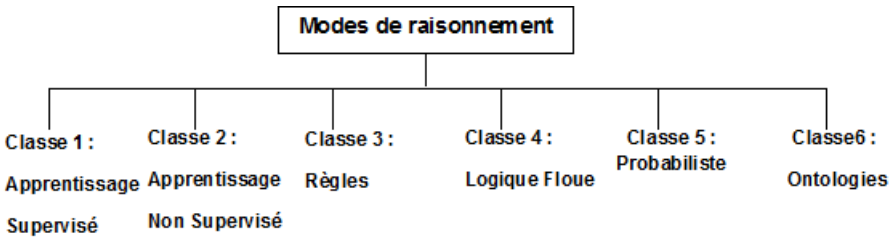

FIGURE 1.2.2 – Modes de raisonnement.

1.2.4 Adaptation

Les travaux qui assurent les phases d'acquisition, modélisation et raisonnement vues dans les sections précédentes, ont pour but de compléter une des taches telles que la reconnaissance, la personnalisation, l'adaptation. La mise en place d'une de ces dernières vise à aboutir à un système sensible au contexte et intelligent avec la prise en compte des évènements survenant dans l'environnement aini que d'avoir la capacité de réagir. On présente dans cette section quelques travaux liés à la reconnaissance, l'adaptation et la personnalisation.

1.2.4.1 Modes d'adaptation

- **Reconnaissance d'activité)**

  Afin de mettre en valeur les données collectées et modélisées, un processus de raisonnent est mis en place pour inférer et identifier l'activité de vie quotidienne effectuée par l'habitant à chaque instant. Ce processus joue un rôle important dans les systèmes d'assistance et de surveillance où il est important de suivre les activités quotidiennes pour la gestion de sécurité des personnes âgées dépendantes. Dans [Rashidi et al. 2013] a identifié cinq paramètres qui sont à l'origine du développement des techniques et outils pour le déploiement de la reconnaissance d'activité et de situation et ce, vu le nombre croissant des maladies, l'augmentation des coûts des soins, le manque de soignants, la dépendance et le large impact sur la société.

- **Définition (Activité)** Une activité est une tâche de la vie quotidienne, telle que dormir, s'habiller, se nourrir, communiquer, . . . que la personne effectue sur un intervalle de temps donné. [Chahuara Quispe 2013]

  La reconnaissance de l'activité est un processus complexe nécessitant la réalisation des quatre tâches suivantes :

  - Tache 1 : choisir et de déployer les capteurs les plus appropriés pour détecter et suivre le comportement des utilisateurs dans leur environnement.

  - Tache 2 : stocker et traiter les données par l'utilisation de technique d'analyse de données puis les représenter dans un niveau d'abstraction le plus approprié..

  - Tache 3 : créer des modèles d'activités pour la gestion de raisonnement.

  - Tache 4 : choisir l'algorithme afin d'inférer les activités des données capturées.

- Personnalisation

Dans [Chen et al. 2004] ont beaucoup travaillé sur la personnalisation et profilisation, en proposant une approche basée sur le service de personnalisation pour les utilisateurs mobiles dans les environnements pervasifs avec le déploiement de son architecture. Leur approche est basée sur les technologies du web sémantique pour modéliser l'utilisateur et raisonner sur la personnalisation en prenant en compte son profil.

1.3 Architectures sensibles au contexte

Les architectures existantes dans la littérature ne répondent pas aux exigences des systèmes orientés santé en termes de sécurité. On a choisi de présenter les architectures à base d'ontologies.

- **CoBrA (Context Broker Architecture) :** C'est une architecture centralisée conçue pour les espaces intelligents, voir la figure 1.3.1. Le courtier de contexte est un agent central qui reçoit des informations de différentes sources (capteurs, agents, appareils, serveurs d'information, etc.). Elle est composée d'une base de connaissances (stockage des données), d'un moteur d'inférence (pour raisonner, interpréter et résoudre les conflits sur le contexte), d'un module d'acquisition (collecte des données) et d'un module de gestion de politique de sécurité (protection de la vie privée). La modélisation et le raisonnement sont à la base d'ontologies [Chen et al. 2004] . Cette architecture est basée sur des agents personnels intelligents qui communiquent avec les « courtier de contexte » pour échanger les informations personnelles d'un utilisateur.

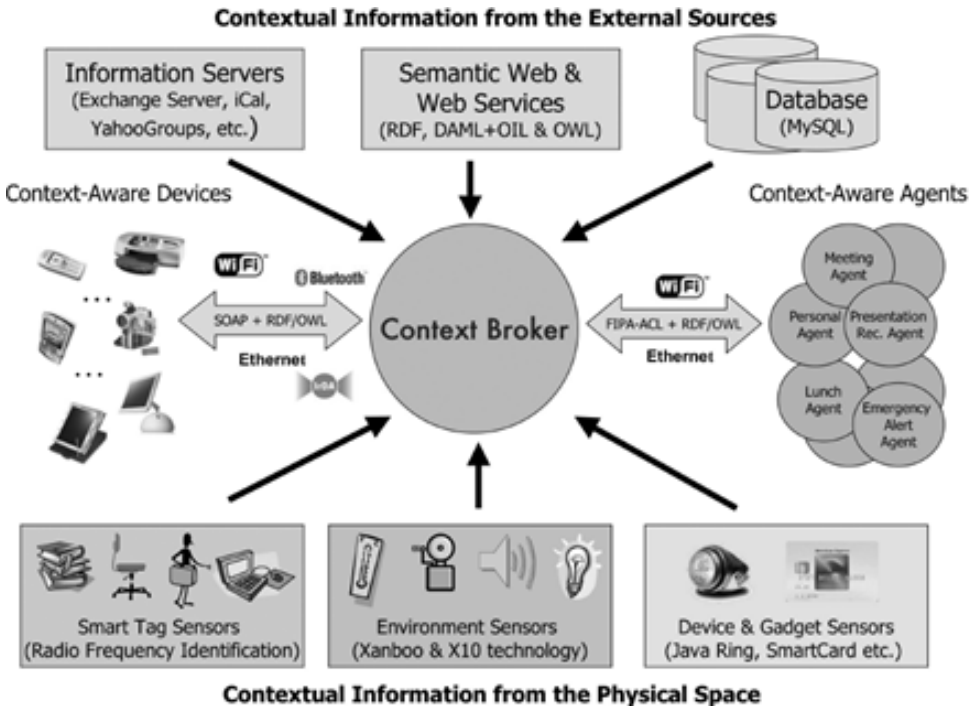

FIGURE 1.3.1 – Architecture CobRA [Chen et al. 2004] .

- **SOCAM (Service Oriented Context-Aware Middleware) :** Est un middleware à base de deux ontologies, l'une représente les concepts généraux et l'autre les termes spécifiques à un domaine [Gu et al. 2004]. Ce middleware est constitué des modules suivants, comme le montre la figure 1.3.2 : Context Provider (ce module permet d'acquérir le contexte de sources différentes et les représenter à l'aide du langage OWL), context intrepreter (ce module effectue le raisonnement ainsi que le stockage des informations dans la base de connaissances) et context service.

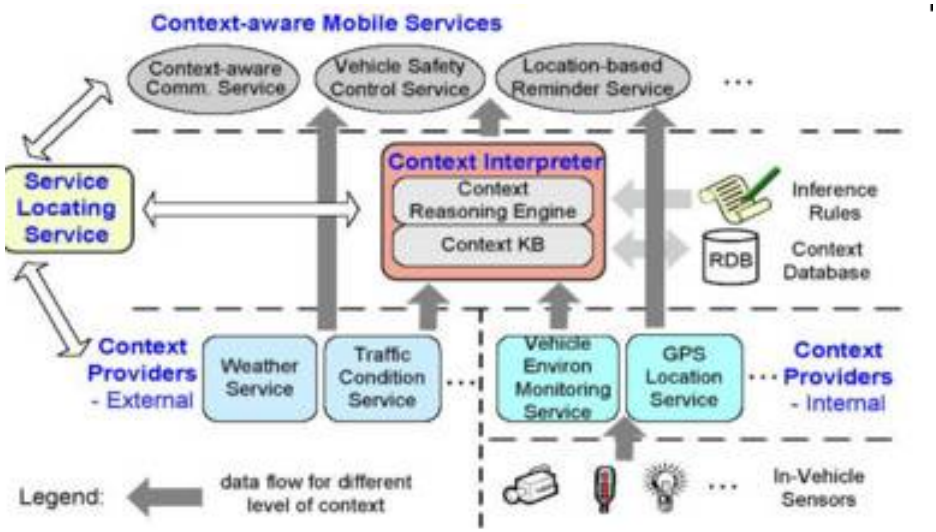

FIGURE 1.3.2 – Architecture SOCAM [Gu et al. 2004].

- CAMAA (Context Aware Mobile Application Architecture) : C'est une architecture pour les systèmes de santé, constituée de trois couches, comme la montre la figure 1.3.3 [Mcheick et al. 2014] :

- Couche de capteurs : La collecte des données se fait de façon continue par l'utilisation de capteurs physiques et virtuels, ensuite distribuées à la couche supérieure.

- Couche d'agents : Pour chaque capteur est associé un agent qui s'occupe de la collecte des observations des capteurs et l'envoi des notifications.

- Couche d'Application : Elle envoie des requêtes à la couche inférieure en mode Pull.

Cette architecture a été utilisée pour voir son efficacité sur des patients qui souffrent de maladies cardiaques et diabètes utilisant différents types de capteurs corporels ou environnementaux) pour gérer les cas d'urgence.

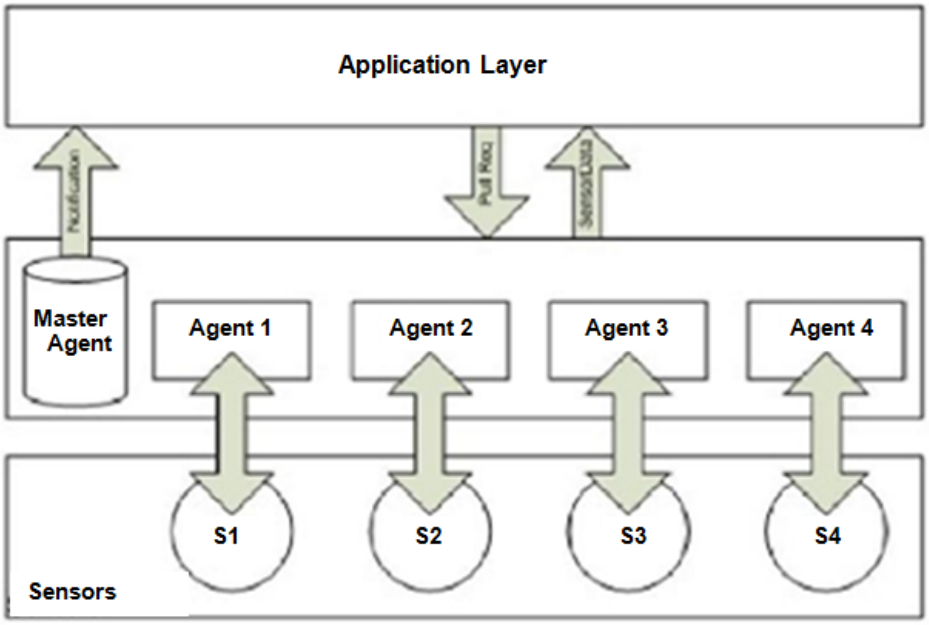

FIGURE 1.3.3 – Architecture CAMAA [Gu et al. 2004].

1.4 Applications de l'intelligence ambiante

La recherche dans le domaine d'intelligence ambiante a donné naissance à différents champs d'application. Le but de ces recherches est d'améliorer la qualité de la vie quotidienne, en fournissant un espace technologique adapté, capable de «comprendre» les caractéristiques des utilisateurs, l'environnement, de s'adapter aux besoins suivant les changements détectés sur les données contextuelles puis de répondre intelligemment aux demandes ou de réagir de façon appropriée.

Dans cette section, on étudie les espaces dotés de l'intelligence et satisfaisant les besoins des personnes âgées dépendantes .

1.4.1 Environnements intelligents

Un environnement intelligent est une application dérivée du concept d'intelligence ambiante ; désigne l'implémentation d'un espace physique dynamique (figure 1.4.1) et adaptable qui optimise les services aux utilisateurs en utilisant des systèmes sensibles au contexte et des technologies ubiquitaires [Chana et al. 2009] .

Selon [Cook et al. 2007] ,

- Environnement : fait référence au milieu dans lequel évolue l'utilisateur.
- Intelligent : fait référence à la capacité d'acquérir et d'appliquer des connaissances de façon autonome.
- Environnement intelligent : moyen d'intégrer les technologies intelligentes et les techniques d'interaction dans les environnements informatisés dont le but de créer des espaces intelligents dans le monde réel.

FIGURE 1.4.1 – L'intégration de l'intelligence dans notre vie quotidienne

1.4.1.1 Maisons intelligentes (Technologie assistée)

Nous avons choisi d'aborder les maisons intelligentes comme domaine d'application des environnements intelligents et cadre applicatif pour notre thèse. Le concept de maison intelligente désigne l'intégration de la technologie et des services au niveau du réseau d'un habitat pour assurer une meilleure qualité de vie avec la prise en compte des besoins des habitants.

Une maison intelligente est une maison ordinaire qui est équipée de différents types de capteurs et actionneurs. Le terme «Maison intelligente» est utilisé pour décrire une résidence équipée de la technologie qui permet la surveillance ainsi que l'assistance de ses habitants en favorisant l'autonomie, l'indépendance et le maintien en bonne santé [Gallissot 2012].

Un habitat intelligent est dirigé par une unité de contrôle centrale, capable d'interpréter les besoins de l'utilisateur et d'exécuter des actions pour y répondre.

Un habitat intelligent est défini suivant [Chahuara Quispe 2013], comme :

« Une maison qui dispose de fonctionnalités susceptibles de simplifier la vie de ses habitants au quotidien, de réaliser des économies d'énergie et d'apporter un certain niveau de confort et de sécurité. Elle est ouverte aux évolutions futures par la nature même de ses infrastructures de câblage et par son ouverture au monde numérique ».

« Une maison intelligent est une résidence équipée de technologie d'intelligence ambiante, qui anticipe et répond aux besoins de ses occupants en essayant de gérer de manière optimale leur confort et leur sécurité par action sur la maison, et en mettant en œuvre des connexions avec le monde extérieur ».

- Domotique

On retrouve aussi le concept de la domotique qui peut être vue comme l'ensemble des techniques et technologies électroniques, informatiques et des télécommunications permettant d'automatiser et d'améliorer les tâches au sein d'une maison.

1.4.1.2 Hôpitaux intelligents

L'hôpital intelligent désigne un milieu de travail très interactif dans lequel le personnel de l'hôpital peut accéder à des renseignements médicaux pertinents à travers une variété hétérogène de dispositifs et collaborer avec des collègues, en tenant compte des informations contextuelles. Ces applications peuvent également adapter et personnaliser l'information en fonction de l'utilisateur du contexte (telles que le rôle spécifique , l'emplacement ou l'état) et de soutenir le périphérique du suivi des patients .

1.4.1.3 Vers l'assistance à la vie quotidienne

Due à la croissance rapide de la population vieillissante, l'assistance à domicile est une nouvelle discipline née grâce aux technologies d'assistances assistées et l'intelligence ambiante. Cette nouvelle approche exploite le suivi et la reconnaissance d'activités ayant pour objectif d'assister et d'apporter une aide personnalisée aux personnes âgées et d'améliorer la qualité de leur mode de vie en favorisant leur autonomie. Ces technologies ont été exploitées par la proposition des systèmes de contrôle des situations d'urgence, l'état de santé et des systèmes de vidéo surveillance. La plupart des systèmes se basent sur la reconnaissance d'activité et de suivi de comportement pour arriver à mettre en place ces systèmes d'assistance [Rashidi et al. 2013].

1.4.2 Challenges

On a présenté dans cette thèse les différentes évolutions connues dans l'informatique et les technologies de communication. Cette évolution a relevé de

nouveaux défis en termes de sécurité, préservation de la vie privée et de gestion de la confiance. Ces derniers sont des axes importants de recherche pour lesquels différentes approches et solutions ont été mises en place pour palier aux problèmes soulevés par ces défis.

1.4.2.1 Sécurité

Le concept de sécurité se distingue en deux classes importantes : La sécurité des informations collectées et la sécurité de l'utilisateur qui occupe un environnement intelligent avec des limites en termes d'autonomie.

- Sécurité d'information : vise à entretenir la confidentialité et l'intégrité des données.
- Sécurité des utilisateurs : vise à gérer l'authentification et le contrôle d'accès des utilisateurs.

1.4.2.2 Respect de la vie privée

Les systèmes intelligents ont recours à l'intégration de capteurs ou de caméras dans l'environnement. Ces dispositifs portent atteinte la vie privée des utilisateurs. Cette diversité de données permet de fournir différentes informations personnelles. Vu le besoin de palier aux problèmes d'hétérogénéité et d'interopérabilité comme conséquence, le partage d'information par l'utilisation des technologies du web sémantique, est devenu nécessaire ; ce qui engendre le problème de la préservation de la vie privée.

1.4.2.3 Gestion de la confiance

La gestion de confiance est complémentaire aux aspects de sécurité et la préservation de la vie privée. Les caractéristiques des systèmes intelligents (système de santé et maisons intelligentes) exigent de mettre en place un processus d'évaluation de niveau de confiance aux différents utilisateurs suivant leurs historique, profils et comportement.

1.5 Population ciblée

Dans cette thèse, on vise à faire face aux besoins de la population âgée dépendante qui est en perte d'autonomie. Cette population est plus concernée par les espaces adaptés de la technologie qui sont capables de tenir en compte les changements détectés dans le comportement de ces personnes [OMS 2015].

- **Dépendance :** La dépendance est l'impossibilité partielle ou totale pour une personne d'effectuer sans aide les activités de la vie, qu'elles soient physiques, psychiques ou sociales et de s'adapter à son environnement.

- **Autonomie :** est définie par la capacité à se gouverner soi-même. Elle présuppose la capacité de jugement, c'est-à-dire la capacité de prévoir et de choisir, et la liberté de pouvoir agir, accepter ou refuser en fonction de son jugement. Cette liberté doit s'exercer dans le respect des lois et des usages communs. L'autonomie d'une personne relève ainsi à la fois de la capacité et de la liberté.

Suivant l'OMS (Organisation Mondiale de la Santé) et le modèle de Wood, la dépendance peut être due à la déficience, incapacité et handicap.

La déficience : correspond à une anomalie ou des troubles manifestés au niveau de l'organe. Cette anomalie peut être sans conséquence pathologique, mais le plus souvent, elle est symptomatique et équivaut à la maladie.

L'incapacité : représente une des conséquences de la déficience et réduction partielle, ou totale, de la capacité d'accomplir une activité.

Le handicap : est le désavantage résultant de l'incapacité. Il traduit l'écart entre l'incapacité physique et intellectuelle de la personne et les normes habituelles de qualité de vie.

1.5.1 Population vieillissante

Le vieillissement est un processus naturel, un phénomène mondial et progressif au cours de la vie. Suivant l'OMS, la vieillesse concerne les personnes âgées de 65 ans et plus [Vieillissement 2015]. Ce phénomène correspond à une modification des fonctions physiologiques, à une perte de relation sociale par l'arrêt de l'activité professionnelle et à une diminution des capacités physiques et cérébrales. Ce phénomène touche les personnes de manières différentes que ce soit socialement, psychologiquement et physiquement, avec un niveau de dépendance différent et une diminution des capacités fonctionnelles de l'organisme [64]. Le taux de cette population augmente progressivement dans l'ensemble du pays, et plus particulièrement au cours des prochaines années comme le montre la figure 1.5.1.

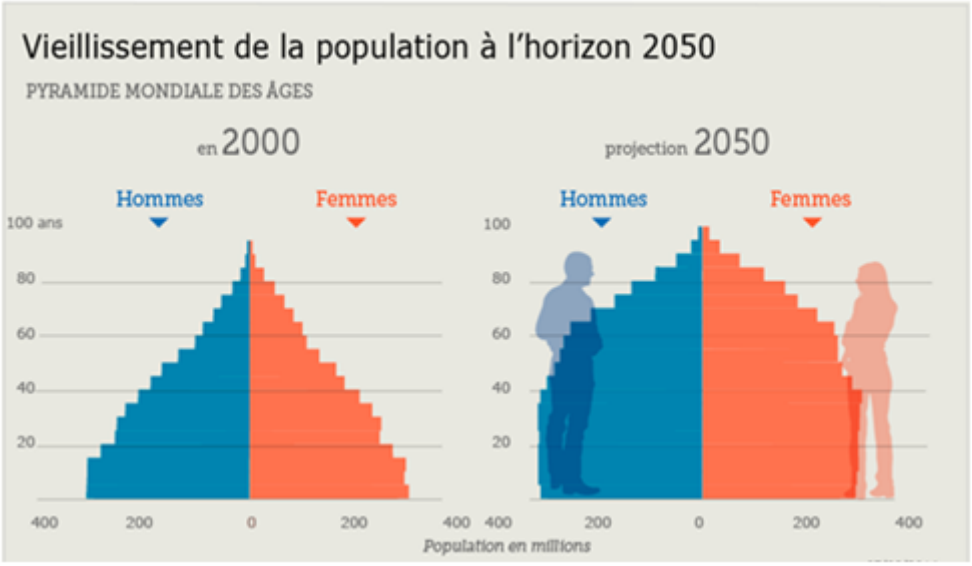

FIGURE 1.5.1 – Progression du taux de vieillissement de la population à l'horizon 2050 .

1.5.2 Population handicapée

Une situation d'handicap est l'ensemble des difficultés rencontrées par un individu pour réagir à une situation de vie en raison de ses déficiences [handicap 2015].

L'handicap est défini comme « une perturbation dans la réalisation des habitudes de vie d'une personne, selon son âge, son sexe et son identité socioculturelle, résultant d'une part de ses déficiences et incapacités et d'autres part d'obstacles causés par des facteurs environnementaux. [Kadouche 2007]

L'handicap désigne la limitation des possibilités d'interaction d'un individu avec son environnement, causé par une déficience provoquant une incapacité, permanente ou non, menant à un stress et à des difficultés morales, intellectuelles, sociales et/ou physiques.

Le terme de handicap renvoie également aux difficultés de la personne handicapée face à son environnement en termes d'accessibilité, d'expression, de compréhension ou d'appréhension.

Une déficience est une « perte de substance ou altération définitive ou provisoire, d'une structure ou fonction psychologique, physiologique ou anatomique». Ce terme dans la traduction française est plus global que celui de trouble, qui n'inclut pas de perte de substance.

1.5.2.1 Types de handicaps et incapacités

L'OMS distingue cinq grandes catégories d'handicap [OMS 2015] :

- Handicap moteur : se caractérise par une capacité limitée pour un individu de se déplacer, de réaliser des gestes, ou de bouger certains membres. Il recouvre aussi l'ensemble des troubles pouvant entraîner une atteinte partielle ou totale de la motricité, notamment des membres supérieurs et/ou inférieurs (difficultés pour se déplacer, conserver ou changer une position, prendre et manipuler, effectuer certains gestes) ;

- Handicap sensoriel : regroupe les difficultés liées aux organes sensoriels, et plus particulièrement :
  - Handicap visuel : concerne les personnes aveugles, mais aussi, dans la majorité des cas, les personnes malvoyantes.
  - Handicap auditif : la perte auditive totale est rare, la plupart des déficients auditifs possèdent « des restes auditifs » pour lesquels les prothèses auditives apportent une réelle amplification. Selon les cas, cet handicap s'accompagne ou non, d'une difficulté à oraliser.

- Handicap psychique : désigne les troubles mentaux, un dysfonctionnement de personnalité ou maladie psychique, névrose, psychose, dépression, dépendance, etc. Il touche principalement les capacités intellectuelles.

- Handicap mental ou intellectuel : c'est une difficulté à comprendre et une limitation dans la rapidité des fonctions mentales sur le plan de la compréhension, des connaissances et de la cognition.

- Maladies invalidantes : toutes les maladies respiratoires, digestives, parasitaires, infectieuse (diabète, hémophilie, sida, cancer, hyperthyroïdie...). Elles peuvent être momentanées, permanentes ou évolutives.

1.5.3 Personnes âgées dépendantes

Avec le vieillissement, les personnes âgées deviennent dépendantes car elles ne peuvent plus prendre en charge des tâches ou activités quotidiennes. Leur prise en charge constitue un enjeu majeur, il est nécessaire d'assurer un accompagnement par des aides (ménages, soins à domicile...), selon le niveau de dépendance et des limitations fonctionnelles de la personne âgée. Les personnes âgées peuvent être dépendantes pour plusieurs raisons (handicap, maladie...) mais n'ont pas toute la chance d'être prises en charge de la même manière. De nombreux travaux de recherche sont dédiés aux défis engendrés par les besoins de cette population [Autonomie et dépendance 2009] [PAD 2015].

1.6 Conclusion

Dans ce chapitre, on a présenté les visions de Mark Weiser concernant l'informatique ubiquitaire, pervasive, sensible au contexte et intelligence ambiante. On a décrit le cycle de développement d'un système ambiant intelligent ainsi que les différents verrous liés à l'acquisition, à la modélisation, au raisonnement, à l'adaptation et la personnalisation. Ces systèmes ambiants intelligents ont pour but de rendre les espaces de vie plus intelligents. Enfin, on a abordé les limites des personnes âgées dépendantes en termes d'autonomie (population ciblée). La sécurité est un défi majeur à considérer au niveau de ces systèmes intelligents. Notre contribution dans ce domaine sera consacrée à la problématique des modèles de contrôle d'accès sensibles au contexte qui sera traitée dans le chapitre suivant.

Chapitre 2

Modèles de contrôle d'accès dynamiques

Selon Mark Weiser, les environnements intègrent de plus en plus de différents dispositifs miniaturisés et de la technologie de communication mobile. Cela permet de déployer des services en tout lieu, à tout moment et pour toute personne (anywhere, at anytime and for anyone). Cette évolution impose de nouvelles exigences et de nouveaux défis par rapport à la sécurité au niveau de ces environnements dynamiques, sensibles au contexte et intelligents. Pour une meilleure sécurité, ils doivent être pris en compte lors de la conception de nouveaux modèles de contrôle d'accès .

Le but de ce chapitre est de présenter un état de l'art sur les politiques de sécurité, les principaux modèles et les architectures de contrôle d'accès dont les développements récents sont marqués par l'intégration des données contextuelles, la gestion de la confiance et la préservation de la vie privée.

2.1 Besoin de sécurité dans les systèmes Intelligents

La sécurité est un problème critique dans les environnements intelligents où de différents défis sont derrière sa mise en place. Ce concept s'appuie sur le maintien de six propriétés essentielles : la confidentialité, l'intégrité, l'authentification, l'autorisation, la non-répudiation et la disponibilité. Avec le progrès technologique, il y a de nouveaux services (trust et privacy) qui ont montré leur importance en termes de mise en place de sécurité et d'autres défis comme illustré dans la figure 2.1.1. Dans cette thèse, on s'intéresse à la sécurité liée à l'utilisateur spécifiquement au service de contrôle d'accès. Ce mécanisme représente une composante importante de la sécurité des systèmes consistant à vérifier si un sujet sollicitant l'accès à un objet possède les droits nécessaires pour le faire. Il est régi avec des règles qui peuvent être exprimées en diffé-

rents langages. L'expression de règles de contrôle d'accès a subi de différents changements au niveau de sa structure. La première notation était (sujet, objet, ressource) et avec la richesse des données contextuelles et l'exploitation des techniques de traitement de données, les règles sont devenues de plus en plus complexes (sujet, objet, service, contexte). L'intégration de la composante contexte est sujette à différents challenges sur différents niveaux (modélisation, interprétation et stockage).

Une règle de contrôle d'accès est composée des paramètres suivants :

- Sujet : peut être un utilisateur, une machine, un processus, un programme, etc.
- Objet : peut être un fichier, une base de données, une machine, un programme, etc.
- Droit d'accès : désigne l'action recherché lorsqu'un sujet accède à un objet (lire, écrire, modifier, etc.).
- Contexte : est une contrainte qui lie le sujet, le droit d'accès et l'objet (contexte temporel, contexte spatial, etc.).

Le système de contrôle d'accès doit évaluer ces paramètres et selon l'évaluation une décision est générée. Celle-ci peut être positive pour permettre l'accès à l'objet ou négative si l'accès est refusé.

La gestion de la politique de sécurité devient de plus en plus complexe dans la mesure où les politiques sont généralement hétérogènes d'un point de vue structurel (rôle, organisation....) et sémantique (langage de spécification, représentation, modélisation et interprétation....).

Dans les environnements intelligents, il y a différents conflits à résoudre pour assurer une meilleure sécurité :

- Définir une politique de sécurité adaptative pour tenir compte de tout changement dans l'environnement.
- Prendre en compte l'environnement lors de la spécification d'une politique de sécurité.
- Déployer différents dispositifs (portés par l'utilisateur ou installés dans l'environnement) pour avoir des données contextuelles plus riches.

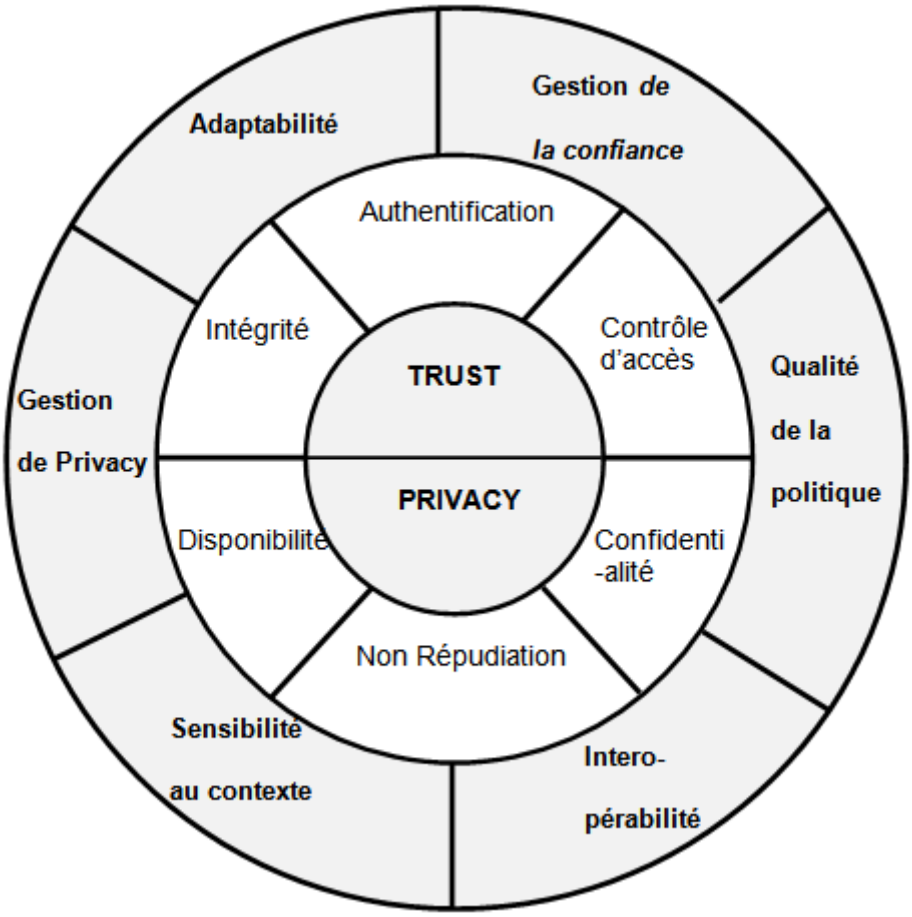

FIGURE 2.1.1 – Services de sécurité et défis.

a) Challenges de sécurité

Les services et les ressources au niveau d'un système intelligent sont caractérisés par l'ouverture, la dynamicité et l'hétérogénéité. Différents challenges sont identifiés pour en tenir compte lors de la conception d'une politique, d'un modèle ou d'un mécanisme de contrôle d'accès.

- Adaptabilité : L'assurance de la sécurité doit réagir face aux situations qui se présentent par l'utilisation de techniques intelligentes.
- Sensibilité au contexte : un système intelligent est complètement équipé de dispositifs. Un mécanisme de sécurité doit collecter toutes sortes de données, les modéliser et les interpréter afin de rendre le système sensible au contexte.
- Gestion de de la vie : L'invisibilité et la transparence des dispositifs exigent, lors de la conception d'un nouveau mécanisme de sécurité, de préserver la confidentialité des données personnelles et sensibles.

- Gestion de la confiance (Trust) : Les systèmes intelligents sont caractérisés par la scalabilité et les utilisateurs sont mobiles. Pour cela, un mécanisme de contrôle d'accès doit avoir un moyen pour vérifier le niveau de confiance lors de l'assignation des droits d'accès aux utilisateurs.
- Interopérabilité : Cette caractéristique exige l'utilisation des technologies du web sémantique pour comprendre correctement les politiques de sécurité dans chaque système.
- Qualité de la politique de sécurité : Cette propriété dépend de la qualité des données contextuelles et le fait d'assurer la préservation de la vie privèe et la gestion de la confiance.

2.2 Services de sécurité

Les systèmes informatiques et les technologies de communication ont connu une évolution rapide caractérisée par une complexité importante plus de dynamicité, plus d'hétérogénéité et plus de mobilité. Les exigences de sécurité sont soumis à de nouveaux challenges vis-à-vis de l'utilisateur où il est devenu nécessaire d'assurer sa sécurité, évaluer son niveau de confiance et préserver sa vie privée. Dans ce travail, on s'intéresse aux services de sécurité liés à l'utilisateur : authentification et contrôle d'accès (autorisation) ainsi que les nouveaux services qui sont de plus en plus demandés : la gestion de la confiance et la préservation de la vie privée.

2.2.1 Authentification

Le processus d'authentification [Auth 2015] sert à vérifier l'authenticité de l'entité en question. Par contre, l'identification, permet de connaitre l'identité d'une entité. L'authentification est le processus qui confirme l'identité de la personne. Pour vérifier la validité de son identité, on a recours à différents moyens associés à :

- Ce qu'il connait (mot de passe, numéro d'identification personnel).
- Ce qu'il possède (acte de naissance, carte grise, carte d'identité, carte à puce, droit de propriété, certificat électronique, diplôme, passeport, téléphone portable, PDA, etc.).
- Ce qu'il est (photo, caractéristique physique, biométrie).
- Ce qu'il sait faire (geste, signature).

2.2.2 Contrôle d'accès / Autorisation

Généralement, ce processus est établi après avoir validé le processus d'authentification. Selon [Tigli et al. 2009] considère l'autorisation comme un type

de contrôle d'accès servant à déterminer les utilisateurs autorisés à effectuer une tâche ou accéder à une ressource. Dans [Tigli et al. 2009] distinguent trois types d'autorisation : statique, quasi-statique et dynamique.

2.2.2.1 Autorisation statique

Ce type d'autorisation est dit statique car il se base sur l'utilisation des données statiques pour accéder à un système. La figure 2.2.1 modélise l'accès d'un utilisateur à un système par un diagramme d'état fini. En premier, l'utilisateur doit s'authentifier, après validation, il doit vérifier aussi quelques règles de contrôle d'accès prédéfinies. Dans ce mode de contrôle, on fait confiance à cet utilisateur où il garde ses droits d'accès jusqu'à la fin de sa session.

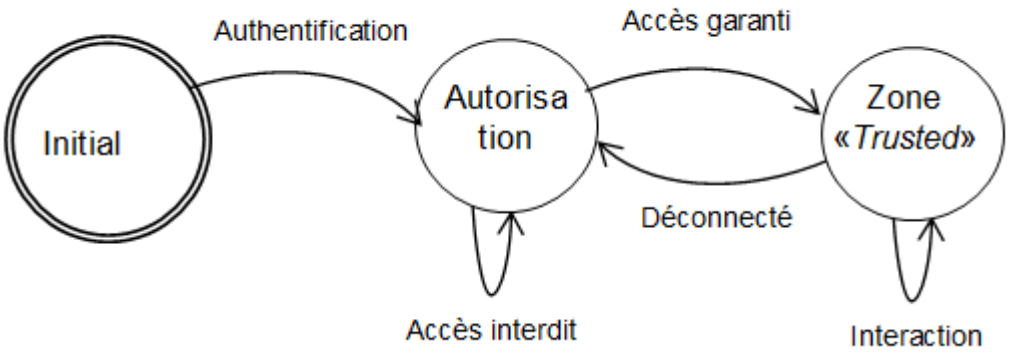

FIGURE 2.2.1 – Schéma d'une autorisation statique [Tigli et al. 2009] .

L'utilisation des données statiques pour l'authentification et l'autorisation est devenue très limitée spécialement avec l'apparition de l'informatique distribuée.

2.2.2.2 Autorisation Quasi-statique

Les données utilisées pour authentifier et attribuer les droits d'accès sont de nature dynamique. Ce type s'apparente à l'autorisation statique mais, une fois que l'utilisateur a accédé à la zone « trusted », un processus de réévaluation

de la validité des paramètres est activé périodiquement, ainsi l'utilisateur peut perdre ses droits à tout moment. La figure 2.2.2 illustre le fonctionnement décrit dans cette section.

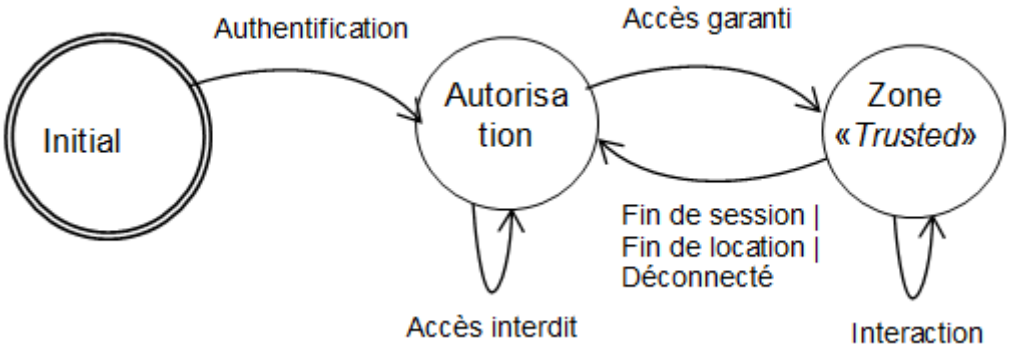

FIGURE 2.2.2 – Schéma d'une autorisation quasi-statique [Tigli et al. 2009] .

Parmi les travaux qui utilisent le principe d'autorisation quasi-statique, il y a CS-RBAC [Kumar et al. 2002] et OrBAC [Cuppens et al. 2003]. Avec l'émergence des environnements très dynamiques, ce type d'autorisation a montré ses limites.

2.2.2.3 Autorisation dynamique

L'autorisation dynamique est conçue pour les environnements hautement dynamiques. Ce type exige de vérifier fréquemment si l'utilisateur est autorisé en raison des changements fréquents dans les données pour accorder les droits d'accès (voir figure 2.2.3). Ces derniers sont accordés suivant la validité des données contextuelles. Parmi les travaux qui se basent sur ce mode de contrôle dynamique, il y a OASIS [Bacon et al. 2005] et CA-RBAC [Kim et al. 2005].

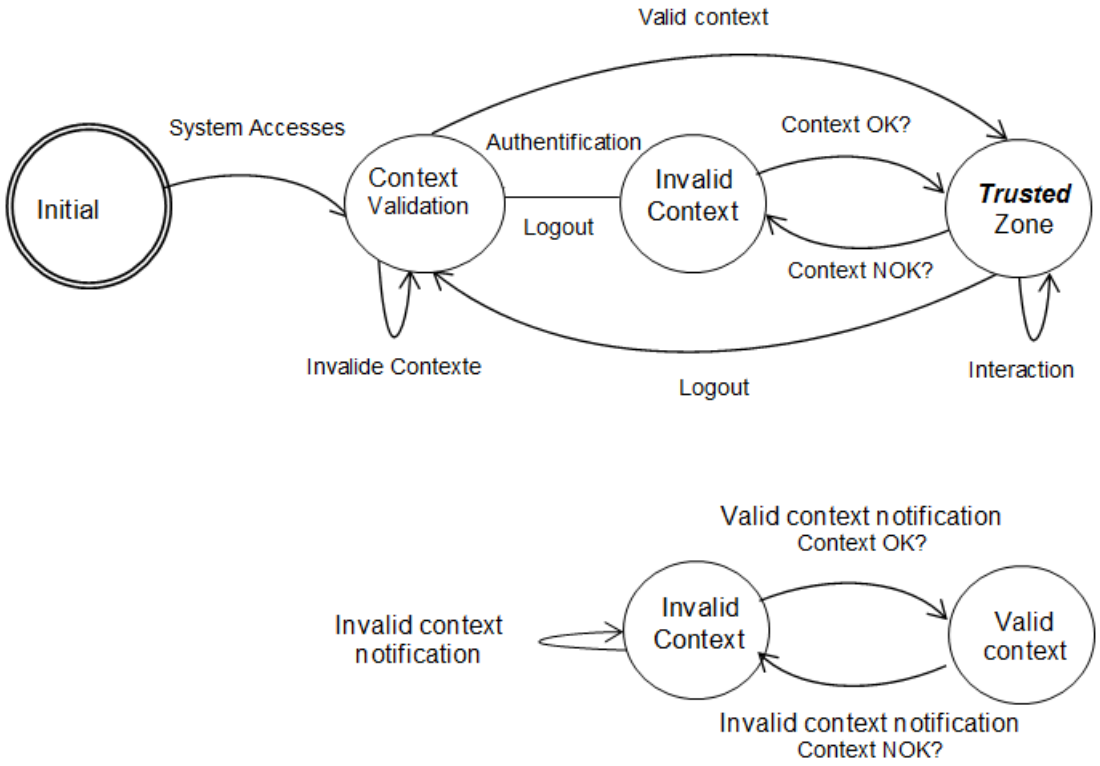

FIGURE 2.2.3 – Schéma d'une autorisation dynamique [Tigli et al. 2009].

2.2.3 Gestion de confiance (Trust)

La mise en connexion des systèmes et la mobilité des utilisaters, ce qui a engendré le problème des utilisateurs nomades. D'où le besoin de la gestion de confiance aux niveaux de ces systèmes dynamiqes. Grâce aux données contextuelles, la gestion de la confiance a eu de nouvelles opportunités lors de la conception de nouveaux modèles de confiance. Ces modèles servent à évaluer le niveau de confiance d'une personne anonyme. Dans la littérature, la gestion de la confiance a été l'objet de plusiers travaux et différentes définitions sont données.

- «La confiance est la probabilité subjective par laquelle un individu, (A) attend qu'une autre personne, (B) effectue une action donnée sur laquelle son bien-être dépend » [Nixon et al. 2004]

- « Un niveau particulier de la probabilité subjective avec laquelle un agent évalue qu'un autre agent ou d'un groupe d'agents vont effectuer une action particulière, à la fois avant qu'il puisse suivre une telle action (ou indépendamment de sa capacité toujours être en mesure de suivre) et dans un contexte dans lequel il affects sa propre action. » [Gambetta 2000]

- «La confiance comme la ferme conviction de la compétence d'une entité à

agir de façon sécurisée et sure dans un contexte précis » (en supposant que la sureté couvre la fiabilité et l'actualité) [Grandison et al. 2000]

- « La méfiance (manque de confiance) ou le manque de conviction de la compétence d'une entité à agir de façon sécurisée et sure dans un contexte spécifié ». [Grandison et al. 2000]

On distingue lors de la gestion de la confiance trois catégories : Service, Information et Utilisateurs.

- La confiance en service : est évaluée et validée par le moyen de la qualité de service.
- La confiance en informations : Cette mesure est assurée par le moyen des services de sécurité : l'intégrité et la confidentialité des informations.
- La confiance en utilisateurs : niveau de confiance est évalué sur la base des paramètres suivants : l'identité, le comportement et l'historique d'utilisateur.

2.2.4 Vie Privée

La communication des données personnelles sur l'utilisateur est devenue exigée par les nouvelles applications. Cependant, la préservation de la vie privée est devenue un enjeu incontournable à assurer au niveau des systèmes intelligents. Ces systèmes manipulent des données issues de différents types de capteurs. La fourniture et la gestion des services personnalisés engendre la manipulation et le partage d'informations personnelles qui doivent être contrôlés.

Dans la littérature, la préservation de la vie privée a été définie par différents chercheurs.

- "La capacité d'un individu à contrôler les conditions dans lesquelles leurs renseignements personnels sont acquis et utilisés ". [Spiekermann et al. 2009]
- "Le droit de l'individu à être protégé contre l'intrus-ion dans sa vie ou des affaires personnelles, ou ceux de sa famille, par des moyens physiques directes ou par la publication de l'information ». [Spiekermann et al. 2009]
- "La réclamation des individus, des groupes et des institutions de déterminer pour eux-mêmes, quand, comment et dans quelle mesure l'information à leur sujet est communiquée aux autres». [Culnan 2000]

2.2.4.1 Exigences de la Vie Privée

La confidentialité de la vie privée couvre différents aspects :

- Comportemental : Contrôler l'utilisation des données personnelles des utilisateurs.

- Communication : Prendre soin de la haute technologie qui peut être exploitée pour divulguer des données personnelles.
- Contexte et information : pour empêcher toute divulgation de l'information liée au contexte d'utilisation d'un service (par exemple ses paramètres actuels de l'appareil) et à partir duquel des informations indirectes sur l'utilisateur pourraient être extraite.
- Anonymat : la garantie pour une personne de rester non identifiable dans un ensemble de sujets.
- Emplacement des impacts de l'anonymat : tant que l'utilisateur est anonyme, l'emplacement privé est préservé.

2.3 Gestion de la sécurité

La gestion ou la mise en place de la sécurité au niveau d'un système, son implémentation exige de passer par trois concepts principaux : Politique de sécurité, modèles et mécanismes de contrôle d'accès. La figure 2.3.1 illustre la relation entre cs différents concepts [AL Kukhun 2012] [Amini 2010] [Li et al. 2008].

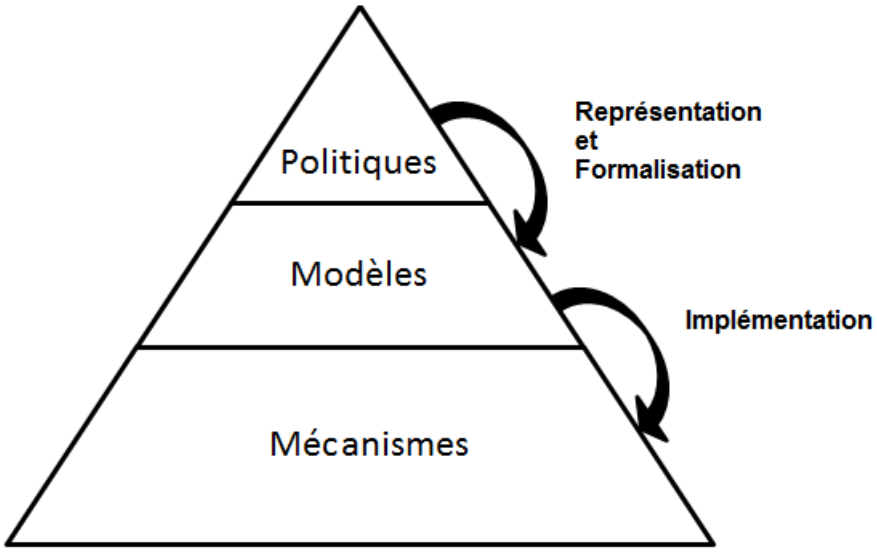

FIGURE 2.3.1 – Les concepts d'implémentation de sécurité.

2.3.1 Politique

Une politique de sécurité est le moyen primordial pour la description et la spécification de la gestion des droits d'accès. Elle constitue la première étape à

réaliser pour assurer les objectifs de la sécurité. On trouve différentes définitions pour une politique de sécurité.

- Les politiques de contrôle d'accès définissent les règles selon lesquelles le contrôle d'accès doit être réglementé. [Samarati et al. 2001]
- Une politique de sécurité dans un système, partitionne ses états en états sécurisés (autorisé) et non sécurisés (non autorisées). [Almulhem 2008]
- Un système sécurisé est un système qui commence par un état autorisé et ne peut pas entrer dans un état non autorisé. [Almulhem 2008]

2.3.2 Modèles de sécurité

Un modèle de contrôle d'accès sert à élaborer une représentation formelle des politiques de contrôle d'accès. Il a pour objectif de décrire de manière non ambiguë les différentes entités répondant à des exigences d'une politique de sécurité au sein d'une organisation. Les modèles de sécurité sont utiles pour prouver les limites théoriques d'un système. Les sections 5 et 6 présentent des modèles statiques (DAC, MAC, RBAC) et dynamiques (à base de données contextuelles).

2.3.3 Mécanismes de sécurité

Les mécanismes de contrôle d'accès sont généralement le moyen au niveau bas d'abstraction, ils appliquent les politiques de contrôle d'accès de haut niveau et traduisent la demande d'accès d'un utilisateur en termes d'une structure spécifique que fournit le système .

2.4 Modèles de contrôle d'accès statiques

Dans [Cheaito 2012] décrit les modèles de contrôle d'accès statiques, où l'assignation des droits est exprimée sous la forme (sujet, objet, ressource) et ne dépend d'aucune autre contrainte .

Un modèle de contrôle d'accès peut être défini comme un formalisme (souvent mathématique) qui permet de développer et spécifier le comportement d'un système de manière exacte afin de mieux le comprendre. Il permet aussi d'abstraire, donc de faciliter la compréhension d'une politique de sécurité et d'implémenter des mécanismes pour assurer certains objectifs de sécurité.

2.4.1 DAC

Les politiques de contrôle d'accès discrétionnaire (ou DAC pour Discretionary Access Control) sont basées sur les notions de sujets, objets et droits

d'accès. Les droits d'accès à chaque information sont manipulés par le propriétaire de l'information.

Définition 1 : Dans TCSEC (Trusted Computer System Evaluation Criteria), le contrôle d'accès discrétionnaire est présenté comme : "un moyen de restriction d'accès aux objets basé sur l'identité des sujets et/ou groupes auxquels ils appartiennent. Les contrôles sont dits discrétionnaires dans le sens où le sujet est capable de transférer les permissions d'accès à d'autres sujets" (La transmission des droits est exercée à la discrétion du sujet).

Définition 2 : Un contrôle d'accès est dit discrétionnaire lorsque la méthode de gestion de l'accès aux objets est basée sur l'identité du sujet. Le contrôle est discrétionnaire dans le sens où un sujet possédant un droit d'accès est capable de conférer ce droit à tout autre utilisateur.

Une politique discrétionnaire n'est applicable que dans la mesure où il est possible de faire totalement confiance aux sujets (utilisateurs). Ce type de politique se retrouve dans la plupart des systèmes d'exploitation actuels (Unix, Windows) dans lesquels pour chaque objet (fichiers, répertoires) une liste de contrôle d'accès associe un utilisateur à une liste de droits (lire, écrire, exécuter). Elle est souvent représentée sous forme d'une matrice des droits d'accès. Les deux principaux modes d'implémentation sont :

- La liste des contrôle d'accès (ou ACL pour Access Control List) : la matrice est stockée par colonne. A chaque objet est associée une liste de règles indiquant pour chaque utilisateur les actions pouvant être exercées par ce dernier sur cet objet.
- La liste des capacités (ou capability) : la matrice est stockée par ligne. A chaque utilisateur correspond une liste, appelée liste de capacité, indiquant pour chaque objet les actions que l'utilisateur est en droit d'effectuer sur cet objet.

Cette politique est acceptable lorsque le nombre d'utilisateurs n'est pas important.

2.4.2 MAC

Une politique de contrôle d'accès obligatoire (ou MAC pour Mandatory Access Control) porte non seulement sur l'accès mais également sur le flux d'information contenu dans les objets. A l'opposé des politiques de contrôle d'accès discrétionnaires, les sujets d'une politique de contrôle d'accès obligatoire ne sont plus propriétaires des informations auxquelles ils ont accès. De plus, l'opération permettant la délégation des droits est contrôlée par les règles de

la politique. Les sujets n'ont plus de pouvoir sur les informations qu'ils manipulent. Le sujet n'a accès à une information que si le système l'y autorise.

Définition : Un contrôle d'accès est dit obligatoire lorsque l'accès aux objets est basé sur le niveau de sensibilité de l'information contenue dans les objets. L'autorisation d'accéder à un objet est accordée à un sujet si le niveau d'autorisation de celui-ci est en accord avec le niveau de sensibilité de l'information [Kumar et al. 2002].

Une politique de contrôle d'accès obligatoire n'est applicable que dans la mesure où toutes les parties du système sont sous le contrôle d'une même entité.

2.4.3 RBAC

La politique de contrôle d'accès (RBAC) est très favorisée pour la gestion de contrôle d'accès au niveau de grandes organisations ou entreprises. Les utilisateurs finaux ne sont pas les propriétaires des documents qu'ils manipulent et pour lesquels ils ont un droit d'accès. L'entreprise est le réel propriétaire de ces informations et des processus qui permettent de les manipuler. Le contrôle d'accès est le plus souvent associé aux rôles qu'assument les utilisateurs au sein de l'entreprise plutôt que sur la propriété des données comme c'est le cas dans le contrôle d'accès discrétionnaire [Cheaito 2012].

Selon [Ferraiolo et al. 2001] définissent la politique de contrôle d'accès à base de rôle RBAC (Role Based Access Control) qui repose sur la description des fonctions qu'un sujet a droit d'accomplir au sein d'une organisation pour établir les règles d'accès aux informations, le modèle est illustré dans la figure 2.4.1 ansi que les différentes entités dans la figure 2.4.2.

Chaque organisation peut créer, pour son propre compte, une politique interne basée sur les rôles des divers sujets au sein de l'organisation. Ce type de politique convient particulièrement bien aux entreprises. Il suffît généralement de définir une fois pour toute la politique en regard de tous les rôles existants au sein de l'entreprise. Par la suite, lorsqu'un nouvel employé est recruté, il suffira de lui assigner les rôles qu'il est censé avoir au sein de l'entreprise pour que le système puisse automatiquement affecter, à ce nouveau sujet, des droits dans les limites autorisées par la politique.

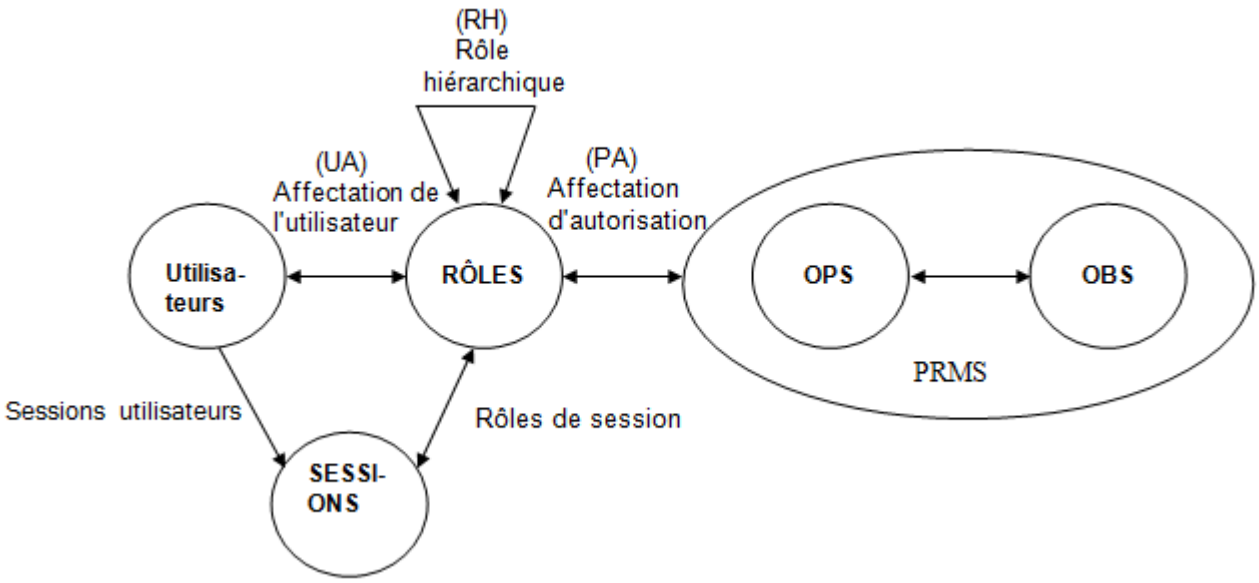

FIGURE 2.4.1 – Modèle RBAC.

	Notation	Description
Concepts	$\mathcal{U}$	ensemble fini d'utilisateurs
	$\mathcal{R}$	ensemble fini de rôles
	$\mathcal{A}$	ensemble fini d'actions
	$\mathcal{O}$	ensemble fini d'objets
	$\mathcal{S}$	ensemble fini de sujets (sessions)
Relations	$\mathcal{P} \subseteq \mathcal{O} \times \mathcal{A}$	une permission est une action sur un objet
	$\mathcal{URA} \subseteq \mathcal{U} \times \mathcal{R}$	affectation many-to-many de rôles aux utilisateurs
	$\mathcal{PRA} \subseteq \mathcal{R} \times \mathcal{P}$	affectation many-to-many de permissions aux rôles
	$\mathcal{SU} \subseteq \mathcal{S} \times \mathcal{U}$	relation many-to-one entre sessions et utilisateurs
	$\mathcal{SR} \subseteq \mathcal{S} \times \mathcal{R}$	relation many-to-many entre sessions et rôles

FIGURE 2.4.2 – Concepts et relations du RBAC.

2.4.3.1 Famille du modèle RBAC

La famille de RBAC est composée de quatre modèles [Cuppens et al. 2003], la relation entre ces modèles est illustrée par la figure 2.4.3 :

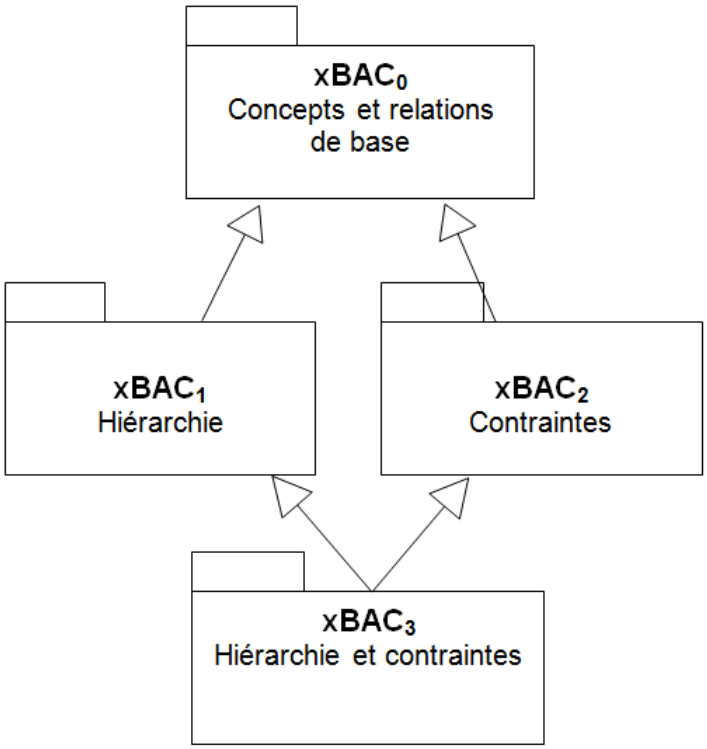

FIGURE 2.4.3 – Famille du modèle RBAC.

- Modèle RBAC0 présente les concepts et relations de base (le noyau du modèle).
- Modèle RBAC1 reprend le modèle RBAC0 et introduit la notion de hiérarchie.
- Modèle RBAC2 reprend le modèle RBAC0 RBAC2 et introduit la notion de contrainte.
- Modèle RBAC3 reprend les modèles RBAC1 et RBAC2.

Les modèles classiques vus précédemment (DAC, MAC, RBAC) ne répondent pas aux exigences de sécurité des systèmes pervasifs car lors du contrôle d'accès, ils ne prennent pas en compte la situation et le contexte des utilisateurs (emplacement géographique, temps, historique,....).

Le modèle RBAC simplifie la gestion et l'administration des droits d'accès, mais présente certaines limites :

- C'est un modèle statique.
- Il ne permet de modéliser que des permissions statiques.
- Il ne permet pas de modéliser des permissions contextuelles.

- Il ne prend pas en compte les dimensions environnementale et temporelle.
- Le concept de hiérarchie de rôle est un peu flou.
- Il ne modélise que des permissions positives.
- La prise de décision dépend seulement du sujet.

2.5 Modèles de contrôle d'accès dynamiques

Étant donné les insuffisances du modèle RBAC en terme d'assurance de la sécurité au niveau des systèmes hautement dynamiques et ouverts, RBAC a été étendu pour être adapté aux changements de l'environnement. Les différentes extensions du modèle portent sur l'intégration des contraintes contextuelles et sont répartis en cinq catégories. Bien que [Asmidar et al. 2009] ont opté pour seulement les trois classes.

- **Catégorie 1 :** Modèles de contrôle d'accès basés sur la sensibilité au contexte.
- **Catégorie 2 :** Modèles de contrôle d'accès basés sur la gestion de confiance (Trust).
- **Catégorie 3 :** Modèles de contrôle d'accès basés sur la gestion de la vie privée (Privacy).
- **Catégorie 4 :** Modèles de contrôle d'accès basés sur l'aspect sémantique.

- **Catégorie 5 :** Modèles de contrôle d'accès basés sur les technologies d'intelligence artificielle

2.5.1 Modèles de contrôle d'accès basés sur la sensibilité au contexte

Cette section présente des extensions du modèle RBAC, dans lesquelles l'activation des rôles est dynamique et en fonction des paramètres incorporés à la validité de contexte. Le contexte est défini comme information décrivant et caractérisant les situations des entités (personne, place, objet). Il peut être temporel, spatial ou environnemental. Les différentes évolutions du modèle RBAC sont décrites à travers les sept extensions décrites ci-dessous.

2.5.1.1 Modèle TRBAC (Temporal Role Based Access Control)

[Bertino et al. 2000] proposent le modèle TRBAC où le facteur temps a été introduit dans la structure d'une politique de sécurité. L'activation et la désactivation des rôles est temporelle. Un rôle peut être actif durant une certaine période et non actif à d'autres, en créant des rôles déclencheurs (trigger rôle). Ce modèle est très approprié aux applications avec une contrainte temporelle

forte, comme les systèmes intégrant des workflows où la notion de temps est importante. Ce modèle est recommandé pour les organisations désirant spécifier des règles d'autorisation valides pendant un intervalle de temps donné.

2.5.1.2 Modèle GeoRBAC (Geographic Role Based Access Control)

[Bertino et al. 2005] proposent une autre extension (GeoRBAC) qui a largement émergé dans le domaine de contrôle d'accès avec l'intégration de la contrainte spatiale, l'extention du modèle RBAC est illustrée dans la figure 2.5.1.

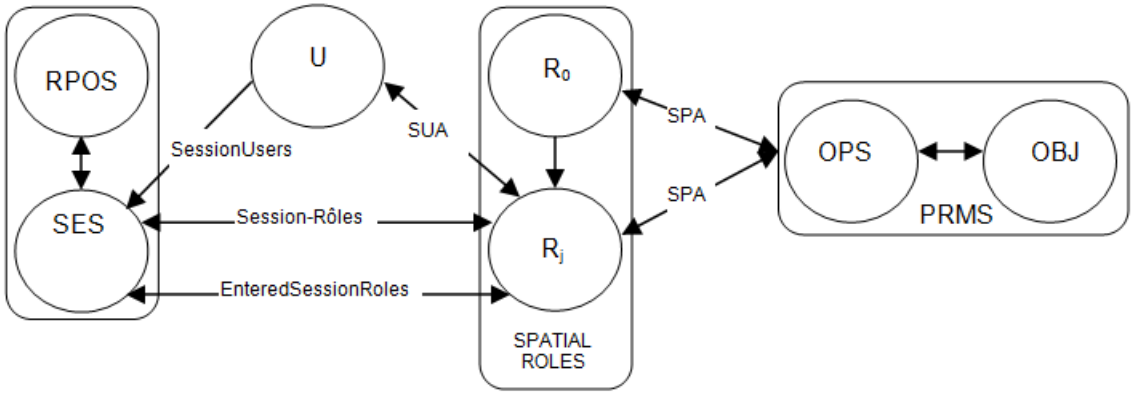

FIGURE 2.5.1 – Modèle GeoRBAC.

Les rôles sont activés dans des places bien déterminées pour limiter géographiquement l'utilisation des rôles. Le modèle a introduit la notion de rôle spatial correspondant au couple <role_name, extent>, c'est-à-dire qu'un rôle spatial est muni d'informations indiquant les localisations où le rôle peut être activé. Afin de valider l'approche, la spécification de Geo-RBAC a été découpée en quatre parties distinctes : Geo-RBAC cœur, Geo-HRBAC (hiérarchie) et Geo-RBAC avec contraintes (SOD et DOD). La localisation géographique est intégrée à la structure d'une politique de sécurité.

2.5.1.3 Modèle spatio-temporel

Pour gérer miex les droits d'accès, [Chen et al. 2008] ont proposé de combiner à la fois l'aspect spatial et temporel lors de l'activation des rôles et des permissions.

2.5.1.4 Context RBAC

[Park et al. 2006] ont été motivé par l'inclusion du concept de contexte, le modèle CRBAC a été proposé pour faire face aux exigences des applications des systèmes pervasifs, avec la prise en compte de la location de l'utilisateur, son état et horaire d'utilisation. La prise en compte du concept de contexte dans les politiques à base de rôles est un domaine de recherche très actif de nos jours .

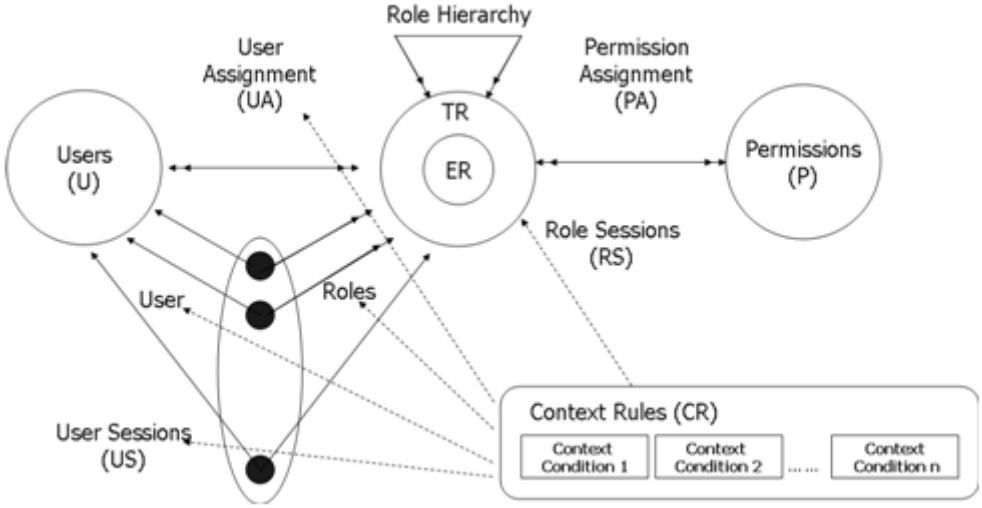

FIGURE 2.5.2 – Modèle CRBAC.

Les éléments du modèle CRBAC sont comme indiqué dans la figure 2.5.2 :

- Utilisateurs, Rôles, Sessions, Permissions, Operations et Objets sont les mêmes notions que dans le modèle RBAC,
- Contexte Rule (CR) : représente un ensemble de rôles contextuels. Le rôle contextuel est utilisé pour capturer des informations de contexte de sécurité pertinentes sur l'environnement pour une utilisation dans les politiques de contrôle d'accès. Le rôle contextuel peut être lié au temps, à la localisation, etc.
- Contexte (C) : sert à regrouper les informations contextuelles du système. L'ensemble « C » capture toutes les informations de contexte qui sont utilisées pour définir le rôle contextuel «CR». Les informations peuvent être le temps, la localisation, la température etc.

2.5.1.5 Modèle organisationnel OrBAC

[Miège 2005] propose un modèle organisationel OrBAC (Organisation Based Access Control) à été conçu pour intégrer plusieurs paramètres contextuels. Cela ajoute la dimension organisationnelle lors de la spécification de la politique de sécurité et la séparation entre le niveau concret (utilisateur, objet, action) et le niveau abstrait (rôle, vue, l'activité), l'intéraction entre ces différentes entités est illusttrée dans la figure 2.5.3. Le modèle OrBAC est une extension et une combinaison de différents modèles existants en structurant diverses entités de l'organisation tels que RBAC, VBAC, TBAC, Rule-BAC. Le modèle OrBAC permet l'expression d'autorisations, d'interdictions, d'obligations et de recommandations. Le contexte contient plusieurs paramètres lors de la validation des autorisations : spatiales, temporelles, provisoires, conditions préalables et déclarées par l'utilisateur. Le modèle est centralisé et ne garantit pas l'interopérabilité, l'hétérogénéité et la distribution.

FIGURE 2.5.3 – Structure du modèle OrBAC.

2.5.1.6 Modèle Mlti-OrBAC

[Abou el kalam et al. 2006] propose le Multi-OrBAC comme extension du modèle OrBAC qui se consacre à l'hétérogénéité, la distributivité et l'interopérabilité. Le Multi-OrBAC affecte les utilisateurs selon une nouvelle entité Rio (Rôle dans l'organisation) qui est une extension du modèle à base de rôle, ViO (vue dans l'organisation), AiO (action dans l'organisation) et CiO (contexte dans l'organisation) pour la spécification de la politique de sécurité.

2.5.1.7 Modèle Poly OrBAC

[Abo el kalam et al. 2006] proposent le Poly-OrBAC qui est une extension du modèle OrBAC qui vise à assurer la sécurité des interactions entre les

organisations. Ce modèle est basé sur deux éléments : modèle OrBAC pour spécifier les politiques locales de chaque organisation et la technologie des services Web pour fournir une plate-forme de collaboration et d'interopérabilité entre ces organisations.

2.5.2 Modèles de contrôle d'accès basés sur la confiance

Dans ces modèles, l'affectation des rôles aux utilisateurs se fait en fonction de la valeur du niveau de confiance afin de pouvoir recevoir une permission. Le niveau de confiance est calculé à base des compétences, comportement (historique) et d'autres connaissances sur l'utilisateur. L'affectation des rôles varie avec le changement de niveau de confiance.

2.5.2.1 Modèle Trust-RBAC

[Toahchoodee et al 2009] prposent le modèle Trust-RBAC qui est basé sur l'évaluation du niveau confiance (trustworthiness) des utilisateurs. Cette valeur est déduite d'une façon dynamique suivant le changement identifié dans le comportement de l'utilisateur, le modèle est schématisé dans la figure 2.5.4. Les entités principales du modèle sont :

- Utilisateurs : ils sont évalués avant d'être affectés aux rôles suivant leur niveau de confiance.
- Rôles : sont associés au niveau de confiance exigé pour qu'ils soient affectés.
- Permissions : sont associées avec le niveau de confiance nécessaire pour activer la permission à un utilisateur.

2.5.2.2 Modèle basé sur trust et risque

Le modèle met en lumière les similitudes entre la gestion de la confiance et de systèmes de contrôle d'accès distribués en démontrant comment le système de contrôle d'accès de OASIS et de sa langue de la politique basée sur les rôles peuvent être étendus à prendre des décisions sur la base de la confiance et de l'analyse des risques plutôt que sur la base d'informations d'identification seul [Dimmock et al. 2004]

2.5.3 Modèles de contrôle d'accès basés sur la préservation de la vie privée

2.5.3.1 Modèle Privacy-RBAC

[Dafa-alla et al. 2005] propose le modèle P-RBAC (Privacy Role Based Access Control) qui sert à incorporer la politique de la vie privé. Cette approche

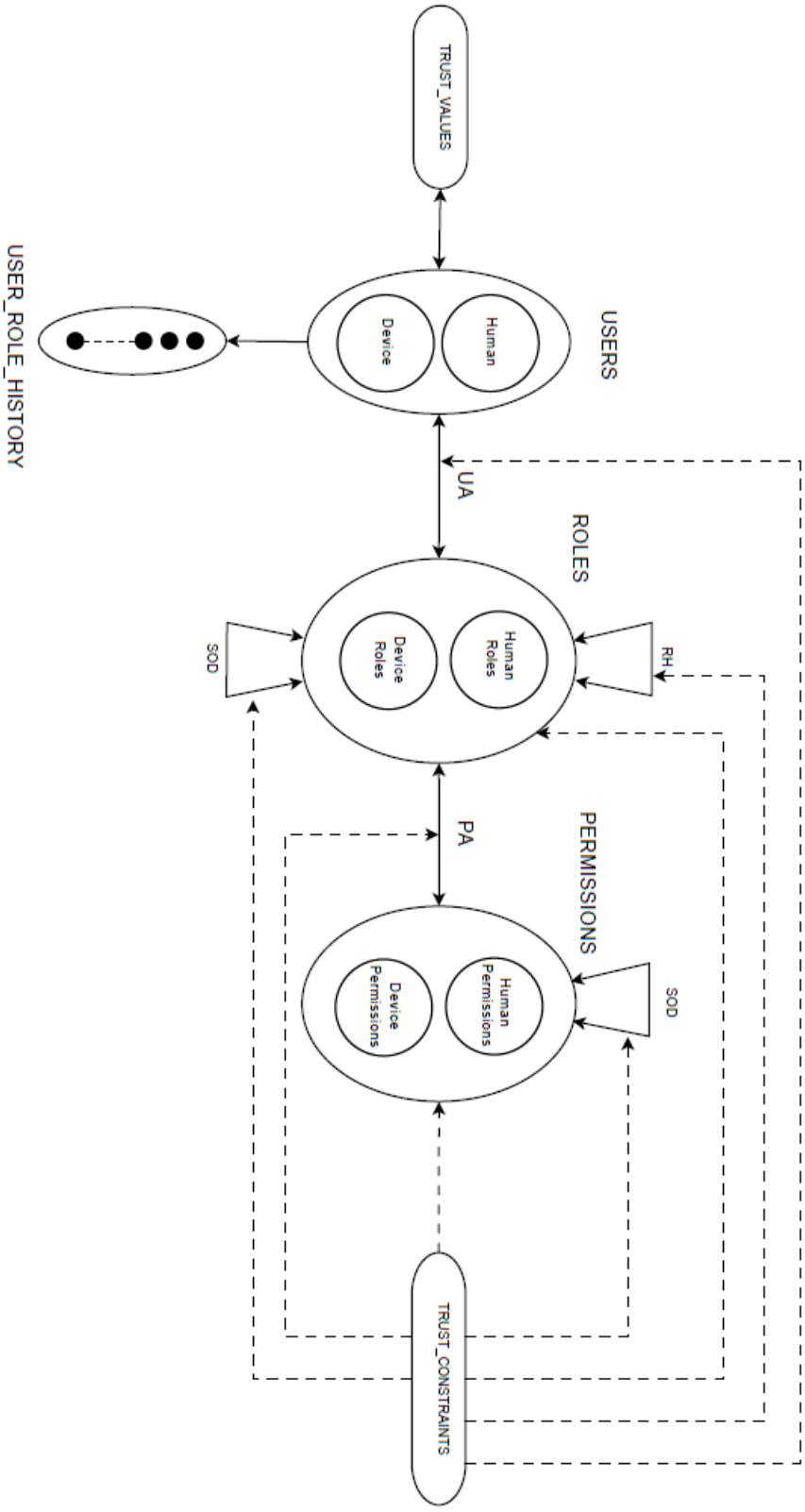

FIGURE 2.5.4 – Modèle Trust RBAC.

encapsule les données, action, but, état et obligation que la permission de données de la vie privée. Une attribution de l'autorisation dans P-RBAC est une cession de l'autorisation de données de la vie privée à un rôle. En outre, des conditions plus complexes ont été considérées dans une version conditionnelle de P-RBAC rapport à P-BAC, le soutien de la contrainte et obligations conditionnelles dans le modèle permet une définition de politique de confidentialité plus concise. P-RBAC nécessite de spécifier explicitement toutes les conditions lorsque les données sensibles de la vie privée peuvent être accessibles.

2.5.3.2 Modèle basé sur la protection de la vie privée

Ils proposent des protocoles de confidentialité préserver pour le contrôle d'accès basé sur les rôles (RBAC) dans l'environnement SOA. L'analyse de la sécurité démontre que nos protocoles sont la vie privée protégée. En outre, la mise en œuvre des protocoles proposés sont compatibles avec les standards SOA actuelles et des technologies telles que XACML et SOAP [Cheung et al. 2014].

2.5.4 Modèles de contrôle d'accès contextuels basés sur l'aspect sémantique

Dans nos jours, la technologie du web sémantique a eu un grand champ d'application dans le domaine de contrôle d'accès. Les modèles cités précédemment négligent l'aspect sémantique lors de la fusion des données contextuelles. Dans cette section, on présente quelques modèles qui exploitent cette technologie ainsi que les ontologies pour la spécification d'une politique de sécurité.

2.5.4.1 Modèle SBAC

[Toninelli et al. 2006] intègrent l'aspect sémantique dans leur modèle sémantique (SBAC) qui est formé de trois entités : les sujets qui sont des entités actives exerçant une demande d'accès, les objets qui sont des entités passives accessibles et / ou modifiés par l'objet et les actions qui sont les opérations effectuées sur l'objet. Chaque entité est modélisée par une ontologie : sujets-ontologie (SO), objets-ontologie (OO) et actions-ontologie (AO). Le langage OWL est utilisé pour la représentation de ces concepts, les règles d'autorisation sont sous la forme de (S, O, +/- A) où S, O, A sont définis respectivement dans les ontologies SO, OO et AO. Dans SBAC, les décisions sont déduites via le moteur d'inférence utilisant les ontologies et des règles explicites stockées dans la base d'autorisation (AB) sous forme de règles d'autorisation implicites exprimées au moyen du langage SWRL dans le but de déterminer si la requête est autorisée ou non dans le modèle SBAC.

2.5.4.2 Modèle ROWLBAC

[Finin et al. 2008] proposent le modèle ROWLBAC qui vise à combiner RBAC comme modèle et OWL comme langage. Le modèle RBAC est un référenciel pour la mise en place de la sécurité et le langage OWL est une norme W3C qui est largement utilisée pour exprimer les vocabulaires de domaine. Auparavant, OWL a été utilisé dans le développement de langages de spécification tels que Rei et Kaos dont le but est de définir des ontologies qui peuvent être utilisées pour représenter le modèle de sécurité RBAC et de montrer comment ils peuvent être utilisés pour spécifier et mettre en œuvre un système de contrôle d'accès. La spécification d'entités est basée sur le langage OWL, chaque entité est modélisée séparément par une ontologie spécifique (sujets, objets, rôles, assignation des rôles et actions).

2.5.4.3 Modèle TSBAC

[Ravari et al. 2008] ont intégré l'aspect temporel (TSBAC) qui est une extension du modèle sémantique (SBAC) qui vise à renforcer ses capacités en prenant l'historique des accès au système. Le modèle utilise les mêmes relations sémantiques de SBAC. Il est capable d'utiliser les relations temporelles entre les évènements d'accès qui se sont produits dans le passé (composées comme une expression temporelle) en spécifiant les règles d'autorisation. Dans ce modèle, un aspect dynamique est également associe aux autorisations en fixant un intervalle de temps qui limite la durée de validité pour chacune des autorisations.

2.5.5 Modèles de contrôle d'accès contextuels basés sur les technologies d'intelligence artificielle

Dans ce groupe, on présente les modèles de contrôle d'accès dynamiques avec l'intégration de la technologie de l'intelligence artificielle. On se limite à la présentation de deux extensions du modèle RBAC avec la combinaison des réseaux de neurones et des systèmes multi-agents.

2.5.5.1 Modèle basé sur les réseaux de neurones

[Lim et al. 2007] ont raffiné le modèle RBAC, en appliquant l'algorithme des réseaux de neurones afin de rendre le modèle intelligent lors de prise de décision avec la prise en compte des préférences des utilisateurs.

2.5.5.2 Modèle basé sur les systèmes multi-agents

Pour assurer l'aspect intelligence, il y a des travaux qui ont préféré d'utiliser l'approche des systèmes multi agents. Dans [Omicini et al. 2004] ont ajouté au modèle RBAC un nouveau concept est celui de l'agent coordinateur de

contexte ayant pour but d'interagir avec l'environnement et de coordonner les informations contextuelles.

2.6 Conclusion

Dans ce chapitre, on a présenté les services de sécurité (authentification, autorisation, gestion de confiance et la préservation de la vie privée), un état de l'art sur les modèles de contrôle d'accès statiques et dynamiques. Plus particulièrement, l'étude est focalisée sur les modèles de contrôle d'accès dynamiques qui dépendent de la validité des données contextuelles, la confiance, la préservation de la vie privée, l'aspect sémantique et d'autres technologies d'intelligence artificielle pour attribuer les droits d'accès. Ces extensions sont considérées comme des approches les plus effectives pour le contrôle d'accès dans les systèmes pervasifs. En outre, on note le besoin de la prise en compte de la personnalisation et l'adaptation de la sécurité au niveau des systèmes intelligents dédiés pour les personnes âgées dépendantes.

Partie 2 : Développement et Validation de la Politique de Sécurité

Chapitre 3

Modèle de contrôle d'accès proposé (UBC-ACM)

Grâce à la sensibilité au contexte et l'intelligence ambiante dans nos environnements actuels, les services fournis de nos jours sont devenus plus ubiquitaires et personnalisés en fonction du profil de l'utilisateur. Avec le progrès des applications sensibles au contexte à distance, de santé et de bien-être, la modélisation de politiques de sécurité devient un enjeu important dans la conception des futurs modèles de contrôle d'accès. Un aspect sémantique riche, utilisant les ontologies dans la modélisation et la gestion des services offerts aux personnes dépendantes, est nécessaire. Cependant, les modèles de contrôle d'accès actuels restent inadaptés en raison du manque d'exhaustivité, de flexibilité et d'adaptabilité à la capacité et au comportement d'utilisateur.

Dans ce chapitre, on présente notre modèle de contrôle d'accès basé sur le comportement et la capacité de l'utilisateur afin d'accorder un service en utilisant n'importe dispositif inclu dans l'environnement intelligent. Cette politique est définie via notre nouveau modèle de contrôle d'accès adaptable nommé (UBC- ACM). La conception de notre modèle est basée sur une ontologie évolutive pour prédire les actions futures des personnes dépendantes.

3.1 Cadre de l'approche proposée

Les systèmes pervasifs contribuent significativement au déploiement de services personnalisés au niveau des systèmes intelligents. En prenant en considération les personnes dépendantes dans leurs espaces de vie, les exigences en matière de sécurité restent un domaine de recherche ouvert. Tandis que les environnements pervasifs soulèvent de nouveaux problèmes de sécurité, ils apportent également de nouvelles possibilités en raison de technologies ubiquitaires et de l'intelligence ambiante qui fournissent des informations contextuelles utiles sur l'utilisateur et son environnement. L'authentification et le contrôle d'accès sont les principaux services de sécurité nécessaires pour véri-

fier l'identité des utilisateurs et les ressources auxquelles ils peuvent accéder. Une sécurité basée sur la sensibilité au contexte est une approche émergente pour faire face aux nouveaux problèmes de sécurité engendrés par la haute dynamicité et l'hétérogénéité des dispositifs mobiles qui caractérisent les environnements ubiquitaires. Grâce aux technologies des capteurs, la sensibilité au contexte nous permet d'obtenir des données contextuelles plus précises sur le profil de l'utilisateur et son environnement. Un environnement ubiquitaire se caractérise par la richesse des contextes dans lesquels les utilisateurs, les dispositifs et les agents sont mobiles. La disponibilité des données contextuelles fournies par les capteurs peut être utilisée pour extraire le comportement des entités mobiles (utilisateurs, dispositifs, agents). La sensibilité au contexte peut apporter une aide précieuse pour comprendre la relation entre les utilisateurs, les dispositifs et les environnements. En raison de la grande étendue et la variété de capteurs déployés, l'espace ubiquitaire peut fournir un ensemble d'informations très riche et précieux qui peut être utilisé pour calculer le "profil dynamique" des utilisateurs (relation sociale et le comportement des utilisateurs).

En combinant le profil dynamique avec les capacités des utilisateurs, notre stratégie de recherche est motivée par les tâches suivantes :

1. Identification de l'utilisateur de manière discrète et transparente.
2. Fourniture de service adaptable aux utilisateurs en fonction de leurs capacités et comportements afin d'assurer plus de personnalisation et de sécurité appropriée.

L'objectif de notre approche est la conception et la mise en œuvre d'un système de sécurité sensible au contexte illustré dans la figure 3.1.1.

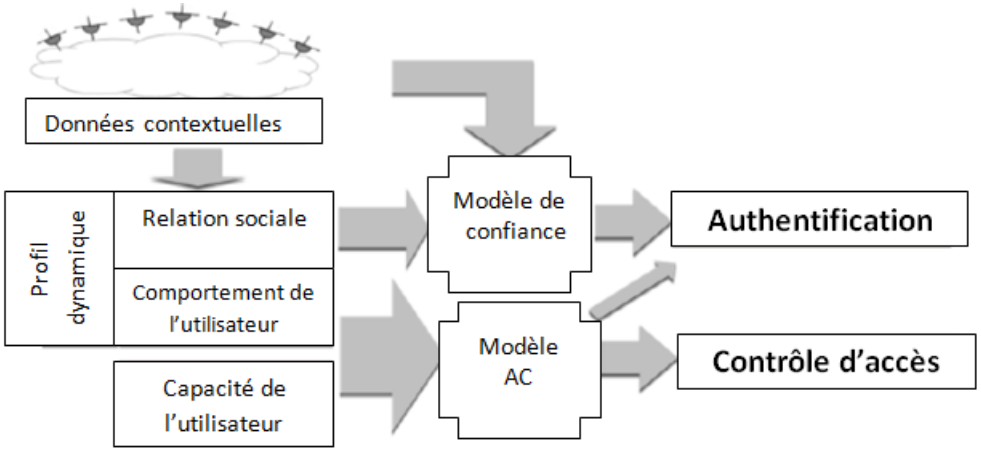

FIGURE 3.1.1 – Positionnement de notre approche de sécurité.

Notre approche permet d'assurer à la fois l'authentification et l'autorisation [M'hamed et al. 2013] :

Authentification : Nous passons à la personnalisation de la personne dépendante, les moyens d'identification utilisés sont pour la plupart le mot de passe et les données biométriques. Les présentes informations d'identification ne permettent pas une personnalisation adaptée et une bonne identification sur le profil de l'utilisateur. Tout d'abord, nous avons besoin d'identifier correctement la personne en vérifiant la capacité de l'utilisateur et le profil en fonction de la surveillance des comportements. En second lieu, pour obtenir la décision d'authentification appropriée, on utilise des règles d'inférence sur les données contextuelles.

Autorisation : C'est un moyen pour attribuer des décisions appropriées (autorisations, interdiction, obligation et recommandation) aux personnes autorisées nécessitant un service d'assistance. Cela dépend de la validité du contexte, du profil, de la capacité, des données comportementales et des règles définies qui permettent de raisonner sur le contrôle d'accès. Les connaissances inférées permettent une meilleure caractérisation des utilisateurs vivant dans une maison intelligente et ayant des besoins particuliers.

3.2 Motivations & Challenges

Notre approche vise à répondre aux besoins des personnes âgées dépendantes, en faisant face aux exigences suivantes :

Personnalisation : Cet aspect est assuré au moyen de la prise en compte du modèle utilisateur qui représente une structure de connaissances sur l'utilisateur.

Adaptation : Cet aspect est pris en compte par l'identification des différentes situations critiques que notre approche doit gérer pour la prise de la bonne décision.

Sensibilité au contexte : l'intégration de sources multiples pour l'acquisition de données contextuelles pour assurer une inférence des droits d'accès plus riche.

Intelligence : L'assurance des fonctionnalités de personnalisation, adaptation et de prise en compte de tout changement survenant dans l'environnement ou au niveau du comportement utilisateur. Cela confère une intelligence au modèle de contrôle d'accès.

3.3 Modélisation d'utilisateur ubiquitaire

Dans les systèmes intelligents destinés à l'assistance et à la surveillance, la personnalisation et l'adaptation aux besoins des utilisateurs sont indisponsables. A cet effet, il est nécessaire de connaitre et de définir toute information concernant l'utilisateur (objectifs, préférences, intérêts, connaissances . . .) ainsi que le contexte d'interaction avec son environnement. L'ensemble de ces données est désigné référencés par le concept de « Modèle d'utilisateur ». Celuici est défini comme « une représentation explicite du système et des caractéristiques de l'utilisateur qui sont nécessaires au processus de personnalisation » [Kobsa 1993].

Ces modèles sont construits par le processus de «modélisation d'utilisateur», où il est considéré comme étant l'inférence d'informations inobservables concernant l'utilisateur à partir des informations observables (ses actions, son comportement, etc) [Kobsa 2001]. Les premiers travaux qui ont focalisé leur systèmes sur «Profil Utilisateur » sont ceux de [Kobsa 2001] [Von et al. 2006] pour la conception des systèmes de dialogue en langage naturels. Kobsa considère un modèle d'utilisateur comme étant la source de connaissances pour les systèmes de dialogue « langage naturel» qui contiennent des caractéristiques explicites de l'utilisateur facilitant l'adaptation.

Pour fournir un service à un utilisateur spécifique, le système doit définir un « Profil Utilisateur » qui est une instance d'un Modèle Utilisateur [Von et al. 2006] par les propres valeurs d'un utilisateur. Suivant [Kadouche 2007], un "Profil Utilisateur " est défini comme étant un simple Modèle Utilisateur où les entités constituant le modèle utilisateur sont assignées à des valeurs de type différents (Booléennes, Numériques, Caractères).

Un modèle d'utilisateur est construit sur la base de deux types de données : statiques et dynamiques.

- Données statiques : se sont les données qui ne changent pas avec les temps telles que (données personnelles, informations sur le travail, ...).

- Données dynamiques : se sont les données qui changent avec le temps telles que (préférences, objectifs, données contextuelles (emplacement géographique), connaissances).

La personnalisation et l'adaptation exigent la prise en compte, lors de construction d'un modèle utilisateur, des attributs suivants [Kadouche 2007] et [Garlatti et al. 2004] :

- Connaissances : il est nécessaire de savoir ce que l'utilisateur connait ou pas. Ce paramètre est de nature dynamique car l'utilisateur toujours acquiert de nouvelles connaissances.

- Compétences et expériences : représentent le savoir faire d'un utilisateur dans un tel domaine.

- Préférences : ce sont des informations déclarées par l'utilisateur qui ne peuvent être déduites par le système et sont propres à chaque utilisateur.

- Objectifs : représentent les tâches ou ce que l'utilisateur souhaite atteindre.

- Comportement : avec les nouveaux dispositifs intégrés dans l'environnement, il est devenu possible de garder trace ou d'enregistrer le comportement utilisateur pour qu' il soit exploité avec l'utilisation de techniques de l'intelligence artificielle pour extraire d'autres informations de haut niveau (habitudes, besoins, situation, activité, position, ...).

- Contexte d'interaction : représente les données issues de chaque capteur tels que l'emplacement, le temps, etc.

Cependant, le modèle utilisateur doit être évolutif et tenir en compte de tous les changements survenus au fil du temps.

La représentation de données joue un rôle important pour aboutir à l'assurance de la personnalisation. Dans l'état de l'art, on a présenté les différentes techniques utilisées pour la représentation de données. Actuellement, la technique la plus adaptée répondue aux exigences des systèmes intelligents, est celle basée sur la technologie du web sémantique qui permet de formaliser la sémantique des connaissances structurées dans un modèle.

L'assurance de la personnalisation et l'adaptation dans un modèle de contrôle d'accès pour un système intelligent, exige de définir un modèle d'utilisateur riche incluant plus d'informations qui caractérisent l'utilisateur.

3.4 De la sensibilité au contexte au suivi de comportement dans le Contrôle d'Accès

Le développement de notre approche a été largement motivé par l'identification des besoins des personnes âgées dépendantes aux systèmes de santé ubiquitaires. Par conséquent, dans notre modèle de contrôle d'accès dynamique, la gestion des droits d'accès est conditionnée par l'exploitation des données contextuelles issues de sources multiples. Les premiers systèmes sensibles au contexte ont utilisé des données contextuelles simples mesurées directement par les capteurs ou inférées depuis des données de bas niveau. Les extensions des modèles RBAC sont basées sur la sensibilité au contexte. Leur but est

d'améliorer RBAC en attribuant les droits d'accès d'une façon dynamique. L'accès est basé sur la validité du contexte, en ajoutant à RBAC des données contextuelles : spatiales, temporelles ou environnementales.

Grâce au développement constaté dans l'évolution des dispositifs, les informations contextuelles deviennent de plus en plus riches, et vue la possibilité d'utilisation des techniques d'intelligence artificielle et de fouille de données pour extraire des connaissances cachées ou implicites ; cette voie de recherche a apporté de nouveaux aspects en terme d'intelligence. Par ce progrès constaté dans la recherche, on vise à assurer une sécurité personnalisée et adaptative aux besoins identifiés des utilisateurs.

L'assurance de la sécurité et sûreté aux personnes âgées dépendantes, nous impose donc, l'exploitation des données contextuelles issues de capteurs embarqués dans l'environnement et d'autres issues de capteurs portés par l'utilisateur. En terme de sécurité, il est nécessaire de garder les traces du comportement de l'utilisateur afin d'identifier toutes les habitudes et les comportements afin de miex prendre en compte les besoins des utilisateurs adaptant et personnalisant la fourniture des services. Pour cette raison, on est passé de l'adaptation selon les changements détectés au niveau des données contextuelles vers la reconnaissance d'activité et maintenant on se dirige vers le suivi de comportement [Favela 2012] [Tentori et al. 2008]. On adapte notre processus de contrôle d'accès suivant les changements détectés dans le comportement et le profil de l'utilisateur.

3.5 Rôle du web sémantique dans le contrôle d'accès

Le web sémantique est une évolution importante qui fournit un framework commun en matière de partage et de réutilisation d'information dans les applications émergentes. Cette technologie joue un rôle important dans les architectures de sécurité lors de la capture des aspects d'hétérogénéité et de distributivité. Le modèle RBAC est à la base de toutes les approches de gestion des nouveaux besoins de sécurité introduits par la forte dynamicité et l'hétérogénéité des dispositifs mobiles qui caractérisent les environnements pervasifs et dynamiques. Différentes contributions ont été apportées dans le développement, l'élaboration et la mise en œuvre des extensions du modèle RBAC et leurs fonctionnalités, mais peu ont tenu en compte le fait d'avoir un modèle de contrôle d'accès de référence RBAC unifié.

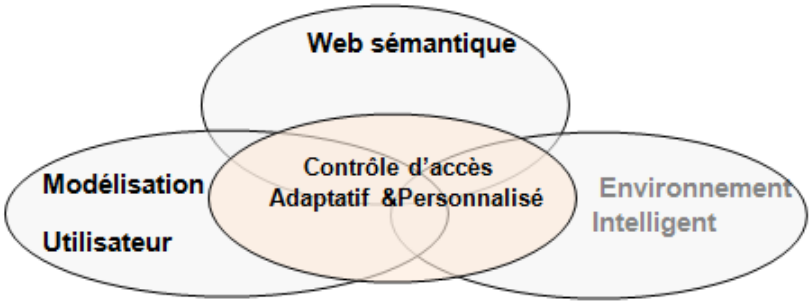

FIGURE 3.5.1 – Interaction des domaines pour un meilleure contrôle d'accès.

Il n'existe aucune source complète qui décrit le cadre général de RBAC comme guide pour les développeurs qui veulent ajouter des contributions au modèle. Un cadre général devrait, entre autres, fournir des outils pour intégrer les différentes contributions de l'élaboration de RBAC. Cependant, la création d'une ontologie commune peut simplifier le travail des développeurs en fournissant un langage indépendant de la plateforme pour la spécification souple des politiques de contrôle. Une description sémantique via une ontologie peut servir à intégrer et faciliter la conception de futures extensions de RBAC. Pour remédier à ces problèmes, on note que l'exploitation de la technologie du web sémantique peut faciliter le déploiement de nouvelles extensions du modèle RBAC. L'assurance d'une meilleure sécurité, cela nécessite l'intéraction de différents domaines (modélisation utilisateur, web sémantique, environnement intéligents) comme illustré dans la figure 3.5.1.

3.6 Politique de sécurité

La conception des modèles de contrôle d'accès est en progrès continu incluant de nombreuses sources de données contextuelles. Cependant, notre contribution est liée au niveau de la conception de la politique de sécurité où le modèle de contrôle d'accès et son architecture sont basés sur la capacité et le comportement qui nécessitent les processus de gestion de contexte suivants : acquisition, modélisation, raisonnement et adaptation.

Notre politique de sécurité ciblée [Zerkouk et al. 2014] est réactive, personnalisée et adaptative à la capacité, à situation, au contexte de l'utilisateur et aux changements de l'environnement survenus. Les décisions ne sont pas limitées à " permis " ou " refusé " comme décision de contrôle d'accès. Afin de délivrer un service d'assistance aux personnes dépendantes, notre politique est étendue pour inclure des décisions plus appropriées : Permission, Obligation, Recommandation ou Interdiction (figure 3.6.1). Les bonnes décisions sont attribuées

en fonction du comportement historique analysé, contexte actuel, situation critique détectée et capacité. Ce contexte complexe est déduit en raison de la richesse des données contextuelles collectées à partir de la plate-forme de télé-surveillance.

Notre modèle de contrôle d'accès vise à mettre en œuvre notre politique de sécurité au moyen de la prise en compte des avantages d'ontologie en matière de modélisation, de raisonnement et d'interrogation, en prenant en considération l'aspect sémantique et l'hétérogénéité des données détectées qui ne se limitent pas à des dispositifs environnementaux. La richesse des données contextuelles utilisées provient de la combinaison de l'environnement et les données du patient recueillies à partir de notre plate-forme de télé-surveillance au moyen des systèmes RFPAT et GARDIEN. La plate-forme de Télé-surveillance permet l'enregistrement du comportement historique qui est utilisé pour analyser en profondeur les activités de l'utilisateur surveillé et de fournir un système sensible au contexte réactif afin d'assurer une meilleure assistance personnalisée aux personnes dépendantes. Par conséquent, les données générées ont permis de valider notre politique de sécurité (voir chapitre 5).

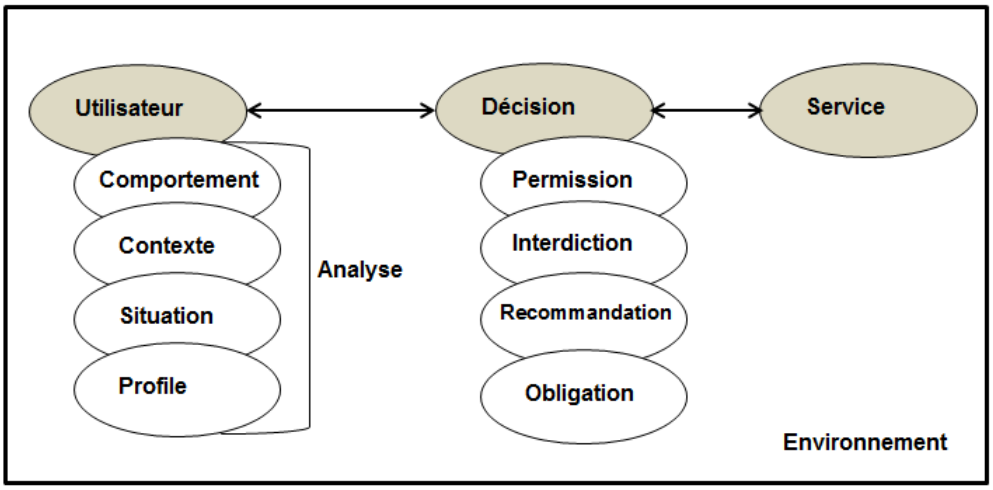

FIGURE 3.6.1 – Politique de sécurité.

Notre politique de contrôle d'accès est définie par (formule 3.6.1) :

$$Politique =< Bi(t), Ctx(t), St(t), Pr(t-1), Cpb], S, Dk > \qquad (3.6.1)$$

Les décisions sont attribuées en fonction de la combinaison des paramètres suivants et leurs valeurs :

- Comportement ($Bi(t)$) : représente ce que l'utilisateur effectue à l'instant (t) comme : marcher, s'allonger ou autre activité où $Bi(t)\_[B0, ..., B5]$.
- Contexte actuel $Ctx(t)$: correspond aux données détectées à un instant t. Elle décrit l'utilisateur et l'état de l'environnement acquis au moyen de dispositifs portables et embarqués. Les valeurs de contexte sont : temps, pouls, posture, emplacement. $Ctx(t) = C1, ..., Cn$.
- Situation $St(t)$: représente les situations de sensibilité qui sont identifiées par le comportement détecté. Dans notre travail, nous avons identifié six comportements sensibles qui sont : hypertension, normale, critique, hypotension, anormal, urgence (chute soudaine).
- Profil de l'utilisateur $Pr(t-1)$: Il est nécessaire pour vérifier si l'utilisateur a déja subi une chute avant ou pas.$Pr(t-1) = chuteur, cardiopath.$
- Capacité (Cpb) : représente les déficiences types : surdité, cécité, ...
- Service (S) : représente le service demandé par l'utilisateur avec certaines contraintes d'accès.
- Décision (Dk) : représente l'analyse de l'état de l'utilisateur, puis une décision est attribuée en fonction de la politique mise en place.

$Dk - \{Autorisation, Interdiction, Obligation, Recommendation\}$

3.7 Modélisation

Le domaine de la représentation des connaissances est devenu un axe de recherche très actif qui a donné lieu à différentes contributions et a attiré l'attention de différents développeurs dans différents domaines.

Afin d'avoir une base de connaissances, un système nécessite un langage de spécification permettant de coder les connaissances dans la base. Un tel système est capable de fournir des services permettant d'inférer les connaissances implicites à partir des connaissances explicites stockées dans la base[Le Duc 2004] [Shehzad et al. 2004] . Par conséquent, la technologie du web sémantique répond à nos besoins et exigences en termes de modélisation et de raisonnement.

3.7.1 Techniques de modélisation

Dans la partie état de l'art (chapitre 1), nous avons cité les différentes techniques utilisées dans la littérature pour le processus de modélisation. Dans le développement de notre approche, on a opté pour la technologie du web sémantique (ontologies) en raison de leurs avantages en termes de modélisation et de raisonnement.

3.7.1.1 Web sémantique

Pour faire face aux exigences et les besoins applications intelligentes, on a souvent recours aux technologies du web sémantique qui contribuent au développement de nouvelles approches. Selon Tim Berners Lee, le web sémantique a été conçu dans le but d'échanger les données d'une manière plus efficace et fiable. L'objectif du Web Sémantique est de rendre le contenu du Web compréhensible à des machines car il se base sur des langages standards pour la description des ressources.

Cette technologie consiste à exploiter [Charlet et al. 2004] [WS 2015] :

• Des ontologies : une ontologie est un vocabulaire constitué de concepts, relations et axiomes liés à un certain domaine.

• Un langage commun pour exprimer les ontologies et décrire des annotations utilisant les termes de ces ontologies.

• Des moteurs de raisonnement permettant d'inférer sur les annotations d'après les axiomes déclarés dans les ontologies.

Le web sémantique fournit les moyens de faire :

• L'automatisation de nombreuses tâches fondées sur le contenu comme la recherche de ressources ayant un contenu particulier, la comparaison du contenu des ressources (pages, bases de données, ontologies, etc...).

• Le Web sémantique permet de résoudre la relative difficulté de trouver de l'information sur le web.

• La description de ressources informatiques (services) par leurs conditions d'activation, leurs résultats, leurs qualités, etc...

3.7.1.2 Ontologies

Les ontologies sont un moyen de représentation des connaissances, des concepts et leurs interrelations. Selon [Gruber 1993], propose la définition suivante : « Spécification explicite d'une conceptualisation ». Ainsi, [Studer et al. 1998] définit l'ontologie comme une « spécification formelle et explicite d'une conceptualisation partagée » :

Formelle : l'ontologie doit être lisible par une machine, ce qui exclut le langage naturel.

Explicite : la définition explicite des concepts utilisés et des contraintes de leurs utilisations.

Conceptualisation : le modèle abstrait d'un phénomène du monde réel par identification des concepts clefs de ce phénomène.

Partagée : l'ontologie n'est pas la propriété d'un individu, mais elle représente un consensus accepté par une communauté d'utilisateurs.

Une ontologie représente un quintuplet : $O := \{C, R, H^c, Rel, A^o\}$ où :

- C : représente un ensemble de concepts permettant la description des objets d'un domaine. Les concepts peuvent être abstraits ou concrets, élémentaires ou composés, réels ou fictifs. Généralement, les concepts peuvent être organisé en taxonomie ou hiérarchie de concepts reliés entre eux en fonction de critères sémantiques particuliers.
- R : représente les relations ou les liens organisant les concepts d'un domaine.

- H^c : représente une hiérarchie de concepts $H^c(C_1, C_2)$, signifie que C_1est un sous concept de C_2.
-*Rel* : représente des cas particuliers des relations dans lesquelles le nième élément de la relation est unique pour les n-1 précédents.
-A^o : représente un ensemble d'axiomes logiques permettant de définir la sémantique des concepts et des relations. Ces axiomes sont exprimés en langage logique.

3.7.1.3 OWL

En 2004, OWL (Web Ontology Language) devient une recommandation du W3C (World Wide Web Consortium). L'OWL découle de RDF (Resource Description Framework) et RDFS (RDF schéma), possède des connecteurs logiques, il permet d'exprimer des cardinalités sur les propriétés et d'en spécifier la nature [Giudicelli 2011]. Ce langage se base sur les notations illustrées dans la table 3.1.

Une ontologie est formalisée en OWL, comprend Un espace de nom : L'entête <owl :Ontology> pour décrire l'ontologie. Celle-ci permet la définition des classes, des propriétés et des instances

OWL LITE : permet d'établir une hiérarchie de concepts et contraintes simples.

OWL DL (DL pour description logic) : comprend toutes les structures de OWL, possède une expressivité plus importante, avec complétude de calcul.

OWL FULL expressivité maximale, liberté syntaxique sans garantie de calcul, une classe peut aussi correspondre à l'instance d'une autre classe.

3.7.2 Outil de modélisation (développement)

Parmi les outils de modélisation, on distingue des éditeurs graphiques (Protégé) ou des interfaces de programmation (Jena).

3.7.2.1 Protégé 2000

L'éditeur Protégé est conçu en 1995 à l'Université de Stanford [Protégé 2015] [Onto_OWL 2015]. C'est un outil graphique qui permet de créer des modèles de connaissances. Un modèle se compose d'un ensemble de classes organisées hiérarchiquement, de slots décrivant les attributs et les propriétés de ces classes

Syntaxe	**Sémantique**	**Description**
A	$A^I \subseteq \triangle^I$	Concept atomique
R	$R^I \subseteq \triangle^I \times \triangle^I$	Rôle atomique
$\top$	$\triangle^I$	Concept subsumant tous les autres (plus général)
$\bot$	$\emptyset$	Concept vide (plus spécifique)
$\neg A$	$\triangle^I \setminus \triangle^I$	Négation atomique
$C \sqcap D$	$C^I \sqcap D^I$	Intersection
$C \sqcup D$	$C^I \sqcup D^I$	Union
$C \sqsupseteq D$	$C^I \sqsupseteq D^I$	Subsomption
$\forall R.C$	$a \in \triangle^I \mid \forall b.\,(a,b) \in R^I \Longrightarrow b \in C^I$	Restriction de valeur
$\exists R.C$	$a \in \triangle^I \mid \exists b.\,(a,b) \in R^I \wedge b \in C^I$	Quantificateur existentiel
$\geq n\ R$ $\leq n\ R$	$a \in \triangle^I \mid\mid b \mid (a,b) \in R^I \mid \geq n$ $a \in \triangle^I \mid\mid b \mid (a,b) \in R^I \mid \leq n$	Restriction de nombre

TABLE 3.1 – Concepts et notations logiques

et enfin d'instances de classes. Il est caractérisé par son architecture modulaire, flexible et permet l'intégration de nombreux langages (OWL, OWL 2, DAML+OIL, etc.) et plugins (Protégé-OWL) spécialement adapté au format OWL. Il permet notamment de visualiser, éditer ou ajouter des classes, des instances et des propriétés OWL ainsi que d'inférer de nouveaux faits grâce aux raisonneurs (Hermit, Pellet, etc.) directement intégrés. L'éditeur Protégé-OWL permet aux utilisateurs :

- de charger et d'enregistrer des ontologies (OWL et RDF).
- de modifier et de visualiser des classes, des propriétés et des règles SWRL (Semantic Web Rule Language).
- d'inférer et de raisonner sur des données hétérogènes.

La figure 3.7.2 montre notre modèle initial conçu sous Protégé et montrant les entités principales (classes, propriétés et objets) de notre ontologie.

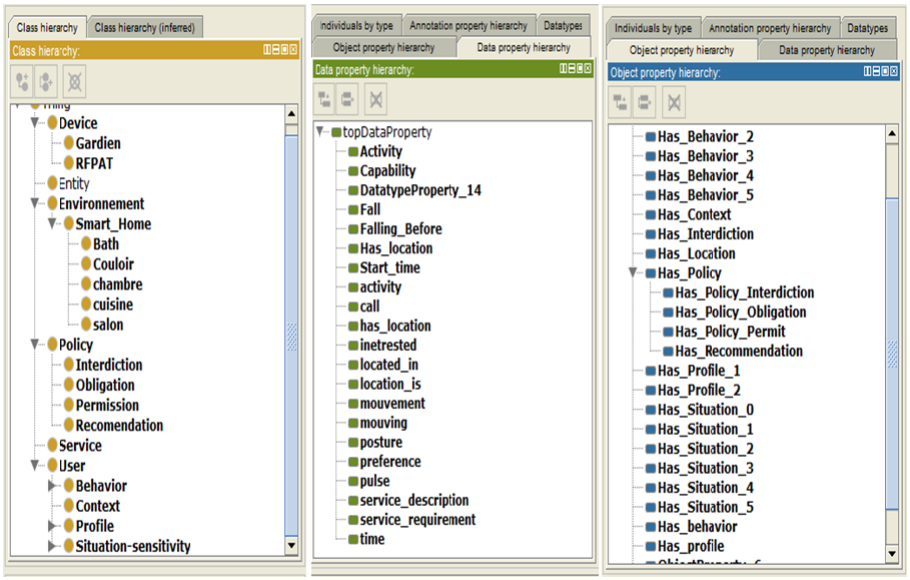

FIGURE 3.7.1 – Création de l'ontologie initiale (classes, propriétés et objets).

3.7.2.2 Jena

L'API (Interface d'application de programmation) Jena est un Framework Open Source développé en langage Java, conçu pour construire des applications destinées au web sémantique [Carroll et al. 2004]. Il intègre une variété de normes RDF, RDFS et OWL, SPARQL et inclut un moteur d'inférence. Il permet notamment la création et la manipulation de graphes dans différents formats (OWL, RDF, etc.) où il peut intégrer des moteurs d'inférence tels que Pellet et Racer. Le modèle conçu par l'outil Protégé, peut être manipuler avec l'API Jena comme le montre le fragment de code suivant. On note que cette manipulation est mise en pratique sous Eclipse comme illustré dans le code ci-dessous.

Algorithme 3.1 Manipulation de l'ontologie via Jena.

```
///Loading the ontology
InputStream in = new FileInputStream(new File
("C:\\Users\\CONNEXION\\Desktop\\Policy.owl"));
InputStream in = new FileInputStream(new
File ("D:\\ZERKOUK\\Meriem\\Desktop\\ontology_workspace\\
      ontology workspace\\DemoAdep.owl"));
OntModel model2 = ModelFactory.createOntologyModel
                  ( OntModelSpec.OWL_MEM);
model2.read( in, null);
in.close();
System.out.println(" ");

  // listing classes
Iterator i = model2.listHierarchyRootClasses().
             filterDrop(new Filter()
{
 public boolean accept( Object o )
      {
      return ((Resource) o).isAnon();
       }
} );
while (i.hasNext()) {
System.out.println(i.next().toString());}
```

3.7.3 Modélisation des entités de notre approche

Le modèle proposé UBC-ACM (User Behavior Capability- Access Control Model) est basé sur l'expérimentation de comportements de l'utilisateur selon les différentes situations qui peuvent se produire. Sur la base de l'étude réalisée précédemment, nous avons identifié six classes de comportement. Les données utilisées sont issues de différents capteurs hétérogènes. Ainsi, un aspect sémantique est nécessaire pour faire face à l'expressivité de façon formelle. Toutefois, les ontologies sont choisies comme moyen de réaliser notre politique de sécurité pour l'expressivité formelle, la réutilisation, l'hétérogénéité et l' interopérabilité. Le modèle proposé est une ontologie.

L'ontologie proposée est définie par les technologies du web sémantique, elle est décrite avec le langage Web (OWL), les règles de contrôle d'accès sont exprimées par le langage SWRL (Sémantic Web Rule Langage) et les décisions sont récupérées par le protocole et le language de requêtes SPARQL

(simple et RDF (Resource Description Framework) Query Language). Ces outils standards ont été utilisés pour définir, représenter et mettre en œuvre notre modèle dans un environnement intelligent.

Notre cadre conceptuel de la politique de contrôle d'accès sémantique est basé sur la définition d'une base de connaissances, ABOX et TBOX pour rajouter l'aspect sémantique et formaliser nos concepts. En fait, l'ontologie de la politique de sécurité est constituée en combinant les principales entités : utilisateurs, dispositifs, services et environnement. L'interaction entre les entités définies est assurée par la définition des relations sémantiques.

Nous nous sommes basés sur les travaux de [Kadouche et al. 2008] pour modéliser l'entité de service et pour proposer notre modèle de l'utilisateur et de l'environnement ; en particulier la sous-classe de comportement a été enrichie. Nous visons à modéliser notre environnement ambiant d'assistance pour faire face aux les différentes composantes.

3.7.3.1 Modèle Utilisateur

Classe Utilisateur : Cette classe distingue deux sous classes d'utilisateurs (personne dépendante et assistante). On a caractérisé la classe d'utilisateur dépendante qui est considérée comme entité principale nécessitant une représentation de l'ensemble des attributs de l'utilisateur :

- Comportement : est divisé en six sous-classes de comportement identifiés de l'expérience réalisée et décrite dans la section précédente (Table 1.1).
- Profil : sert à représenter l'historique des accidents, à savoir si la personne avait subi auparavant une chute on non et d'autres problèmes de santé.
- Contexte (situation actuelle) : cette entité définit le temps , le lieu , le mouvement et le déplacement de l'utilisateur au sein de son environnement.
- Situation : sert à qualifier le degré de gravité de l'évènement. On distingue quatre cas : urgence, critique, normale et anormale.

Les liens sémantiques sont établis par la définition des attributs sémantiques : asked_service (utilisateur, services) , has_policy (utilisateur , politiques) , located_in (utilisateur, environnement). La propriété (notify) est un lien avec la classe personne-assistante, elle sert à notifier l'évènement dans le cas où une situation est apparue.

3.7.3.2 Modèle Service

Classe de service : cette entité représente le service demandé (de l'éclairage à l'ouverture de fenêtres , ouverture de porte pour sortir, cuisiner , prendre une douche) qui sont très sensibles après une situation de détresse identifiée.

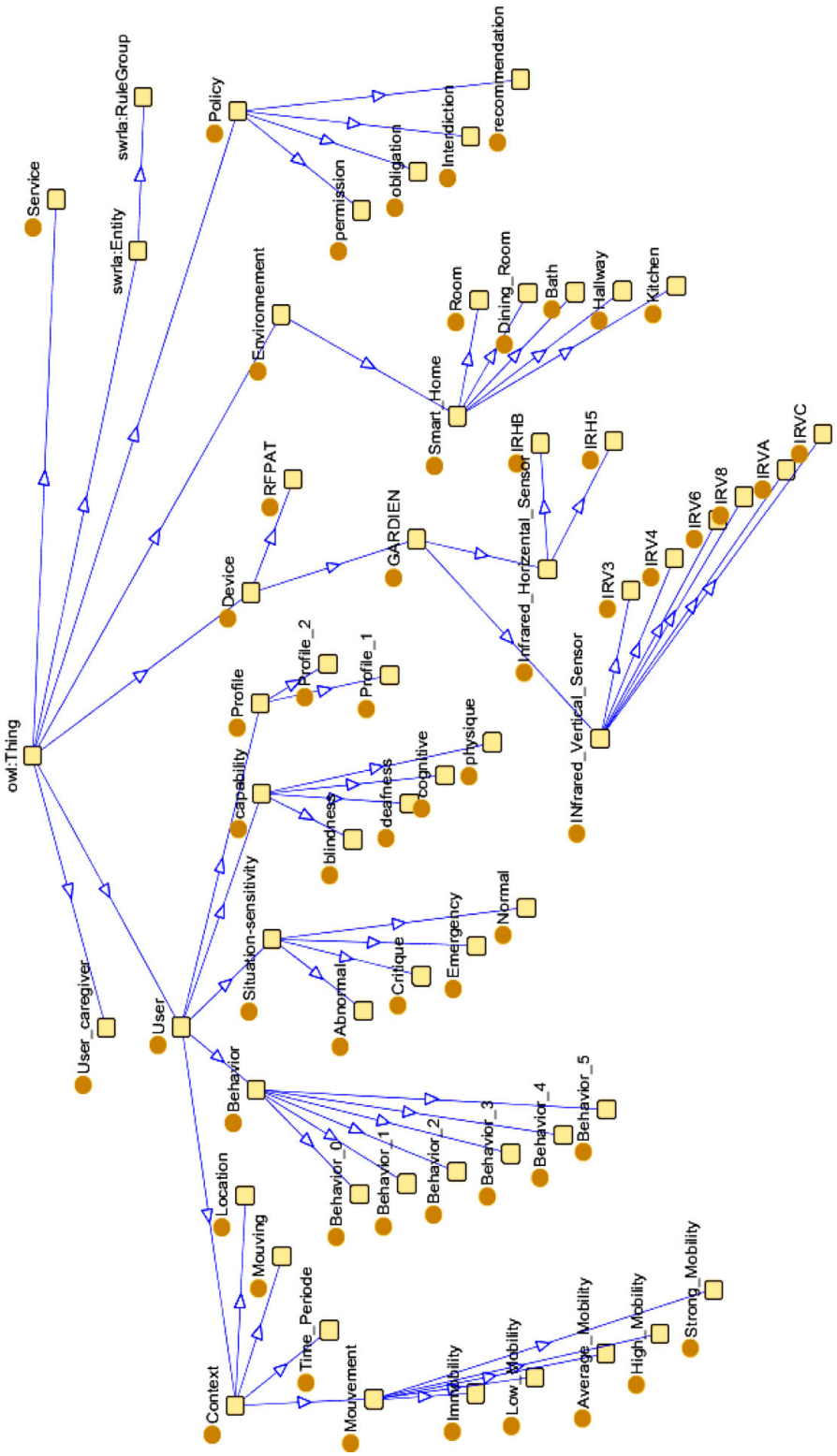

FIGURE 3.7.2 – Modèle ontologique.

3.7.3.3 Modèle Environnement

Classe de l'environnement : Le processus de modélisation est limité à l'espace de vie intérieure comme la salle à manger, la salle de bains et la cuisine. Les propriétés requises pour mettre en œuvre cette entité sont : Equiped_by_sensor_x .

3.7.3.4 Modèle Sécurité

Classe politique de sécurité : comprend quatre sous-classes :

Autorisation : accordée dans le cas où il n'y a aucun risque sur l'utilisateur en termes de santé.

Interdiction : après avoir détecté une situation anormale ou critique, il est strictement interdit à l'utilisateur d'effectuer n'importe quelle tâche.

Obligation : suivant la situation identifiée, le système oblige l'utilisateur à appliquer les consignes affichées.

Recommandation : dans des cas de détresse, le système assiste la personne par des recommandations.

Chaque politique sera définie plus précisément comme une règle pour accorder une décision en fonction du comportement identifié , la situation , le profil et les capacités .

3.7.3.5 Modèle dispositifs

Classe de dispositif : le processus de modélisation est limité aux dispositifs intégrés dans la maison et regroupés en deux sous systèmes : GARDIEN et RFPAT. On distingue des capteurs de présence verticaux (IRV 3 , 4 , 6 , A, C) et horizontaux (IRH5 , IRHB). Les propriétés définies sont : Sensor_X_State .

3.8 Conclusion

Dans ce chapitre, on a présenté les domaines exploités (suivi de comportement, modélisation de profil utilisateur et la technologie du web sémantique) pour la mise en place de notre politique de sécurité. Celle-ci a permis à la fois de contribuer au niveau de l'authentification afin d'assurer une meilleure identification et au niveau du contrôle d'accès pour attribuer les droits d'accès d'une façon très appropriée à la personne.

Chapitre 4

Développement et mise en place de l'architecture (UBC-ACA)

La conception d'un modèle exige un support architectural pour sa mise en place dans le monde réel. Pour atteindre notre objectif de sécurité visant à extraire les droits d'accès les plus appropriés, une architecture UBC-ACA (User Behavior Capability- Access Control Architecture) de contrôle d'accès constituée de quatre couches, est mise en place. Ce chapitre décrit les étapes principales de développement du modèle de contrôle d'accès (UBC-ACM) : l'apprentissage, la modélisation et le raisonnement. L'apprentissage sert à l'identification des différents motifs après un suivi de comportement d'utilisateur. La modélisation avec le langage OWL sert à structurer les différents concepts de la politique de sécurité. Le raisonnement intelligent intègre les résultats d'apprentissage et les données contextuelles pour inférer des connaissances complexes et implicites en utilisant le langage SWRL pour l'expression des règles qui mènent à la prise de décisions.

4.1 Architecture de Contrôle d'accès

Notre approche est mise en pratique par le développement de l'architecture illustrée dans la figure 4.1.1 [Zerkouk et al. 2014], composée de quatre couches principales dans le but d'assister des personnes âgées dépendantes.

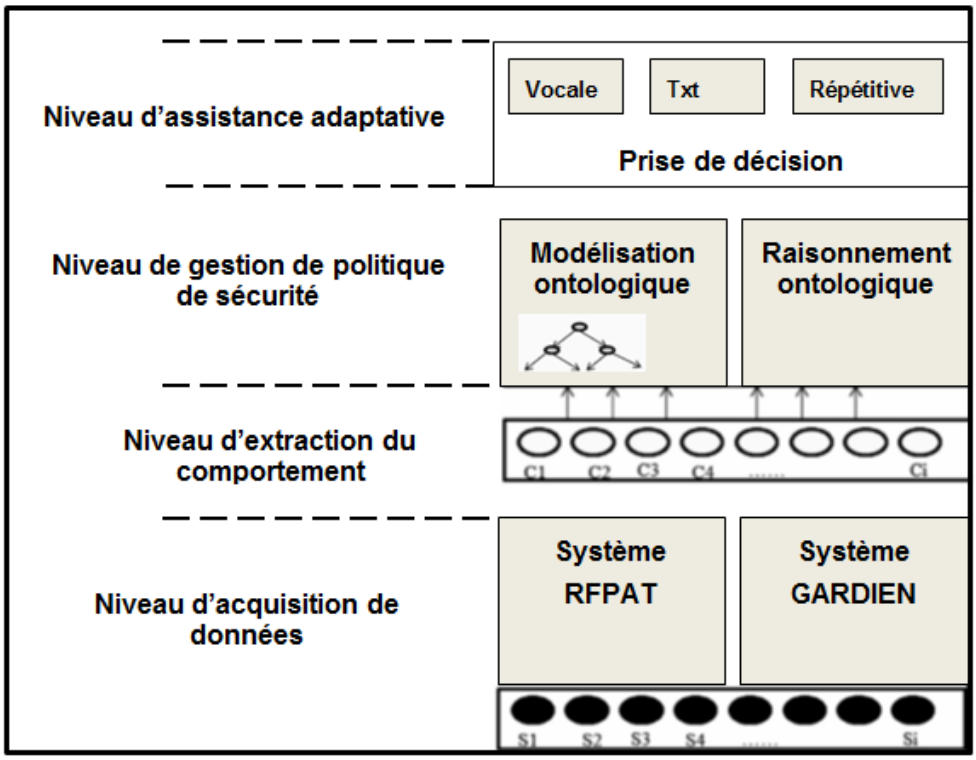

FIGURE 4.1.1 – Architecture de contrôle d'accès.

– **Couche d'acquisition de données :** Cette couche de base sert à collecter les données détectées par les systèmes RFPAT et GARDIEN de notre plate-forme. Le processus d'acquisition permet la récupération des données contextuelles via les différents capteurs embarqués dans l'environnement et portés par l'utilisateur. Ce processus est indispensable pour mettre en place un système sensible au contexte riche en terme de déploiement de sources multiples. On a tenu dans cette couche deux modes d'acquisition (portable et ambiant) des données contextuelles qui peuvent servir à proposer un modèle de contrôle d'accès adaptatif et personnalisé. L'environnement exploité est intelligent par l'intégration de différents dispositifs, les modes d'acquisition exploités permettent de fournir des données très riches. Les données capturées sont liées soit à l'utilisateur soit à l'environnement. L'utilisation des caméras n'est pas intégrée dans la plateforme en raison de l'atteinte à la vie privée des personnes.

1. **Dispositifs portables :** Ce mode consiste à placer des capteurs au niveau du corps humain ou les vêtements pour surveiller l'état de la personne en détectant les signaux tels que le pouls, la chute et la posture.
2. **Dispositifs ambiants :** Ce mode est basé sur un réseau de cap-

teurs embarqués dans l'environnement, la combinaison des données contextuelles collectées sert à favoriser l'extraction d'autres types de contextes complexes (activité, profil et comportement) exploités pour la mise en place des plateformes de télésurveillance, de télémédecine ou de télé-santé.

- **Couche d'extraction de comportement :** Cette couche consiste à combiner les différentes données décrivant le contexte de l'utilisateur et son environnement par l'utilisation de différents types de capteurs (infrarouge et accéléromètres). Plus précisément, le comportement de l'utilisateur surveillé est enregistré depuis de nombreux jours. L'ensemble de données est stocké dans un fichier de type ARFF qui va servir comme une base d'apprentissage lors de classification pour identifier les principaux modèles de comportements suivant les attributs discriminants choisis. Les classes obtenues seront utilisées pour établir les règles de contrôle d'accès.

- **Couche de gestion de la politique de sécurité :** Cette couche est constituée de deux modules fondamentaux : modélisation (OWL) et raisonnement (SWRL).

  * Modélisation de la politique de sécurité : Une fois les données collectées et les classes de comportement identifiées, un processus de modélisation est nécessaire pour représenter les données sous un format standard et en ajoutant l'aspect sémantique pour les différentes entités décrivant l'utilisateur et son environnement afin de mettre en place le processus de raisonnement.
  * Raisonnement sur le contrôle d'accès : au niveau de ce module, les règles seront définies afin d'inférer des connaissances nouvelles et implicites sur le contexte, l'activité, la situation et analysant tout les paramètres pour extraire la bonne décision.

- **Couche d'assistance adaptative :** Cette couche est utilisée pour envoyer la décision d'assistance en tenant compte de la capacité de l'utilisateur qui pourrait être vocale pour les personnes aveugles, sous forme txt pour les personnes sourdes et répétitive pour les gens qui souffrent de problèmes cognitifs. Selon les données acquises, l'ontologie construite est interrogée pour obtenir la décision inférée sur l'authentification ou contrôle d'accès.

4.2 Apprentissage (Identification des classes de comportement)

4.2.1 Apprentissage pour extraction de comportement

La conception d'un système de reconnaissance d'activités en temps réel reste un grand défi dans les recherches actuelles. L'identification des activités et situations humaines est une tâche clé dans notre processus de contrôle d'accès adapté au domaine de l'assistance ambiante à domicile. Par la reconnaissance d'activité, on vise le suivi du comportement d'un utilisateur et son environnement pour détecter tout changement au niveau des activités, des situations et des cas de détresses.

Suivant la nature des données acquises et les enregistrements effectués, on distingue des données étiquetées et non étiquetées. Cette différence crée deux classes d'apprentissage : supervisée et non supervisée.

4.2.1.1 Apprentissage supervisé

L'apprentissage supervisé est désigné aussi par l'analyse discriminante. Les données d'apprentissage sont étiquetées au préalable à l'aide d'un expert. Le processus passe par deux phases : la phase d'apprentissage, effectuée hors ligne, qui sert à déterminer un modèle de données étiquetées et la phase de test, effectuée en ligne, qui prédit l'étiquette d'une nouvelle donnée, connaissant le modèle préalablement appris. Les problèmes majeurs traités avec ce mode d'apprentissage sont la classification et la régression [Pellier 2015].

4.2.1.2 Apprentissage non supervisé

L'apprentissage non supervisé est appelé aussi classification automatique ou clustering. Les données d'apprentissage ne sont pas étiquetées et dans ce mode, l'avis d'un expert n'est pas demandé. Les vecteurs de données sont considérés comme des observations. Il est impossible de calculer le taux d'erreur pour évaluer une solution potentielle. Ce mode vise à trouver des structures cachées dans le jeu de données par la classification de celles-ci en groupes homogènes en mesurant les similarités. Après avoir obtenu les partitions possibles, il est envisageable de faire ressortir de l'information à partir des données disponibles [Pellier 2015].

4.2.2 Processus d'extraction de comportement

Pour la mise en place de notre processus d'extraction des motifs de comportement, on a exploité la technologie de la fouille de données qui est extrêmement

importante pour l'identification des différents motifs par l'analyse de l'historique enregistré au niveau de notre plateforme de télé-vigilance. Vu la nature de nos données qui ne sont pas étiquetées, on note qu'il est nécessaire de faire un apprentissage non supervisé ou plus précisément la partition.

L'outil Weka est le plus répandu dans le domaine de la fouille de données et l'apprentissage machine [Apprentissage_Wiki 2015]. Weka est une plateforme indépendante et facile à utiliser : elle admet diverses caractéristiques : logiciel libre et disposant de différents algorithmes d'apprentissage et de classification. On a donc opté pour l'utilisation de "Weka clusterer" qui sert à regrouper les instances similaires d'un corpus de données en groupes.

Comme le montre la figure 4.2.1, le processus d'extraction de comportement comporte les tâches suivantes :

- **Construction de corpus de données :** Cette tâche consiste à préparer les données au format ARFF (Attribut-Relation File Format) exigé par l'outil Weka.
- **Classification :** Cette tâche sert à regrouper en partition les vecteurs définis dans le fichier, en calculant des similarités entres les instances après avoir analysé et identifié les attributs discriminants.
- **Reconnaissance / Étiquetage :** Cette étape a pour rôle de reconnaitre la spécificité de chaque partition obtenu par rapport aux situations possibles dans lesquelles l'utilisateur peut se retrouver.
- **Prédiction :** Cette tâche est complètement détaillée dans le reste du chapitre. On introduit les motifs obtenus dans le processus de contrôle d'accès par le biais d'une ontologie afin de mieux assister la personne surveillée.

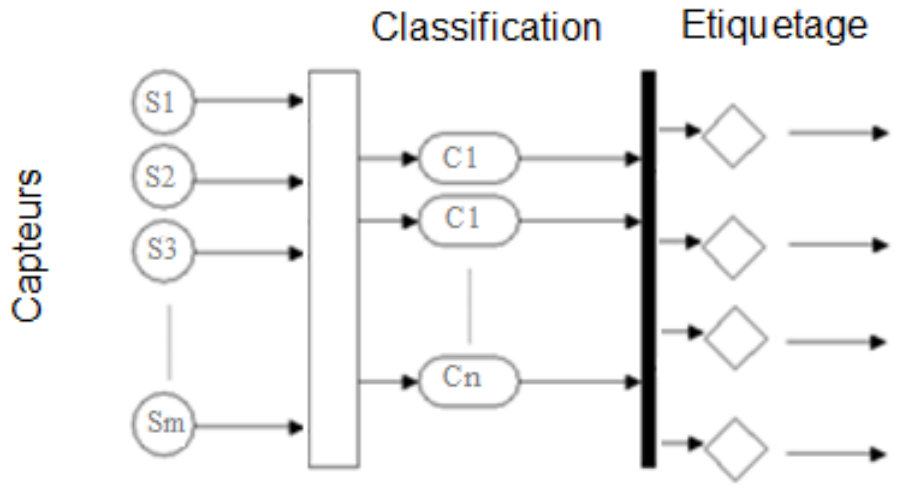

FIGURE 4.2.1 – Processus d'extraction des motifs de comportements.

4.2.2.1 Corpus de données

Dans notre travail, nous avons effectué un véritable enregistrement dans l'espace de vie où chaque instance reflète un scénario réel afin d'identifier le modèle de comportement de l'utilisateur en appliquant un processus de classification. Cette étape nécessite en entrée le vecteur des caractéristiques définies $< F1, F2, F3, \ldots Fn >$ décrivant un utilisateur et l'environnement par un ensemble d'attributs. Le corpus de données généré est formé de 6409 vecteurs. Les données utilisées pour structurer un vecteur de caractéristiques sont très hétérogènes, acquises à partir de sources multiples (dispositifs portables et des capteurs omniprésents).

L'outil Weka exige comme entrée dans le système un type particulier de fichier sous la forme ARFF (Attribut-Relation File Format). Un fichier ARFF est un fichier texte ASCII qui décrit une liste d'instances partageant un ensemble d'attributs. Ce type de fichier est caractérisé par deux sections distinctes. La première section est l'en-tête, qui est suivie des données. La figure 4.2.2 montre un aperçu sur notre fichier de définition des données.

```
@relation test_clustered

@attribute Instance_number numeric
@attribute 'IR 3' {0,3,4,5,6,8,A,B,C}
@attribute 'IR 4' {0,3,4,5,6,8,A,B,C}
@attribute 'IR 5' {0,3,4,5,6,8,A,B,C}
@attribute 'IR 6' {0,3,4,5,6,8,A,B,C}
@attribute 'IR 8' {0,3,4,5,6,8,A,B,C}
@attribute 'IR A' {0,3,4,5,6,8,A,B,C}
@attribute 'IR B' {0,3,4,5,6,8,A,B,C}
@attribute 'IR C' {0,3,4,5,6,8,A,B,C}
@attribute ''date day' numeric
@attribute heure numeric
@attribute 'minute ' numeric
@attribute 'seconde ' numeric
@attribute annee numeric
@attribute Batterie numeric
@attribute Chute numeric
@attribute Position numeric
@attribute 'Appel ' numeric
@attribute 'Activity ' numeric
@attribute Pulse numeric


@data
0,0,0,0,0,0,0,0,0,23,10,3,18,2009,0,0,1,0,0,52
1,0,0,0,0,0,0,0,0,8,16,27,10,2009,0,0,0,0,15,76
2,0,0,0,0,0,0,0,0,23,10,34,53,2009,0,0,0,0,4,58
3,0,3,5,0,0,0,0,0,5,16,1,42,2009,0,0,0,0,15,80
4,0,0,0,6,0,0,0,0,22,17,11,14,2009,0,0,0,0,0,60
5,0,0,0,0,0,0,0,C,9,18,53,31,2009,0,0,0,0,15,76
```

FIGURE 4.2.2 – L'en-tête de notre fichier ARFF.

4.2.2.2 Classification

Le clustering est une méthode statistique d'analyse de données intelligente [Nathiya et al. 2010]. Celle-ci sert à explorer les inter-relations entre les données par le groupage de celles-ci en clusters homogènes. Cette approche est largement appliquée dans différents domaines tels que la recherche d'information (RI), la reconnaissance d'activité et de motifs. Parmi les algorithmes les plus connus, il y a : k-means et EM (Expectation Maximization).

D'après [Nathiya et al. 2010], l'objectif principal du partitionnement est de déterminer une catégorisation intrinsèque des données non étiquetées. Elle

précise que l'utilisateur doit fournir le critère de la bonne classification suivant les besoins et les exigences d'utilisateur.

Après l'exécution des algorithmes (k-means et EM), en faisant varier leurs paramètres, nous avons choisi celui qui donne la classification la plus appropriée ; précisément, l'algorithme capable de regrouper tous les vecteurs qui ont le comportement le plus sensible avec (chute = 1) et (posture = 1) dans un cluster. Le résultat obtenu est apprécié en utilisant l'algorithme le plus populaire (k-moyennes).

L'expérimentation de données consiste à faire varier le nombre souhaité de classes jusqu'à k = 6, qui est le meilleur découpage. Enfin, nous avons obtenu six motifs communs issus de nos données expérimentées. Les résultats examinés dans les figures 4.1.5 à 4.18 sont obtenus à partir de l'outil d'extraction de connaissances Weka. Les motifs obtenus sont ensuite fournis en entrée au processus de modélisation et de raisonnement.

Algorithme K-means

Selon [k-means_wiki 2015], l'approche des k-moyennes (ou K-means) est un algorithme de partitionnement de données relevant des statistiques et de l'apprentissage automatique (plus précisément de l'apprentissage non supervisé). C'est une méthode dont le but est de diviser des observations en K partitions (clusters) dans lesquelles chaque observation appartient à la partition avec la moyenne la plus proche. Les nuées dynamiques sont une généralisation de ce principe, pour laquelle chaque partition est représentée par un noyau pouvant être plus complexe qu'une moyenne. Les principales tâches de cet algorithme et son déroulement, sont illustrés par la figure 4.2.3 ainsi son algorithme est présenté dans la figure 4.2.4 :

- Déterminer le centre de gravité de coordonnées.
- Déterminer la distance de chaque objet aux centre de gravité.
- Construire des groupes en fonction de la distance minimale par la recherche du centre de gravité le plus proche.

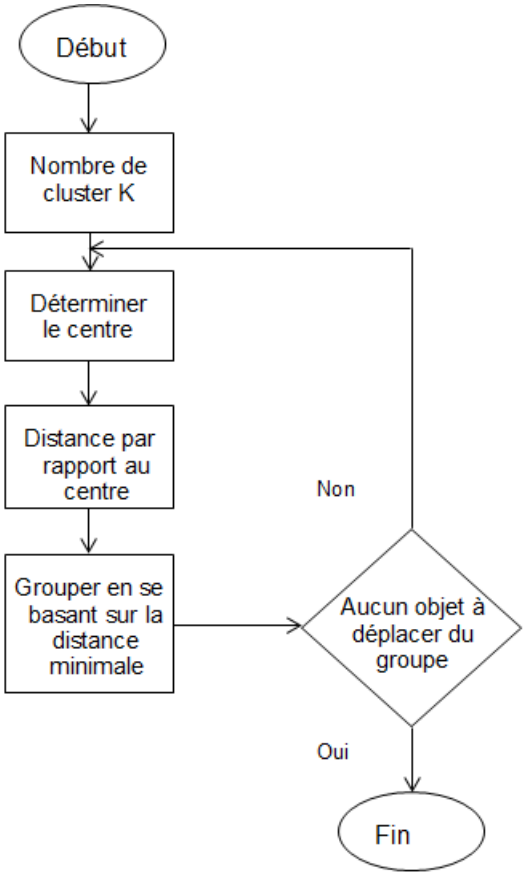

FIGURE 4.2.3 – Etapes de déroulement de l'Agorithme K-means.

Le but de l'algorithme est de minimiser $J(\mu, z)$, il se présente sous la forme d'un algorithme de minimisation alternée :

- Etape 0 : "choisir le vecteur μ"
- Etape 1 : on minimise J par rapport à z : $z_i^k = 1$ pour $k \in \arg\min \|x_i - \mu_k\|$, *ie* on associe à x_i le centre μ_k le plus proche.
- Etape 2 : on minimise J par rapport à μ : $\mu_k = \frac{\sum_i z_i^k x_i}{\sum_i z_i^k}$.
- Etape 3 : retour à l'étape 1 jusqu'à convergence.
- Les $x_i \in \mathbb{R}^p$, $i \in \{1, ..., n\}$ sont les points à séparer.
- Les z_i^k sont des variables indicatrices associées aux x_i telles que $z_i^k = 1$ si x_i appartient au cluster k, $z_i^k = 0$ sinon. z est la matrice des z_i^k.
- μ est le vecteur des $\mu_k \in \mathbb{R}^p$, où μ_k est le centre du cluster k.

On définit de plus *la mesure de distorsion* $J(\mu, z)$ par :

$$J(\mu, z) = \sum_{i=1}^{n} \sum_{k=1}^{n} z_i^k \|x_i - \mu_k\|^2$$

FIGURE 4.2.4 – K-means.

4.2.2.3 Analyse des classes obtenues

Le processus de clusterisation est effectué afin de regrouper les mêmes comportements par cluster en fonction de la sensibilité des différentes situations détectées. Le corpus de données inclut les paramètres discriminants ainsi que leur valeurs comme illustré dans la table 4.1 :

Attributs	Domaine de variation
Temps	<Jeu 9 Oct 18 :38 :2009>
Localisation	$(Loc)\,(t)\epsilon\{Chambre, cuisine, salledebain, couloir, salon\}$
Pouls	{40,75}
Mouvements	Immobilité [0-1] Mobilité faible [1-7] Mobilité forte [8-15]
Posture	{0,1}
Chute	{0,1}

TABLE 4.1 – Les attributs du corpus de données.

Temps

L'attribut temps est utilisé pour identifier et faire la distinction entre les différents états : l'utilisateur se trouve dans la salle, l'utilisateur est en train

de faire une activité donnée ou l'utilisateur a fait une chute. L'attribut temps est décrit comme suit :

$$< Jeu\, 9\, Octobre\, 18 : 38 : 46\, 2009 >$$

Localisation

L'attribut localisation est capturé par l'activation des capteurs infrarouges installés dans chaque espace de vie pour détecter la présence de l'utilisateur et son déplacement. La valeur de localisation peut être comme suit : $(Loc)\,(t)\epsilon\{Chambre, cuisine, salledebain, couloir, salon\}$

Pouls

L'attribut pouls sert à surveiller l'état cardiaque de la personne où il vari entre {40,75}. Selon l'ensemble des données, parfois, les valeurs descendent à 40 et montent à 75, cela est dû à des erreurs de mesure, car les données sont simulées par de jeunes chercheurs environ les trentaines.

Mouvement

L'attribut mouvement a pour but de détecter le rythme de la mobilité où ses valeurs varies entre nt objectifs pour détecter le rythme de mobilité qui les valeurs varient entre {0,15}. Après notre analyse, nous avons distingué trois plages de valeurs :

Immobilité [0-1] : signifie que la personne ne réalise aucune activité.

Mobilité faible [1-7] : signifie que la personne est moins dynamique.

Mobilité forte [8-15] : signifie que la personne est trés dynamique.

Posture

L'attribut posture vise à identifier si la personne est allongée ou debout.

La valeur de l'attribut est entre {0,1} où (0) signifie debout et (1) signifie allongée. Il est important de combiner les valeurs des paramètres temps et localisation pour valider l'attribut posture.

Par exemple, si la personne est allongée dans la cuisine à 12h, cela signifie qu'il ya une la situation anormale.

Chute

L'attribut chute peut prendre deux valeurs possibles {0,1} où la situation chute est détectée si sa valeur est à (1).

Les résultats obtenus dans la figure 4.2.5 - 4.2.8 sont résumés et discutés dans le tableau 4.2.2.4 qui sera exploité en entrée pour l'élaboration de la politique

de sécurité et pour la mise en place du moteur d'inférence par le processus de raisonnement.

- **Cluster 0** : Ce groupe est discriminé par les valeurs des attributs mouvement et pouls. Le comportement de l'utilisateur dans ce groupe est très dynamique avec des valeurs varient entre 12 et 15 avec un déplacement fort entre les pièces de la maison et sans détection de chute (0) ou position allongée avec posture (0). Il souffre d'un problème cardiaque car les valeurs de pouls sont élevées. L'utilisateur dans ce cluster est très actif dans l'intervalle de temps [14h, 18h] et le paramètre appel est à (1).
- **Cluster 1 :** Ce groupe est discriminé par le fait qe toutes les valeurs des attributs sont dans un état normal, valeurs varient entre 7 et 12. Le comportement de l'utilisateur dans ce groupe est normal avec une activité moyenne avec déplacement fort entre les pièces de la maison et sans détection de chute (0) ou position allongée avec posture (0), il n'y a pas de problème cardiaque et les valeurs de pouls sont dans un état normal. L'utilisateur dans ce cluster est très actif dans l'intervalle de temps [9h, 12h] et [14h, 18h].
- **Cluster 2 :** Ce groupe se distingue par les valeurs des attributs mobilité et posture. L'utilisateur est immobile, aucune activité n'est détectée (0), sans déplacement entre les parties de la maison, la position (1) signifie qu'il est allongé mais pas de chute détectée. Les situations détectées ont eu lieu dans la matinée [9h, 12h] et le soir [14h, 18h].
- **Cluster 3 :** Ce groupe est distingué par les valeurs de l'attribut pouls et mobilité, variant entre 12 et 15. L'utilisateur dans ce groupe a une mobilité moyenne et n'est pas très dynamique avec une forte mobilité entre les pièces de la maison et sans détection de chute (0) ou de position allongée avec posture (0). Le problème cardiaque est provoqué avec les valeurs de pouls basses, cela indique que la personne est dans un état anormal. Ce comportement est détecté à partir de 18h et à un moment donné l'utilisateur a signalé une urgence car le paramètre appel est à (1).
- **Cluster 4 :** Ce groupe rassemble les comportements discriminés par les valeurs de l'attribut mobilité, le valeurs varient entre 12 et 14. L'utilisateur dans ce groupe est moins dynamique avec moins de déplacement entre les pièces de la maison et sans détection de chute (0) ou la posture (0) pas de problème cardiaque provoqué où les valeurs d'impulsions sont dans un état normal. Ce comportement est identifié dans l'intervalle de temps [14h, 18h].
- **Cluster 5 :** Ce groupe recueille le comportement majeur qui est discriminé par les valeurs des attributs, les valeurs qui varient entre 12 et 15. L'utilisateur dans ce groupe est très dynamique avec une forte dynamicité ou mobilité entre les pièces de la maison mais d'un seul coup il y

a détection de chute (1) et la posture (1) est sans problème cardiaque provoqué car les valeurs d'impulsions sont dans un état normal. Cette situation d'urgence est détectée le matin et le soir.

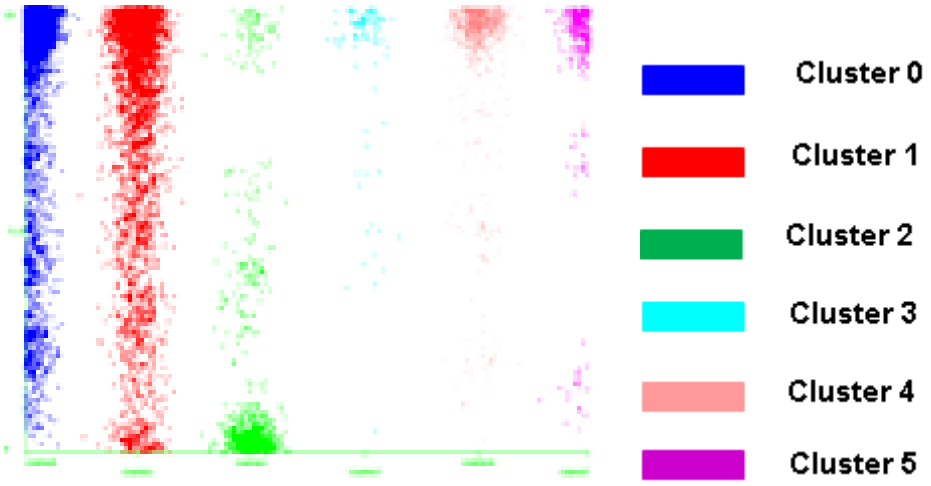

FIGURE 4.2.5 – Regroupement des instances suivant le paramètre pouls.

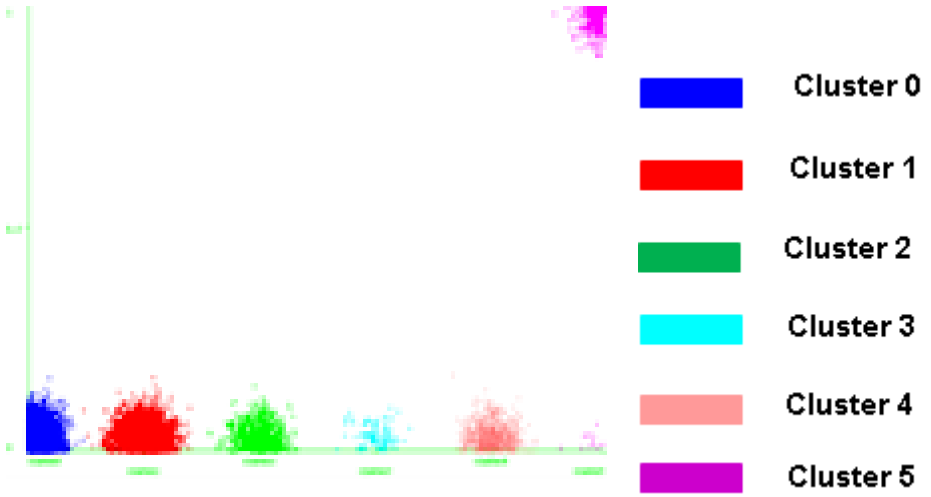

FIGURE 4.2.6 – Regroupement des instances suivant le paramètre chute.

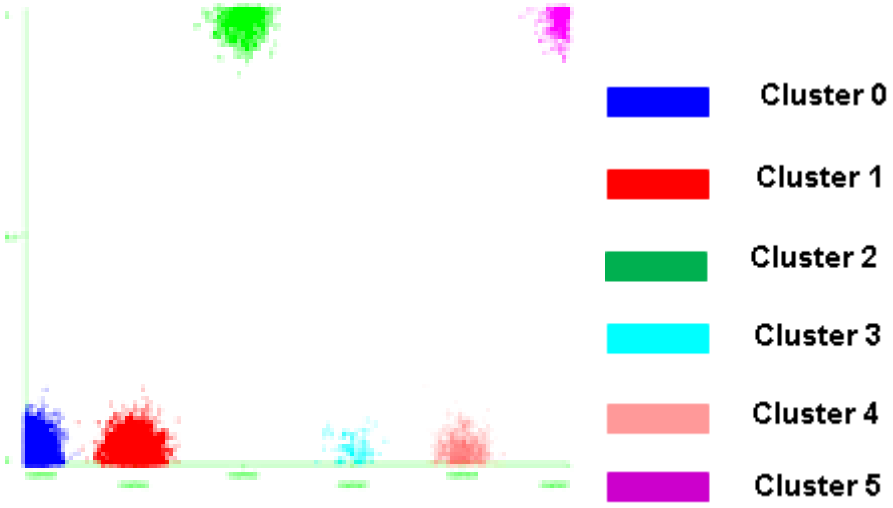

FIGURE 4.2.7 – Regroupement des instances suivant le paramètre posture.

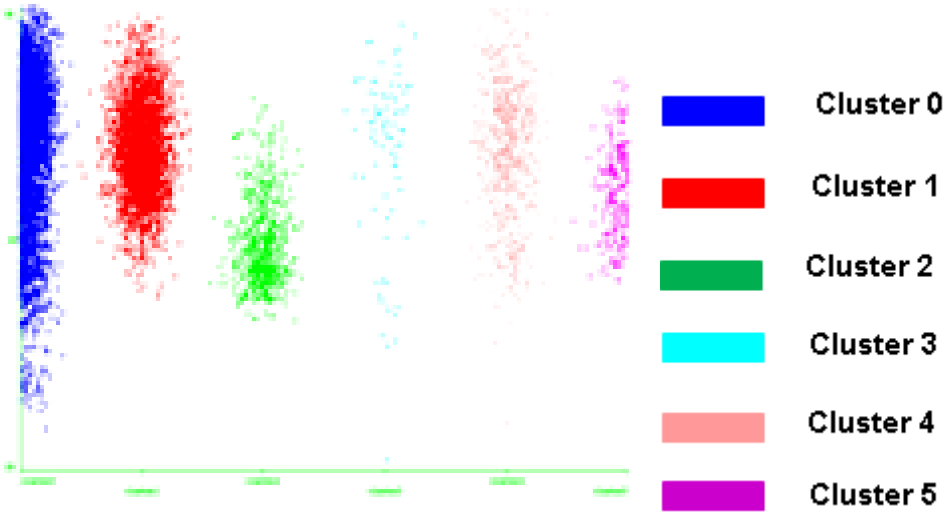

FIGURE 4.2.8 – Regroupement des instances suivant le paramètre temps.

Les résultats obtenus seront intégrés dans le processus de modélisation et seront utilisés dans le processus de raisonnement pour déduire de nouvelles connaissances.

4.2.2.4 Reconnaissance des motifs obtenus (Étiquetage)

Grâce au processus de classification, on a obtenu six classes où chaque classe est caractérisée par une situation sensible par rapport à une personne âgée

dépendante qui vit toute seule. Afin de finir cette tâche et pour une gestion plus simple, on a opté d'étiqueter chaque cluster par un label décrivant la situation de l'utilisateur comme le montre la table 4.2.

Label ={Alerte (hypertension), Alerte (hypotension), Normale, Critique, anormale (inquiétante), urgence (chute soudaine)}.

ID Cluster	Description du Cluster	Étiquète du Cluster
0	L'utilisateur est très mobile et souffre d'hypertension artérielle	Vigilance (hypertension)
1	L'utilisateur est très dynamique, non cardiaque ou des problèmes de santé	Normale
2	L'utilisateur est immobile avec (posture = 1)	Critique
3	L'utilisateur souffre de pression artérielle basse à mobilité moyenne. L'utilisateur n'a pas de problèmes de santé	Vigilance (hypertension)
4	L'utilisateur dispose d'une faible mobilité sans problèmes cardiaques	Anormale (déranger)
5	L'utilisateur est immobile et soudain fait une chute et (la posture = 1) signifie que l'utilisateur est couché	Urgence (chute soudaine)

TABLE 4.2 – Étiquetage des clusters obtenus.

4.3 Modélisation & Base de connaissance

Une base de connaissance permet le stockage des données contextuelles, elle interagit avec différents modules (moteur d'inférence, modèle de contexte, moteur de requêtes) comme illustré dans figure 4.3.1.

Lors de la modélisation des connaissances, on distingue deux niveaux abstraction de données [Baader et al. 2003] :

- Le premier niveau est Terminologique (TBox) : décrit les connaissances générales d'un domaine.

- Le second niveau est Assertionnel (ABox) : représente une instanciation spécifique. Une TBox comprend la définition des concepts et des rôles, alors qu'une ABox contient un ensemble d'assertions sur les individus.

Une ontologie est l'ensemble des instances individuelles des concepts qui constituent une base de connaissances.

Si le système permet un raisonnement sur l'ABox, les inférences suivantes sont proposées :

1. Vérifier la consistance de l'ABox () par rapport à la TBox ().

2. Vérifier les instances présentées dans la base de connaissance par rapport aux assertions de la TBox et de l'ABox.

3. Identifier l'ensemble des rôles présents entre deux individus i et j par rapport à la connaissance.

4. Identifier les instances d'individus avec les noms de concepts les plus spécifiques mentionnés dans la TBox et les assertions dans l'ABox.

5. Identifier tous les individus cités dans l'ABox () qui sont les instances d'un concept donné dans la TBox (), appelé le problème de l'inférence de récupération.

6. Identifier l'ensemble des charges de rôle pour un individu i à l'égard de la TBox et de l'ABox.

Les services de raisonnement de la TBox sont les suivants :

1. Vérification de la cohérence des concepts identifiés dans la TBox.

2. Vérification du concept de subsomption à l'égard de TBox.

3. Vérification de la cohérence de la TBox en vérifiant la cohérence de tous les concepts mentionnés dans la TBox sans calculer les relations avec les concepts descendants / ascendants.

4. Identification de la hiérarchie des noms de concepts au sein d'une TBox (classement).

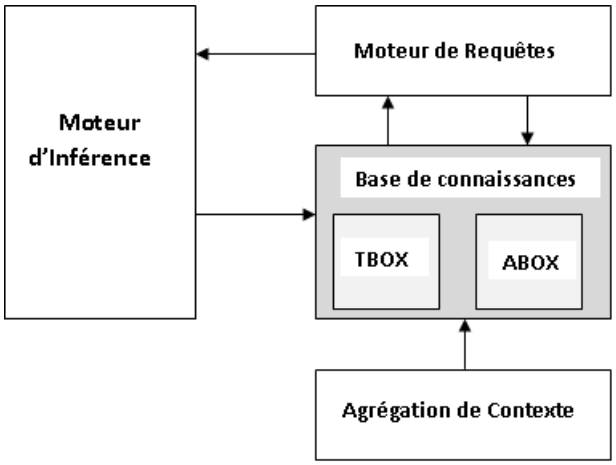

FIGURE 4.3.1 – Base de connaissances

4.4 Raisonnement (Inférence)

Dans notre approche, on s'intéresse aux données contextuelles au fil du temps ;

Suivant [Mayrhofer et al. 2004], la prise en compte du paramètre contexte au fil du temps fait la distinction entre deux types de systèmes sensibles au contexte réactif et proactif comme le montre la figure 4.4.1. Formellement, la différence entre la réactivité et proactivité réside dans la sortie dépendance du système.

Un système réactif est décrit comme suit :

$$q(t) = \delta(q(t-1), a(t-1))$$

où
q(t) : représente l'état courant à l'instant (t),
$q(t-1)$: représente l'état précédent,
$a(t-1)$: représente les valeurs d'entrée à $(t-1)$.

D'où la sortie du système est défini comme suit :

$$b(t) = \lambda(qt).$$

Dans un système est réactif, la sortie $b(t)$ à l'instant (t) ne dépend que de l'état courant et implicitement des états passés.

Dans un système proactif, il peut aussi dépendre des états futurs prévus où il est défini comme suit :$b(t) = \lambda(q_t, q_{t+1}, q_{t+2}, ...q_{t+m})$

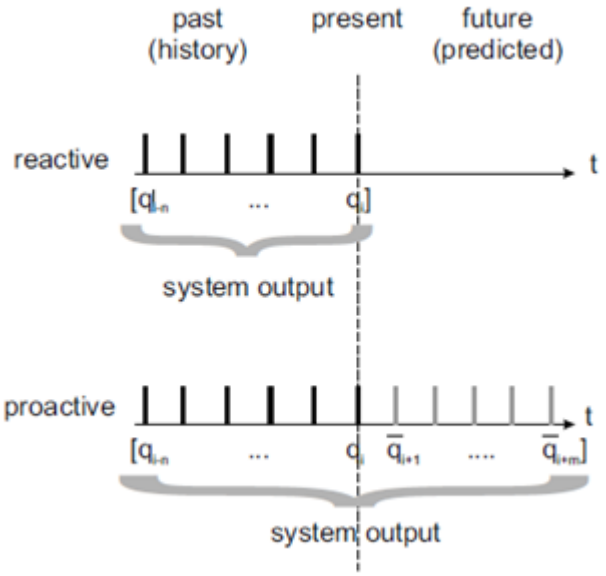

FIGURE 4.4.1 – Différence entre un système réactif et proactif.

On note que dans notre travail, on s'intéresse à la mise en place d'un système proactif où la prédiction de la bonne décision est la motivation de ce travail pour assurer l'adaptation des services aux besoins des personnes âgées dépendantes.

4.4.1 Technique de raisonnement (raisonnement sémantique à base de règles)

Un raisonneur sémantique (moteur de raisonnement ou moteur de règles) ou tout simplement un raisonneur, est capable de déduire des conséquences logiques d'un ensemble de faits ou axiomes revendiqués. Un langage de description est nécessaire pour la spécification des règles d'inférence. La logique des prédicats du premier ordre est la base sur laquelle se focalisent les raisonneurs pour effectuer les inférences [Fortineau et al. 2012] [Nurmi et al. 2004]. Pour ce faire, on distingue deux modes d'inférence par chaînage avant et chaînage arrière. Ces derniers sont les stratégies des raisonneurs ontologiques .

- Chainage avant : Selon cette stratégie, le raisonneur commence à partir des faits connus pour en tirer des inférences valides. Les objectifs de ce raisonnement sont :

Calculer la fermeture présumée, répondre à une requête particulière, déduire une sorte particulière de la connaissance (une taxonomie de classe). L'algorithme 4.1 montre les instructions de son déroulement.

Algorithme 4.1 Chainage avant

– Raisonnement en chaînage avant

Exemple d'algorithme

```
Procédure  CHAINAGE-AVANT
Début
        Répéter
        REGLE_DECLENCHABLE := DECLENCHEMENT(ensemble des règles)
        Jusqu'à  non REGLE_DECLENCHABLE;
Fin  CHAINAGE-AVANT

Fonction  DECLENCHEMENT (ensemble des règles) : booléen  ;
Début
        DECLENCHE := Faux ;
        Pour  toute règle appartenant à l'ensemble des règles
        Tant que  non DECLENCHE faire
        Début
                Si TEST-SI(règle)
                Alors  DECLENCHE := APPLICATION(règle)
        Fin Pour  ;
        Retourner  (DECLENCHE) ;
Fin  DECLENCHEMENT
```

- Chainage arrière : Selon cette stratégie, le raisonneur commence à partir d'un fait particulier ou une requête pour vérifier ou trouver toutes les solutions possibles. L'algorithme 4.1 montre les instructions de son déroulement.

Algorithme 4.2 Chainage arrière

– Raisonnement en chaînage arrière

Algorithme

```
Procédure  CHAINAGE-ARRIERE(liste des buts à vérifier)
Début
        Si liste est vide
        Alors  arrêt
        Sinon
        Début
           F = premier fait de la liste;
           Si VERIFICATION (F)
                Alors
                 Début
                    Afficher F comme vérifié;
                    CHAINAGE-ARRIERE (reste de la liste);
                 Fin;
           Sinon  CHAINAGE-ARRIERE (reste de la liste);
           Fin Si;
        Fin;
        Fin Si;
Fin  CHAINAG-ARRIERE
```

Dans [Tiberghien 2013] présente une étude détaillée sur les différents raisonneurs sémantiques ainsi que les raisonneurs ontologiques (Racer, Pellet, Hermit et Fact+).

Un service de raisonnement a pour but d'assurer les caractéristiques suivantes [Abburu 2012] :

Vérification de la consistance : s'assure que l'ontologie ne contient aucun fait contradictoire ;

Satisfiabilité des concepts : vérifie s'il est possible pour chaque classe d'avoir une instance ;

Classification : calcule les relations de sous-classe entre chaque classe nommée pour créer la hiérarchie de classe complète. Cette hiérarchie peut être utilisée pour répondre aux requêtes telles que « trouver toutes les sous-classes d'une classe ou les sous classes directes » ;

Réalisation : trouve la classe la plus spécifique dans laquelle un individu a sa place. En d'autres termes, elle calcule le type direct pour chaque individu. La Réalisation peut seulement être effectuée après une Classification puisque les types directs sont définis en fonction de la hiérarchie de classe. En utilisant une hiérarchie de Classification, il est possible d'obtenir tous les types pour les individus.

4.4.2 Outils de raisonnement

4.4.2.1 SWRL

Le langage de règles SWRL (Semantic Web Rule Language) est proposé par le W3C qui combine OWL-DL avec RuleML (Rule Markup Language), un langage de balisage pour la mise en œuvre de règles logiques. SWRL est un langage qui enrichit la sémantique d'une ontologie définie en OWL. Les règles en SWRL sont spécifiées à travers des clauses de Horn dont les atomes sont des concepts, des relations, ou des fonctions définis dans une ontologie [Fortineau et al. 2012].

Le langage SWRL manipule des instances contrairement à OWL manipule variables (?x, ?y, ?z). Il permet simplement d'ajouter des relations suivant les valeurs des variables et la satisfaction de la règle sans rajouter de nouvelles concepts ou relations. Les règles SWRL sont construites suivant ce schéma :

antécédent -> conséquent

L'antécédent et le conséquent sont des conjonctions d'atomes.

Un atome est une instance de concept, une relation OWL ou une des deux relations SWRL same-as(?x, ?y) ou different-from (?x, ?y)).

Le fonctionnement d'une règle est basée sur le principe de satisfiabilité de l'antécédent ou du conséquent. Pour une règle, il existe trois cas de figure :

- l'antécédent et le conséquent sont définis. Si l'antécédent est satisfait alors le conséquent doit l'être ;
- l'antécédent est vide, cela équivaut à un antécédent satisfait ce qui permet de définir des faits ;
- le conséquent est vide, cela équivaut à un conséquent non satisfait, l'antécédent ne doit pas être satisfiable

L'utilisation des ontologies pour la construction de base de connaissances est devenu un champ d'application très important surtout dans le domaine des maisons intelligentes et systèmes orientés santé. Il existe notamment plusieurs travaux utilisant SWRL pour la reconnaissance de situations, et d'activités dans la vie quotidienne.

4.4.3 Expression des règles dans le modèle ontologique (Rules design)

Afin de déduire les décisions de contrôle d'accès les plus appropriées, nous utilisons un raisonneur sémantique capable de déduire la décision d'un ensemble d'observations revendiquées sur la personne dépendante située dans un

espace de la maison intelligente. Par conséquent, ces personnes doivent accéder à des services intelligents en prenant en compte le profil, le comportement et la capacité à l'aide des appareils fonctionnels. Nous spécifions les règles sémantiques par le biais de technologies du web sémantique selon la forme suivante <si conditions alors conclusion> pour effectuer le raisonnement. Un raisonneur sémantique vise à vérifier la cohérence de notre modèle d'ontologie proposée et d'en tirer des connaissances de haut niveau et implicites sur le comportement, la situation, le profil, la capacité et la décision de contrôle d'accès de l'utilisateur.

Nous avons choisi de mettre en œuvre le raisonnement en utilisant une source complètement ouverte OWL -DL conforme à notre modélisation de l'ontologie. Le processus de raisonnement est effectué pour aboutir à une décision, grâce un ensemble de règles sera effectuées comme suit ; nous devons vérifier le comportement, la mobilité. Plus précisément, le temps de contexte et l'emplacement sont vérifiés.

- Raisonnement sur Mouvement

Le paramètre Mouvement prends 3 valeurs : immobilité, forte mobilité et faible mobilité.

$$Immobilité(?x) \rightarrow Utilisateur(x?) \wedge mouvement(x, y?) \wedge swrlb : égal(?Y, 0).$$

$$\text{Low Mobility(x ?)} \rightarrow Utilisateur(x?) \wedge mouvement(x, y?) \wedge swrlb(x?) : LessThanOrEqual(y, 6?) \wedge swrlb : (y, 1)GreaterThanOrEqual$$

$$High\,Mobility(x?) \rightarrow Utilisateur(x?) \wedge mouvement(x, y?) \wedge swrlb(x?) : LessThanOrEqual(y, 14?) \wedge swrlb : GreaterThanOrEqual(?Y, 8).$$

Comme il est mentionné dans les règles , l'immobilité est identifiée lorsque la valeur de déplacement est (0) , la mobilité faible lorsque la valeur de déplacement est comprise entre un et six et le dernier est identifié lorsque la valeur de déplacement est entre huit et quatorze.

- Raisonnement sur Comportement

L'identification de mouvement est exigée dans le codage des règles de comportement :

$$Behavior_0(?x) \leftarrow User(?x) \wedge Fall(?x, ?c) \wedge swrlb : equal(?c, 1) \wedge \text{posture(?x, ?a)}$$

$$\wedge swrlb : equal(?a, 1) \wedge pulse(?x, ?z) \wedge swrlb : equal(?z, 67) \wedge HasMouvement(?x,\ High\,Mobility) \wedge$$

$$appel(?x, ?e) \wedge swrlb : égal(?e, 0)$$

$$Behavior_1(?x) \leftarrow User(?x) \wedge Fall(?x, ?c) \wedge swrlb : equal(?c, 0) \wedge \text{posture(?x, ?a)}$$

$$\bigwedge swrlb : equal(?a, 1) \bigwedge pulse(?x, ?z) \bigwedge swrlb : equal(?z, 67) \bigwedge HasMouvement(?x, immobility) \bigwedge$$

$$appel(?x, ?e) \bigwedge swrlb : égal(?e, 0)$$

$$Behavior_2(?x) \leftarrow User(?x) \bigwedge Fall(?x, ?c) \bigwedge swrlb : equal(?c, 0) \bigwedge \text{posture}(?x, ?a)$$

$$\bigwedge swrlb : equal(?a, 0) \bigwedge pulse(?x, ?z) \bigwedge swrlb : equal(?z, 67) \bigwedge HasMouvement(?x, LowMobility) \bigwedge$$

$$appel(?x, ?e) \bigwedge swrlb : égal(?e, 1)$$

$$Behavior_3(?x) \leftarrow User(?x) \bigwedge Fall(?x, ?c) \bigwedge swrlb : equal(?c, 0) \bigwedge \text{posture}(?x, ?a)$$

$$\bigwedge swrlb : equal(?a, 1) \bigwedge pulse(?x, ?z) \bigwedge swrlb : equal(?z, 67) \bigwedge HasMouvement(?x, Avg\ Mobility) \bigwedge$$

$$appel(?x, ?e) \bigwedge swrlb : égal(?e, 1)$$

$$Behavior_4(?x) \leftarrow User(?x) \bigwedge Fall(?x, ?c) \bigwedge swrlb : equal(?c, 0) \bigwedge \text{posture}(?x, ?a)$$

$$\bigwedge swrlb : equal(?a, 0) \bigwedge pulse(?x, ?z) \bigwedge swrlb : equal(?z, 67) \bigwedge HasMouvement(?x, High\ Mobility) \bigwedge$$

$$appel(?x, ?e) \bigwedge swrlb : égal(?e, 1)$$

$$Behavior_5(?x) \leftarrow User(?x) \bigwedge Fall(?x, ?c) \bigwedge swrlb : equal(?c, 1) \bigwedge \text{posture}(?x, ?a)$$

$$\bigwedge swrlb : equal(?a, 1) \bigwedge pulse(?x, ?z) \bigwedge swrlb : equal(?z, 67) \bigwedge HasMouvement(?x, High\ Mobility) \bigwedge$$

$$appel(?x, ?e) \bigwedge swrlb : égal(?e, 0)$$

- Raisonnement sur Situation

Nous devons introduire ce paramètre complexe qui est déduit des données simples afin d'identifier la sensibilité de la situation. Le paramètre Situation peut prendre quatre valeurs : critique, urgence , normale et anormale .

$$Emergency\ Situation(?X) \leftarrow utilisateur(?X) \bigwedge posture(?X, 1)$$

$$Critical\ Situation(?X) \leftarrow utilisateur(?X) \bigwedge posture(?X, 1) \bigwedge \text{fall}(?X, 1)$$

$$Abnormal\ Situation(?X) \leftarrow utilisateur(?X) \bigwedge Mouving(?X, 0) \bigwedge \text{Located In Bath}(?D, 1)$$

$$Normal\ Situation(?x \leftarrow utilisateur(?x) \bigwedge \text{temps}(?x, «matin»)$$

$$posture(?x, 0) \bigwedge mouving(?X, 1).$$

- Raisonnement sur Profil

Le paramètre Profil est considéré comme caractéristique principale de notre politique de sécurité, il vise à vérifier la capacité de l'utilisateur, si l'utilisateur a subi une chute ou non .

$$Profile_1(?x) \leftarrow utilisateur(\text{?x}) \wedge capacités(?x, y?) \wedge Falling\,Before(?x, z?) \wedge$$

$$swrlb : equal(?z, 0)$$

Ces règles sont nécessaires pour déduire la situation antérieure de la personne. En fait pour assurer une meilleure assistance.

- Raisonnement sur Contexte (localisation)

Parmi les données contextuelles, nous avons le temps et la localisation, dans le corpus de données, il n y a pas de valeur bien déterminée pour le paramètre localisation. En fait, chaque valeur d'emplacement est définie par l'utilisation de capteurs horizontaux et verticaux. Pour cela, nous devons définir pour chaque emplacement une règle, comme le montre la règle ci-dessous :

$$Bath(\text{?x}) \leftarrow User(?x) \wedge Environnement(?X) \wedge IRH5(?Y) \wedge Equiped\,By\,Sensor1(?x, y?) \wedge$$

$$IRH5\,State(?y, z?) \wedge swrlb : égal(z, 1) \wedge Equiped\,By\,Sensor1(?x, ?a) \wedge$$

$$IRV3(?a) \wedge IRV3\,State(a, b) \wedge swrlb : égal(b, 1)$$

$$\text{Living\_room(?x)} \leftarrow user(?x) \wedge Environnement(?x) \wedge IRHB(?y)$$

$$\wedge \text{EquipedBy Sensor5(?x, ?y)} \wedge \text{IRHB state(?y, ?z)} \wedge \text{swrlb :égal(?y,1)} \wedge$$

$$\text{Equiped By Sensor5(?x, ?a)} \wedge \text{IRV6(?a))} \wedge IRV6\,state(?a, b?) \wedge swrlb(?b, 1) \wedge$$

$$IRV6(?a) \wedge IRV6\,state(?a, b?) \wedge swrlb : égal(?b, 1?)$$

Cette règle vise à reconnaitre l'emplacement de la salle de bain qui est vrai lorsque les capteurs IRH5 et IRV3 sont activés. Ainsi, l'utilisateur est situé dans la salle de bains. Cependant, nous avons exprimé les mêmes règles pour les espaces cuisine, salle de séjour, hall, salle à manger.

4.4.4 Exécution des règles avec Jess

Jess est un moteur de règles écrit en langage JAVA, offrant une implémentation à base de langage Clips pour réaliser un système de programmation par règle permettant de développer des moteurs d'inférence [Jess 2015].

La figure 4.4.2 montre l'intégration et la transformation de la structure de données (classes, instances et règles) vers (faits, règles) sous Jess pour activer le processus de raisonnement. Une fois notre modèle ontologique chargé sous Jess, le processus d'inférence déduit de nouveau faits qui seront intégrés dans la base de faits. En fin d'exécution du moteur Jess, la nouvelle base de faits va être transformée en connaissances OWL [Wang et al. 2006] .

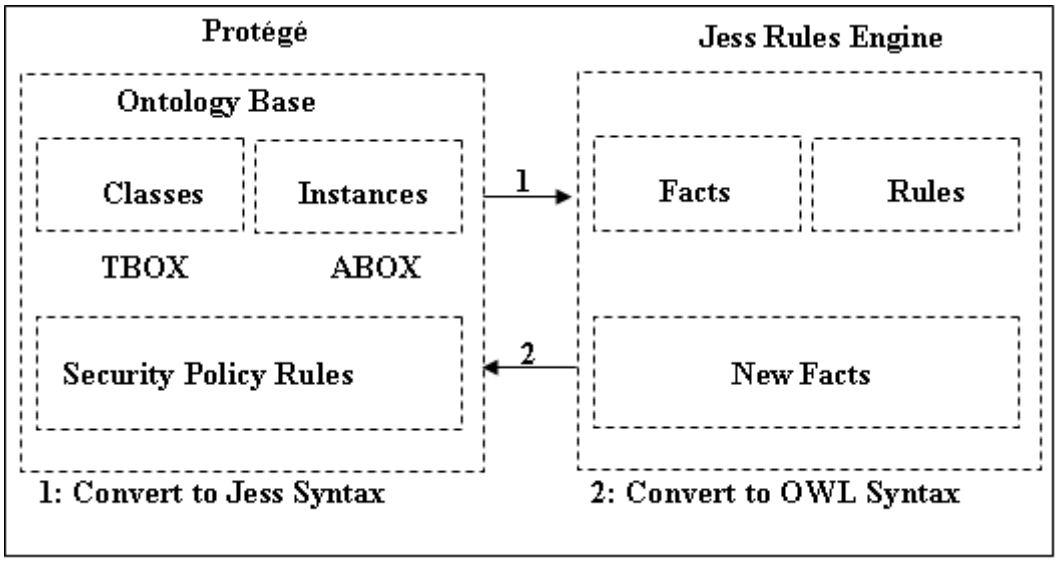

FIGURE 4.4.2 – Conversion des règles SWRL aux règles JESS.

Les règles définies ci-dessus peuvent être exploitées avec le moteur d'inférence Pellet [Sirin et al. 2007] [Pellet 2015] sous Jena [Carroll et al. 2004] comme illustré dans le code de l'algorithme 4.3.

4.5 Prise de décision

Le processus de prise de décision est assuré par la mise en place du raisonneur sémantique, il finalise le processus de raisonnement décrit dans la section 4.4 pour inférer les bonnes décisions.

Algorithme 4.3 Activation du processus de raisonnement sous Jena.

```
Reasoner reasoner = ReasonerRegistry.getOWLMiniReasoner();
reasoner = reasoner.bindSchema (model2);
Reasoner reasoner = PelletReasonerFactory.theInstance().
                    create();
 // Create the inference model with Pellet reasoner;
InfModel infModel = ModelFactory.createInfModel(reasoner,
                    model2);
//Resource infBusDriver = infModel.getResource(NS+
                            "BusDriver");
```

La décision est formalisée comme règle, qui combine les différentes données complexes. Nous avons introduit dans notre modèle quatre politiques qui sont principalement : Permission, Recommandation, Obligation et Interdiction. Les politiques sont définies comme suit :

- La politique d'autorisation est attribuée dans le cas où la règle suivante est vérifiée :

$Policy\,Permission(x) \leftarrow utilisateur(?X) \wedge Has\,Behavior_5(?X, ?Y) \wedge$

$Has\,Normal\,Situation(?X, ?Z) \wedge Has\,Profile_1(?X, ?A) \wedge$

$Asked\,Service(?X, Service\,Open\,Door\,To\,go\,Out)$

- Une décision d'Obligation est attribuée dans le cas où la règle suivante est vérifiée :

$Policy\,Obligation(x) \leftarrow utilisateur(?X) \bigwedge Has\,Behavior_3(?X, ?Y) \bigwedge$

$Has\,Critic\,Situation(?X, ?Z) \bigwedge Has\,Profile_1(?X, ?A) \bigwedge Asked\,Service(?X, ?C)$

- Une décision d'interdiction est attribuée dans le cas où la règle suivante est vérifiée :

$Interdiction(?X) \leftarrow utilisateur(?X) \bigwedge Has\,Behavior_0(?X, ?Y) \bigwedge$

$Has\,Emergency\,Situation(?X, ?Z) \bigwedge Has\,Profile_2(?X, ?A) \bigwedge Asked\,Service(?X, ?C)$

- Une décision de recommandation est accordée dans le cas où la règle suivante est vérifiée :

$Recommendation(?X) \leftarrow utilisateur(?X) \bigwedge Has\,Behavior_0(?X, ?Y) \bigwedge$

$Has\,Emergency\,Situation(?X, ?Z) \bigwedge Has\,Profile_2(?X, ?A) \bigwedge Asked\,Service(?X, ?C)$

4.6 Mesure de performance

Pour évaluer la performance de notre modèle de contrôle d'accès, on a choisi le paramètre « temps de réponse », celui-ci est le temps nécessaire pour résoudre la tâche de raisonnement. Cela signifie que nous ignorons l'utilisation des ressources du système, ce qui pourrait être une autre mesure intéressante pour mesurer les performances. On sépare le temps de chargement et le temps interrogation de l'ontologie pour comparer équitablement la performance de raisonneurs.

- Temps de chargement (P) :

Ce temps est pris pour charger ainsi pour contrôler de ABox.

- Temps de réponse (Q) :

Commençant par l'exécution de la requête et se termine lorsque tous les résultats de la requête ont été stockés dans une variable locale. Habituellement, le moment de la requête signifie lorsqu'une requête est exécutée alors sans compter le temps pour l'itération les résultats.

L'évaluation des performance est indiqué dans le tableau 4.3.

Paramètres	Valeurs
Temps de chargement	0.010
Temps de réponse	0.008

TABLE 4.3 – Évaluation des performances.

4.7 Conclusion

Ce chapitre décrit le processus d'élaboration de notre politique de sécurité à travers ses quatre principales phases : apprentissage , modélisation, raisonnement et prise de décision.

Ce chapitre a montré l'exploitation des technologies du web sémantique et la technologie de fouille de données (Data Mining) pour la conception d'un système de contrôle d'accès personnalisé et adaptatif, appliqué au domaine de la télé-assistance. Des cas d'étude vont faire l'objet du chapitre suivant montrant l'utilité de l'approche proposée vis-à-vis des personnes âgées dépendantes en terme d'assistance personnalisée et adaptative.

Chapitre 5

Validation

Les environnements intelligents sont une application spécifique des domaines émergents : l'informatique ubiquitaire et l'intelligence ambiante. En particulier, les espaces intelligents sont conçus pour supporter les personnes âgées dépendantes qui préfèrent vivre chez eux, avec plus de sécurité, plus d'autonomie dans des conditions de santé et de bien être de bonne qualité. Grâce au développement des technologies de l'information et de communication, la télémédecine est mise en place dans ces espaces de vie intelligents. Ce chapitre a pour but d'explorer les principaux concepts liés à la télémédecine et plus particulièrement à la plateforme de télé-vigilance qui a pour but de suivre le comportement de la personne dans son espace de vie. On exploite toute cette avancée technologique pour mettre en valeur l'approche développée dans ce travail de thèse.

5.1 Télémédecine

Grâce au progrès des nouvelles technologies de communication et des réseaux mobiles, les personnes âgées dépendantes peuvent bénéficier d'un grand nombre d'applications dédiées à leur cadre de vie. La Télémédecine est devenue possible au sein des habitats de cette population. Afin de leur fournir un soutien médical ou des soins à distance.

[Wootton et al. 1999] définit la Télémédecine :
«L'investigation, la surveillance et la gestion des patients et l'éducation des patients et du personnel médical, qui permettent un accès facile à des conseils d'experts et de l'information du patient, peu importe où se trouve le patient ou l'information pertinente ».

D'après [Wiki 2015], « La télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle

met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figure nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients. La définition des actes de télémédecine ainsi que leurs conditions de mise en œuvre et de prise en charge financière sont fixées par décret, en tenant compte des déficiences de l'offre de soins dues à l'insularité et l'enclavement géographique».

Selon [Thiberghien 2012] et [Alloulou 2013], ont montré dans leur étude que le taux de croissance de la population âgée dépendante est en progression très rapide ainsi que leurs besoins en termes de surveillance et d'assistance. Cependant, les espaces de vie sont devenus de plus en plus connectés et chargés de dispositifs. Les services de surveillance et d'assistance sont devenus possibles grâce aux technologies dont disposent nos environnement actuels.

5.1.1 Services de Télémédecine

Dans le domaine de la Télémédecine, [TMD 2015] distingue quatre types de service possibles à fournir aux patients :

- **Télé-consultation :** ce service est assuré par un professionnel médical qui effectue une consultation à distance pour un patient.
- **Télé-expertise :** ce service a pour objet de permettre à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux en raison de leurs compétences particulières, sur la base des informations médicales liées à la prise en charge d'un patient.
- **Télésurveillance :** ce service est assuré par un professionnel médical qui interprète à distance et prend les décisions relatives à la prise en charge du patienttout en sebasant sur les enregistrements effectués auprés du patient.
- **Téléassistance :** ce service consiste a exploité la télésurveillance pour assister à distance le patient.

5.1.2 Télé-surveillance

La télésurveillance est une branche de la télémédecine, dédiée à la surveillance, à distance, du comportement des personnes âgées dépendantes ou à risques afin de leur assurer plus de sûreté et d'autonomie le plus long possible. Cela est mis en place grâce à automatisation des traitements médicaux.

La mise en place de ce service nécessite l'utilisation de capteurs de données de types différents (portés par la personne ou installés dans l'environnement) qui peuvent capter le maximum de données (pression artérielle, poids, température, saturation du sang en oxygène, température ambiante, temps, emplacement). Ces capteurs sont, dans la plupart des cas, sans fil (Bluetooth, Wi-Fi, etc) pour plus de liberté de mouvement et de portabilité.

Les données doivent êtres transmises et interprétées par des spécialistes de la santé (médecin, infirmière, etc) pour assurer un contrôle et une assistance de bonne qualité.

Dans le cadre de ce travail de thèse, les fonctionnalités de suivi de la personne et de surveillance du comportement ont été exploités grâce à la plateforme de télévigilance, qui sera décrite dans la section 5.2.

5.1.3 Télé-assistance

Ce service assure une assistance à distance pour les personnes tout en exploitant les données collectées et interprétées avec le service de surveillance. Principalement, ce service a pour objet de prendre des décisions d'assistance et des conseils relatifs à la prise en charge des personnes.

Notre modèle de contrôle d'accès développé dans cette thèse est validé dans le cadre de la mise en place d'un service de téléassistance par l'exploitation de la plateforme de télé-vigilance.

5.2 Plateforme de Télé-vigillance TSP / ESIGETEL

La plateforme de Télévigilance médicale développée conjointement par l'Esigetel et Télécom SudParis [Medjahed, 2010], est intégrée dans un environnement de type habitat intélligent, peut avoir recours à la fusion des signaux actimétriques / vitaux du système porté par le patient avec d'autres capteurs ou modalités (selon le degré de traitement). Ces dispositifs sont munis d'un réseau de capteurs infrarouge de détection de présence généralement situés dans chaque pièce de l'habitat ou de capteurs sonores (microphones). Ils permettant de détecter des sons liés à la chute anormale d'objets dans l'habitat potentiellement provoquée par une situation de détresse. D'autres modalités peuvent être ajoutées et fusionnées avec les précédentes pour détecter par exemple les

chutes, comme la vision par ordinateur permettant la localisation précise de la personne et le suivi de ses postures de manière assez fiable lorsque les conditions d'éclairage le permettent.

La plateforme de Télévigilance médicale [Medjahed, 2010] composée essentiellement de trois systèmes : GARDIEN, RFPAT et ANASON, a pour but de détecter des situations de détresse diverses comme la chute, des modifications du rythme cardiaque (tachycardie, bradycardie), des profils quotidiens anormaux et la détection de sons anormaux procurant ainsi des informations contextuelles précieuses. Elle simule une maison avec cinq éspaces de vie : Salon, chambre à coucher, salle à manger, salle de bain et un espace technique comme illustré dans la figure 5.2.1.

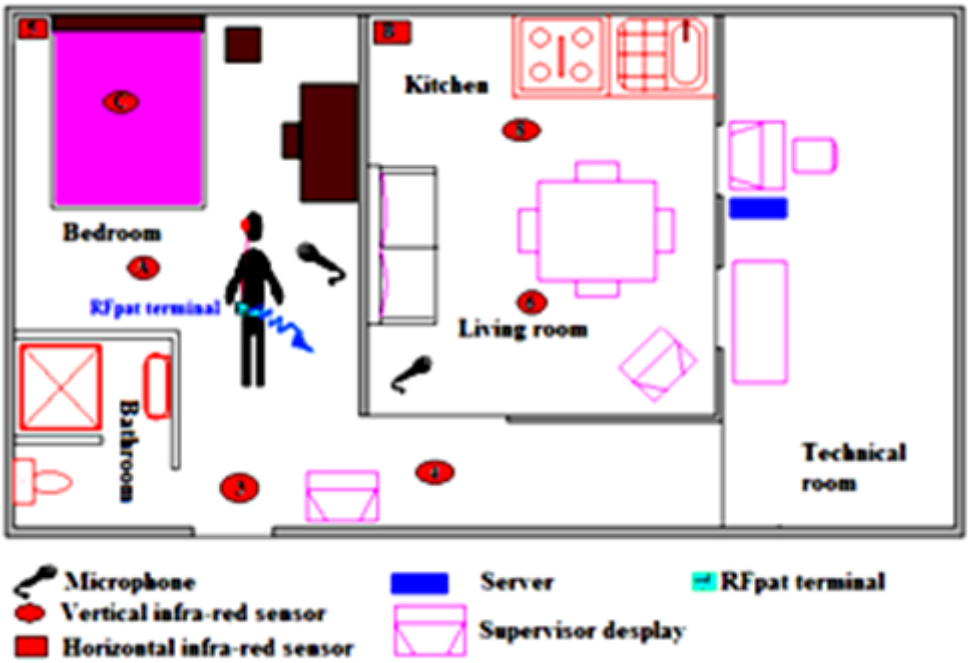

FIGURE 5.2.1 – Plateforme de télé vigilance.

La plateforme est capable de détecter les situations de détresse à distance en croisant trois modalités différentes : un capteur embarqué sur la personne qui mesure les signaux vitaux et détecte la chute de la personne (RFPAT), des capteurs infrarouges qui détectent la présence et la position de la personne (Gardien) et une analyse de l'environnement sonore (ANASON).

Cette variante de dispositifs comme illustré dans la figure 5.2.2, cela fournit un aspect d'hétérogénéité à la plateforme, cela exige des systèmes de décision

de diverses natures (classifieurs basés sur des seuils, algorithmes de reconnaissance de formes ou experts) et d'un ensemble de plusieurs capteurs de signaux de mouvement, vitaux, sonores et de localisation. Le recours à des méthodes de fusion de données hétérogènes est donc nécessaire, afin d'obtenir des informations plus fiables.

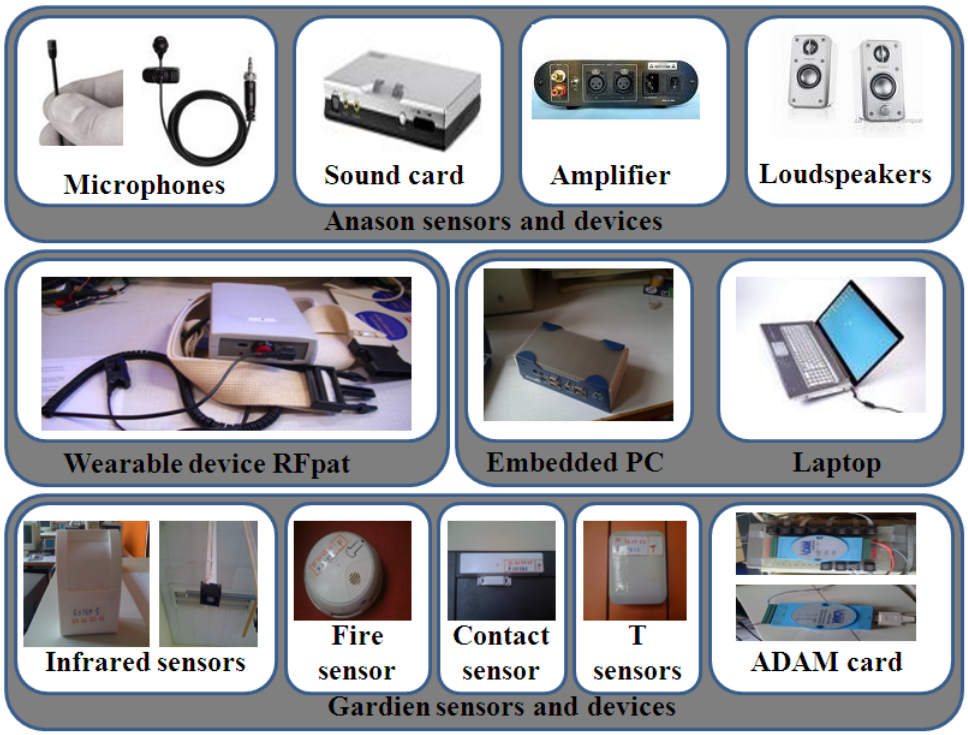

FIGURE 5.2.2 – Les capteurs et dispositifs exploités dans la plateforme de Télévigilance.

5.2.1 Système ANASON

Les informations extraites à partir de sons de l'environnement sont de plus en plus utilisées dans les applications de Télévigilance, comme la détection de chutes et des activités habituelles, situations de détresse ou sons anormaux. L'utilisation de systèmes sonores possède des avantages comme son intrusivité limitée, son coût modéré et son installation facile où les données sont stockées dans un ordinateur pour le traitement et l'analyse. Le système classification sonore proposée nommé ANASON analyse en temps réel les sons de l'environnement et utilise un premier module de détection et d'extraction des signaux de son et de parole utiles basé sur la transformée en ondelettes. Ce module est utilisé sur tous les canaux audio simultanément, en temps réel. Seulement

des signaux sonores extraits sont traités par les modules placés en amont. Le deuxième module classifie les événements sonores extraits entre son ou parole. Ce module, comme un mécanisme d'identification sonore, est basé sur l'utilisation de modèles GMM (Gaussian Mixture Model). Si un son a été détecté, le signal est traité par un mécanisme d'identification et classifié parmi des classes prédéfinies comme claquement de porte, bris de verre, chute d'objet, vaisselle, sonnerie de téléphone, etc. Si un son de parole est détecté, un mécanisme de reconnaissance de parole est initialisé. Le système de reconnaissance de parole détecte des expressions de détresse classiques comme : " à l'aide ! ", " au secours ! ", " Appelez le Médecin ! ".

5.2.2 Système RFPAT

Le système RFPAT est destiné à aider les personnes dépendantes (personnes âgées, cardiaques, ...) au travers du traitement de signaux physiologiques et actimétriques relatifs à cette personne ; cela passe en particulier par la réalisation de capteurs robustes et d'algorithmes de traitement du signal embarqués, mais aussi d'algorithmes de reconnaissance des formes et de fusion de données multimodales en vue d'identifier de manière automatique des situations de détresse telles que les chutes de personne, le changement brutal de profil médical (bradycardies et tachycardies) ou actimétrique du patient (c'est-à-dire relatif à son activité), ceci au travers de ses paramètres médicaux (pouls,..) et de son comportement général (activités, mouvements, démarche....).

Le terminal portable est constitué :

- d'un terminal mobile : il s'agit d'un boîtier que le patient ou la personne âgée porte en permanence à la ceinture lorsqu'elle est chez elle. Il mesure les données vitales et actimétriques (mouvement, posture) de la personne et les transmet à une station réceptrice, applique les traitements d'analyse et de fusion de ces signaux avec ceux des autres modalités
- d'un terminal fixe : il s'agit d'une station de réception connectée à un ordinateur personnel (PC). Il reçoit les signaux vitaux déjà traités du terminal mobile placé sur le patient

Le terminal portable RFPAT, comporte des filtres numériques de réduction du bruit et des algorithmes de traitement des données. Ces filtres et algorithmes sont appliqués respectivement à tous les signaux acquis : signaux de mouvements, de posture et de pouls (fréquence cardiaque). Ces signaux sont détaillés ci-après :

Signal de Mouvement : décrit l'état acté-métrique de la personne surveillée qui représente le pourcentage de mouvement. Il calcule la durée totale des mouvements de la personne surveillée pour chaque intervalle de temps. La sortie du paramètre mouvement est représentée sur 4 bits avec des valeurs variant de 0 (état immobile) à 15 (activité intense). La période d'échantillonnage est de 30 secondes.

Signal d'inclinaison (posture) : est représenté en deux états : debout / assis et allongé. La posture est un paramètre très utile sur l'activité de la personne. Grâce à des dispositifs acté-métriques embarqués ce système peut détecter la posture de la personne. Cette information peut être interprétée comme des informations utiles sur les activités de la personne, comme la discrimination entre les activités "dormir" et "chute".

Signal de détection de la Chute : le terminal portable possède des algorithmes embarqués pour traiter ses propres données acquises. Un algorithme très utile de détection de la chute est implémentée dans le boitier. Lorsque la personne se rapproche du sol très rapidement, l'accélération et le capteur détecteur de l'impact dépassent des valeurs de seuil, une chute est alors détectée. Cette méthode est très performante : en effet plus de 92% des chutes sont détectées.

Signal du Pouls : est mesuré par un capteur ambulatoire de pouls placé à l'oreille de la personne surveillée. Après l'acquisition, le signal est traité, débruité et enregistré. La fréquence cardiaque est mesurée sur une moyenne des signaux de pouls toutes les 30 secondes. Le dé-bruitage des données de pouls est une tâche très importante pour avoir des mesures de qualité. Les valeurs du pouls sont mesurées avec une marge d'erreur de 5%, ceci en conformité avec les recommandations des professionnels de santé. Les données recueillies par les différents capteurs sont transmises, par radio grâce au protocole Zigbee, à une base fixe de réception. L'utilisation de composants électroniques de faible consommation garantissent une autonomie qui reste en conformité avec les recommandations des professionnels de santé.

5.2.3 Système GARDIEN

Le système GARDIEN est composé par un réseau filaire ou sans fil de capteurs de mouvement infrarouge. Ces capteurs sont excités par le mouvement des corps dégageant de la chaleur et peuvent par conséquence indiquer la présence d'une personne dans sa zone de couverture. Les informations mesurées par les capteurs sont de type binaire 0 (inactif) et 1 (actif). Les signaux sont transmis avec une période d'échantillonnage de 0,5 secondes par protocole radio ou filaire vers une base fixe connectée à un ordinateur pour le traitement des données. Dans l'étape de traitement, l'algorithme GARDIEN transforme les données binaires en paramètres : localisation, mouvement et posture de la personne.

Localisation : Chaque capteur est associé à une pièce de la maison et peut indiquer la localisation de la personne. La précision de localisation peut être augmentée avec l'utilisation de plusieurs capteurs par pièce.

Mouvement : Le mouvement est une information mesurée à partir du nombre de capteurs excités par minute. Ce paramètre est important et indique si la personne est immobile ou active. Il peut être utilisé comme information supplémentaire par d'autres modalités.

Posture : La posture de la personne peut être estimée à partir de la combinaison de deux types de capteurs infrarouges, l'un à champ de détection horizontal, l'autre vertical.

Le capteur horizontal est placé, dans un niveau d'environ 1 mètre du sol, et détecte la présence de la personne au-dessus de ce niveau. Si la personne est au-dessous de ce niveau, par exemple allongée, ce capteur ne détectera pas sa présence.

Un capteur à champ vertical permet alors de confirmer la présence de la personne dans la pièce.

Cette combinaison peut indiquer une chute, l'état allongé de la personne ou une situation où la personne est en train de chercher quelque chose par terre. Ces informations, combinées avec les autres modalités comme RFPAT et ANASON peuvent indiquer plus précisément l'état réel de la personne.

5.2.4 Bases de données de la plateforme de Télé-vigilance

5.2.4.1 Base HOMECAD

Cette base a été construit dans le cadre des travaux de [Medjahed 2010], c'est une base multimodale, appelée HOMECAD (Home Remote Medical Care Database), constituée de données physiologiques, acté-métriques et sonores issues des systèmes RFPAT, GARDIEN et ANASON. Cette base garde la trace du contexte de la vie quotidienne des personnes âgées. Les scénarios enregistrés reflètent des cas réels, la durée de chaque scénario est de 10 minutes. les scénarios sont distingués en deux classes suivant l'occurrence ou non d'un évènement de détresse.

1. Types de scénario obtenus

- Scénario critique
  - L'acteur est assis sur une chaise dans le salon, il lit un journal (120) ;
  - Il se lève et va au toilettes et à la salle de bain (60) ;
  - Il quitte la salle de bain, il se rend à la cuisine pour préparer son café (180) ;
  - Il retourne au salon, et il boit son café (120) ;
  - Il se lève, il trébuche et tombe, et il reste couché (120) ;
- Un scénario normal
  - L'acteur rentre à la maison, il ferme la porte, il met les clés sur la table (60)
  - Il se dirige vers la salle de bain pour laver les mains (60)
  - Il va à la salle de séjour et il allume la télé pour regarder les nouvelles (240)
  - Il s'allonge sur le canapé pour faire une sieste (240)

5.2.4.2 Base Collégiale

Cette base correspond au données vocales collectées du système ANASON, l'enregistrement des données a été effectué dans le cadre du projet compagnon. Cette base n'a pas été exploitée dans ce travail.

5.2.4.3 Base Chute

Cette base a été construite dans le cadre des travaux de [Cavalcante 2012], Cette base de données est constituée de signaux vitaux, de signaux de mouvement et de localisation, extraits des systèmes RFPAT et GARDIEN, et ils sont utilisés pour composer essentiellement des scenarios simulés ayant des situations de chutes d'accélérations fortes ou bien faibles (appelées respectivement "fortes" ou "molles"). Les chutes fortes sont de quatre types : chute debout vers l'avant, chute debout vers la droite, chute debout vers la gauche et chute latérale depuis une chaise. Par contre, les chutes molles sont de deux types : chute molle par affaissement le long d'un mur et chute molle en se retenant à une table.

Cinq scénarios de 2 minutes environ ont été enregistrées en simulant des chutes fortes et molles sont décrits ci-dessous :

Scenario 1 :
- Le patient est dans la chambre (30)
- Il se dirige vers la salle de bain pour se brosser les dents (30)
- Il se dirige vers la cuisine pour préparer son petit déjeuner et il chute dans la cuisine (60)

Scenario 2 :
- Le patient se prépare à manger dans la cuisine (30).
- Il se dirige vers le séjour (30).
- Il fait une chute dans le séjour (60).

Scenario 3 :
- Le patient est dans la cuisine (30).
- Il se dirige vers la salle de bain (30).
- Il chute dans le couloir (60).

Scenario 4 :
- Le patient est assis dans le bureau (30).
- Il se sent fatigué et se dirige vers la chambre (30).
- Il chute dans la chambre (60).

Scenario 5 :
- Le patient est assis au séjour et regarde la télé (30).
- Il se dirige vers le bureau pour voir ses emails. (30)
- Il chute dans le bureau (60)

5.3 Étude de cas

Dans ce chapitre, on présente une étude de cas afin de montrer l'utilité de notre politique de sécurité, plus précisément on montre les apports en matière d'intelligence, de personnalisation et d'adaptabilitédans la sécurisation de la personne âgée dépendante.

Scénario :

Nous proposons un scénario expérimental pour montrer l'importance d'une politique de sécurité adaptée et personnalisée. Jean est une personne âgée , mais récemment, il devient plus fragile et il peut se trouver dans une situation de détresse (chute) et il vit avec un handicap visuel. Cette situation a commencé il y a deux ans. Pour cela, il a besoin d'une assistance automatique en surveillant ses activités quotidiennes (rentrer à la maison , prendre une douche ou la préparation des repas). Parfois, Jean a le comportement critique suivant :

— Il est assis sur une chaise dans le salon (bureau),

— Il se lève et va à la salle de bain et aux toilettes (60).

— Il quitte la salle de bains ; il va à la cuisine pour préparer le café (180).

— Il retourne dans le salon pour y rester, et il boit son café (120).

— Il se lève , il trébuche puis il tombe et il reste couché (120)

Les données captées sont injectés dans l'ontologie comme des instances sur les classes définies et il fait appliquer les règles définies à déduire de la décision et la notification appropriée , comme illustré sur la figure 5.3.1. Selon le scénario enregistré , la personne est tombée dans le salon pendant qu'elle prenait son café. Les paramètres suivant sont identifiés : (chute = 1) , (activité = 14) , (posture = 1) et (dispositifs activés : IRV6 , IRHB) .

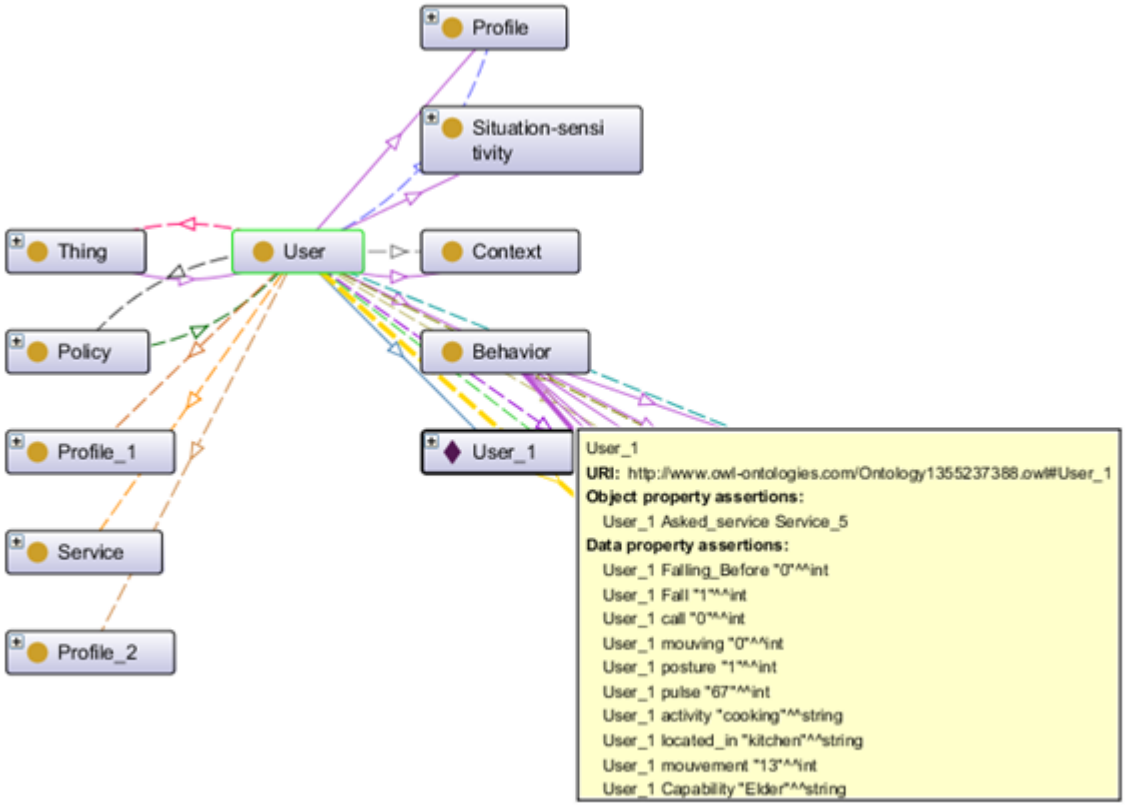

FIGURE 5.3.1 – Injection des données du scénario en tant que instances.

A partir des données détectées, les règles infèrent que l'utilisateur a un comportement associé au motif (pattern_5) ; une situation d'urgence est identifiée. L'utilisateur se trouve dans le salon parce que les dispositifs (IRV6 , IRHB) sont activés et l'utilisateur a fait une chute avant où le soignant doit être informé afin de recommander des orientations d'aide sous forme vocale en tenant en compte de la déficience visuelle de l'utilisateur. l'enchainement des règles est comme illustré dans la figure 5.3.2.

5.3.1 Dérivation des droits d'accès

Une fois que la décision est dérivée par le processus de raisonnement, une requête est construite pour récupérer la décision au moyen du protocole SPARQL. La réponse est envoyée par l'intermédiaire d'un SMS à la personne mobile concernée et affichée dans la plate-forme de télé-surveillance. Selon le cas présenté ci-dessus, une situation d'urgence est détectée, personne aveugle alors un message vocal est envoyé afin d'assister cette personne.

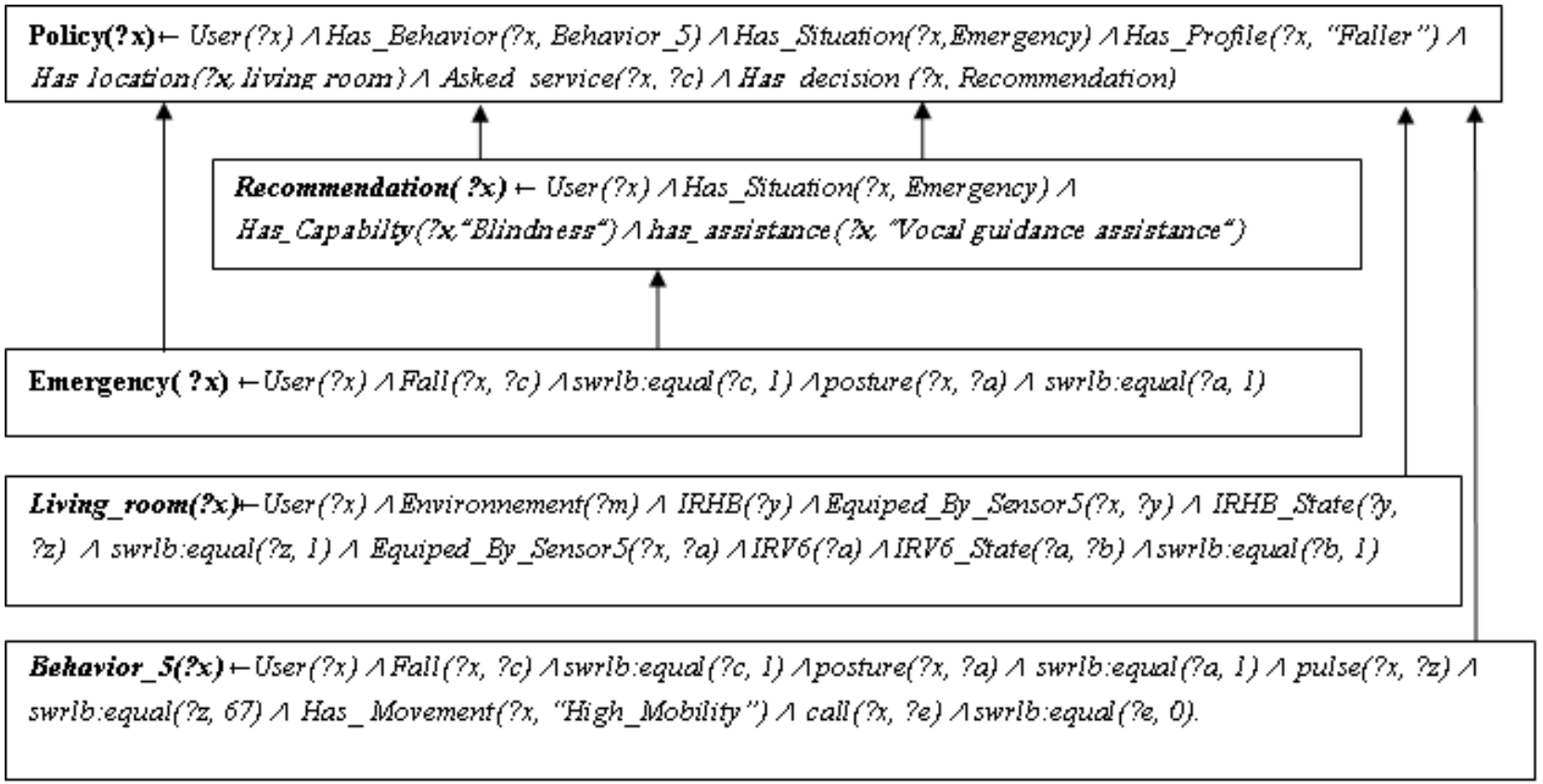

FIGURE 5.3.2 – Dérivation de la décision suivant les données acquises.

Algorithme 5.1 Interrogation de l'ontologie.

```
// Create a new query
String queryString =              "PREFIX onto:
<http://www.owl-ontologies.com/Policy.owl>"
+                 "SELECT *"+
"WHERE {"+
"?User a  <http://www.owl-ontologies.com/Ontologypolicy.owl#User>} \n ";
  Query query = QueryFactory.create(queryString);
        System.out.println("----------------------");
        System.out.println("Query Result Sheet");
        System.out.println("----------------------");
        System.out.println("Direct&Indirect Descendants (model1)");
        System.out.println("--------------------");
// Execute the query and obtain results
QueryExecution qe = QueryExecutionFactory.create(query, infModel);
com.hp.hpl.jena.query.ResultSet results =
qe.execSelect();
// Output query results
ResultSetFormatter.out(System.out, results, query); }
```

Une fois les données sont acquises, une requête est construite afin de récupérer la politique de décision qui est réalisée au moyen de SPARQL requête sous Jené da, comme illustré dans Algorithme 5.1. La personne assistante (caregiver) sera notifiée, la décision sera affichée et par conséquent, l'assistant va adapter les décisions en fonction de la situation de détresse, les capacités et les préférences des utilisateurs en tenant compte les déficiences de l'utilisateur. Au niveau de ce processus, on distingue deux types de requête, d'authentification et d'autorisation où les décisions récupérées sont (oui ou non) ou (permis, interdit, obligé ou recommandé) respectivement.

5.3.1.1 Requête d'authentification

Dans notre cas, il est inutile de passer une requête d'authentification car il y a qu'une seule personne dans l'habitat mais elle sera utile dans le cas où il y aura différents profils dans le même environnement.

5.3.1.2 Requête d'autorisation

Lors de la demande d'un service, l'utilisateur est notifié par la décision la plus appropriée avec la prise en compte de son capacité. Comme l'utilisateur est non voyant, il doit être notifié par signal vocal.

5.3.2 Analyse et discussion

La politique de sécurité est focalisée sur l'enregistrement de données réelles pour la mise en place du processus de gestion et de l'affectation de décision de validation qui dépend de la capacité de l'utilisateur. La spécificité de notre politique de sécurité est due à l'utilisation des données contextuelles riches comprenant les données d'environnement (lieu, temps) et les données du corps (chute, impulsion, mouvement) . Grâce aux données issues de sources multiples, nous sommes capables d'en déduire des données contextuelles plus complexes, qui sont principalement : le comportement , le profil et la situation de détresse. Afin de faire face à toutes ces données hétérogènes, nous avons choisi de mettre en œuvre une ontologie pour notre modèle proposé vu les avantages de modélisation , de raisonnement et d'interrogation. Notre objectif est atteint par le moyen du comportement historique et l'exploitation de profil. Spécialement , le contexte actuel nous permet de réagir sur les situations identifiées dand le but d'assurer une politique de sécurité plus adaptative . Après de nombreuses expériences , l'approche est sensible au nombre de cas de plus en plus définie par contraste , il n'est pas important que le nombre de règles. Le système prend en charge jusqu'à 60 instances des entités entières. Il n'y a pas de limitation du nombre de règles et de la réponse temporelle de la requête ne dépend pas de la taille de l'ontologie qui est en moyenne de 0,0080 ms . Nous espérons améliorer notre politique de sécurité en explorant le troisième système ANASON. Ainsi, il est utile d'étendre le modèle et ajouter des données et des règles en fonction de chaque situation particulière . En fait , le modèle est conçu pour satisfaire les besoins des médecins et des personnes dépendantes vivant seules dont le but est d'aider plus adéquatement cette population dépendante. Nous notons que notre modèle peut être largement utilisé pour identifier et authentifier les utilisateurs anonymes en vérifiant leur comportement basé sur l'historique.

5.3.3 Conclusion

A partir de cette étude de cas, on a montré l'utilité d'une politique de sécurité personalisée et adaptative et son apport dans le domaine de la télé surveillance pour mettre en place une solution de téléassistance.

Ce chapitre présente la plateforme de télé vigilance ainsi que les trois systèmes qui la composent : ANASON, GARDIEN et RFPAT. Cette plateforme nous a servi dans la phase d'acquisition de données et la phase d'adaptation aux

différentes situations identifiées tout en montrant l'utilité et l'apport d'avoir une politique de contrôle d'accès personnalisée et adaptative.

Partie 3 : Conclusion

Conclusion Générale et Perspectives

Travail accompli

Avec la croissance démographique, on assiste à une augmentation du taux de la population en perte d'autonomie en raison de déficiences physiques ou mentales, soit en raison de leur vieillissement (personnes dépendantes). Au cours des deux dernières décennies, on assiste au développement de services et d'application dédiées à l'amélioration de l'état et du bien être de ces personnes dans leurs espaces de vie. Dans les applications de télé-assistance et télémédecine, l'intelligence ambiante a permis d'introduire plus de confort et d'apporter plus d'autonomie à ces personnes dépendantes. Les données collectées dans ces espaces de vie sont exploitées par les techniques d'apprentissage, de modélisation, de raisonnement pour fournir des services sensibles au contexte. On constate une certaine complexité lors de la gestion de ces données contextuelles mais cela fournit des solutions intelligentes, flexibles et plus adaptées aux besoins des personnes dépendantes.

Le défi principal motivant ce travail réside dans le fait de développer une solution d'aide et d'assistance pour les personnes dépendantes tout en exploitant les avantages des environnements intelligents.

Le travail effectué dans cette thèse porte sur la conception et l'implémentation d'une politique de sécurité et sa mise en place par un modèle de contrôle d'accès représenté par une ontologie évolutive. Le modèle est basé sur le comportement et les capacités des utilisateurs dans les environnements intelligents. La politique de sécurité est mise en place par un modèle nommé UBC-ACM (User Behavior Capability based Access Control Model) et son architecture UBC-ACA (User Behavior Capability based Access Control Architecture) dont le but est de répondre aux insuffisances identifiées d'après l'étude effectuée sur les modèles de contrôle d'accès et les anomalies possibles liées à la sécurité en termes d'adaptabilité et de personnalisation des services.

Notre travail est constitué de deux volets principaux :

Le premier volet porte sur l'étude bibliographique et l'analyse des travaux existants afin de mettre en valeur les éléments clés pour la résolution de

la problématique. Le chapitre 1 présente l'évolution de l'informatique ubiquitaire, l'impact de l'intelligence ambiante sur les applications de communication puis une introduction sur la sensibilité au contexte dans les espaces de vie (habitats, espaces de travail, hôpitaux). La suite du chapitre, est consacrée au cycle de vie des données contextuelles (acquisition, modélisation, raisonnement et adaptation). Dans le chapitre 2, une étude sur les modèles de contrôle d'accès dynamiques sensibles au contexte, la préservation de la vie privée et la confiance est développée. Dans les modèles existants, les données contextuelles sont limitées aux données spatio-temporelles et environnementales. D'où l'approche proposée qui consiste à intégrer le comportement et les capacités de l'utilisateur pour atteindre une authentification plus forte des utilisateurs et une gestion plus fine de contrôles d'accès aux services. Le développement de cette politique a eu recours aux technologies de fouille de données (classification).

Le deuxième volet consiste à présenter l'approche développée dans cette thèse. Elle définit les entités principales du modèle décrivant la politique de sécurité ainsi que l'architecture assurant le développement du modèle. L'approche proposée est basée sur le suivi du comportement et l'identification de la capacité où l'assignation des droits d'accès liée à la validité de la situation par rapport au service demandé. Celle-ci est mise en place via un modèle défini par le bais d'une ontologie et alimentée avec une architecture qui sert à acquérir et traiter les données contextuelles. L'architecture assure la gestion des données contextuelles. Le chapitre 3 présente le nouveau modèle de contrôle d'accès baptisé UBC-ACM (User Behavior and Capability based Access Control Architecture) ainsi que son architecture qui sont basés sur une ontologie comportant 5 classes principales : utilisateur, dispositifs, service, environnement et politique de sécurité. Ces politiques sont spécifiées comme un ensemble de règles au format SWRL. Un raisonneur sémantique a été utilisé pour l'inférence des décisions relatives à l'authentification et le contrôle d'accès. Ce raisonneur a été implémenté en utilisant un outil open source OWL-DL. Deux types de requêtes relatives à l'authentification et à l'autorisation ont été effectuées en utilisant le langage SPARQL. Le chapitre 4 présente les différentes phases de développement de l'architecture associée au modèle. Il s'agit d'une architecture de gestion semi-automatique qui à partir du profil, du comportement et du contexte courant de l'utilisateur ; fournit les décisions sur l'authentification et l'autorisation. Une étude de cas illustrant cette approche a été élaborée en s'inspirant de quelques scénarios extraits du corpus de données. Le dernier chapitre présente la validation de la politique de sécurité au moyen de la plateforme de télé-vigilance utilisée pour extraire les comportements à risque et leur utilisation pour définir l'ontologie de contrôle d'accès et ce afin de montrer la dérivation des droits d'accès suivant la situation de l'utilisateur qui se présente. Dans la phase de test et de validation du modèle et de l'architecture développés (UBC-ACM et UBC-ACA), on a exploité les travaux réalisés sur la plateforme de télé-assistance et télé-vigilance pour :

1. L'extraction d'un corpus d'apprentissage et d'un corpus de test afin d'enrichir la base de connaissances du modèle UBC-ACM.
2. La mise en œuvre de scénarios de prise en compte du comportement et des capacités de personnes dépendantes dans les environnements intelligents.

Contributions

Notre contribution est liée à la conception d'une politique de sécurité basée sur la capacité et le comportement, la mise en place est assurée via un modèle de contrôle d'accès et son architecture. La politique de sécurité ciblée est réactive, personnalisée et adaptée à la capacité et le comportement de l'utilisateur, le contexte de l'utilisateur et les changements survenues dans l'environnement. Les décisions ne sont pas limitées à " permis " ou " refusé " comme droits d'accès. Afin, d'assurer le service d'assistance aux personnes dépendantes notre politique est étendue pour inclure des décisions plus appropriées : Permission, Obligation, Recommandation et Interdiction.

Le modèle de contrôle d'accès vise à mettre en œuvre la spécification de la politique de sécurité au moyen des ontologies en termes de modélisation , de raisonnement et d'interrogation en prenant en compte l'aspect sémantique et l'hétérogénéité des données issues de sources multiples.

L'architecture associée est mise en place au moyen des données contextuelles collectées dont la richesse est due à la combinaison des données sur l'environnement et les données sur le patient qui sont acquises via notre plate-forme de télésurveillance composée des systèmes RFPAT et GARDIEN. La plateforme de surveillance permet l'enregistrement du comportement passé (historique) qui est utilisé pour analyser en profondeur les situations à risque et de fournir un système sensible au contexte réactif pour assurer une meilleure assistance personnalisée aux personnes dépendantes. L'architecture est constituée des couches : acquisition, modélisation, raisonnement et adaptation.

La nouveauté de notre approche est due à la richesse des données contextuelles acquises de la plateforme de télé-surveillance. La particularité des données réside dans le fait qu'elle permet la détection d'une situation critique, urgence, anormale et normale.

Perspectives

Bien que nous ayons accompli un certain nombre de contributions mentionnées dans la section précédente, d'autres améliorations sont encore possibles. Comme suite de ce travail, on envisage de réaliser une extension du modèle présenté dans cette thèse, en tenant en compte les propositions suivantes sur différents niveaux :

1. Gestion de la qualité et de la confidentialité des données contextuelles
2. Modélisation et stockage avec le suivi continu du comportement de l'utilisateur rend alors la taille des données très importante.
3. Intégration d'autres modes de raisonnement, probabiliste ou floue pour remédier au problème d'incertitude des données.
4. Cadre applicatif réel : injecter le résultat obtenu au niveau des actionneurs
5. Acquisition des données :

— Extension du suivi de l'utilisateur dans son environnement (Interne et externe).
— Exploitation de diverses données contextuelles issues de différents types de capteurs portés, installés dans l'environnement ou issues des microphones.
— Intégration du système ANASON (données issues de microphone) dans le processus de modélisation et de raisonnement.
— Identification de différents profils au sein d'un habitat.
— Exploration d'autres jeux de données ayant pour but l'assurance de la télé-médecine.

Annexes

Annexe A

Logique Descriptive

Le développement d'une approche sensible au contexte exige de différents mécanismes pour la gestion de la connaissance. Pour cela, le fondement de base est la représentation de ces données avec une bonne expressivité. On s'est intéressé à la « logique descriptive » qui constitue la base indispensable à la compréhension des outils de la technologie du web sémantique en termes de modélisation et de raisonnement.

La représentation des connaissances est un domaine qui manipule les données symboliques tout en assurant des traitements automatiques. Cette discipline a eu une grande part d'utilisation dans le domaine d'intelligence artificielle.

A.1 Introduction à la Logique Descriptive

La logique de description aussi appelée logique descriptive (LD) est une famille de langages de représentation de connaissances qui peuvent être utilisées pour représenter la connaissance terminologique d'un domaine d'application d'une manière formelle, structurée et expressive. Le nom de logique de description se rapporte, d'une part à la description de concepts utilisée pour décrire un domaine et d'autre part à la sémantique basée sur la logique qui peut être donnée par une transcription en logique des prédicats du premier ordre [wiki] où les deux concepts désignent :

'Description' : représenter les connaissances afin d'exprimer celle-ci plus qu'en logique propositionnelle.

'Logique' : raisonner à partir de ces connaissances dont le but d'avoir de meilleures propriétés calculatoires que la logique des prédicats et étudier correctement le raisonnement.

La logique s'intéresse à trois aspects importants lors de la manipulation des données : syntaxe, sémantique et raisonnement.

Syntaxe : cet aspect traite les symboles atomiques, construction des règles et les structures symboliques.

Sémantique : cet aspect traite le sens des symboles atomiques et les règles dans la logique.

Raisonnement : cet aspect concerne les théorèmes logiques.

A.1.1 Base de connaissances dans la logique de description

La logique de description divise les connaissances en deux parties :

- Informations Terminologiques (TBOX) : définition des notions basiques ou dérivées et de la façon dont elles sont reliées entre elles. Ces informations sont « génériques » ou « globales », vraies dans tous les modèles et pour tous les individus.

- Informations Assertionnelles sur les individus (ABOX) : ces informations sont « spécifiques » ou « locales », vraies pour certains individus particuliers. Toutes les informations connues sont alors modélisées comme un couple < T,A>, où T est un ensemble de formules relatives aux informations terminologiques (la TBox) et où A est un ensemble de formules relatives aux informations sur les assertions (la ABox).

Le regroupement de ces données forme une base de connaissances.

A.2 Représentation des connaissances

La représentation des connaissances est considérée comme sous domaine de l'intelligence artificielle, elle vise à mettre en place les moyens de représentation des données au niveau des ordinateurs pour assurer d'autres fonctionnalités : planifier les nouvelles activités, décider la tache prochaine à faire.

A.2.1 Ajout de l'aspect sémantique

Une interprétation $\mathit{\Gamma} = \left(\Delta_{\mathit{\Gamma}}, .^{\mathit{\Gamma}}\right)$est la donnée d'un ensemble $\Delta_{\mathit{\Gamma}}$ appelé domaine de l'interprétation et d'une fonction d'interprétation $.^{\mathit{\Gamma}}$ qui fait correspondre à un concept un sous ensemble de $\Delta_{\mathit{\Gamma}}$ et à un sous-ensemble de $\Delta_{\mathit{\Gamma}}$X $\Delta_{\mathit{\Gamma}}$, de telle sorte que les équations suivantes soient satisfaites :

$$\tau^{\mathit{\Gamma}} = \Delta_{\mathit{\Gamma}}$$

$$\perp^{\mathit{\Gamma}} = \theta$$

$$(C \sqcap D)^{\mathit{\Gamma}} = C^{\mathit{\Gamma}} \cap D^{\mathit{\Gamma}}$$

$$(C \sqcup D)^{\mathit{\Gamma}} = C^{\mathit{\Gamma}} \cup D^{\mathit{\Gamma}}$$

$$(\neg C)^{\Gamma} = \triangle_{\Gamma} - C^{\Gamma}$$

$$(\forall r.C)^{\Gamma} = \left\{x \in \triangle_{\Gamma} / \forall y \ : \ (x,y) \in r^{\Gamma} \rightarrow y \in C^{\Gamma}\right\}$$

$$(\exists r.C)^{\Gamma} = \left\{x \in \triangle_{\Gamma} / \exists y \ : \ (x,y) \in r^{\Gamma} \wedge y \in C^{\Gamma}\right\}$$

$$(\geq n\ r)^{\Gamma} = \left\{x \in \triangle_{\Gamma} / | \left\{y \in \triangle_{\Gamma} / \ (x,y) \in r^{\Gamma}\right\} | \geq n\right\}$$

$$(\leq n\ r)^{\Gamma} = \left\{x \in \triangle_{\Gamma} / | \left\{y \in \triangle_{\Gamma} / \ (x,y) \in r^{\Gamma}\right\} | \leq n\right\}$$

$$(r_1 \sqcap \cdots \sqcap r_n)^{\Gamma} = r_1^{\Gamma} \cap \cdots \cap r_n^{\Gamma}$$

A.3 Inférence et Raisonnement

La modélisation d'un nouveau domaine exige la définition des concepts ainsi que leurs relations dans T afin de construire une base de connaissances. Pour assurer la cohérence et la consistance de la base de connaissances, le processus de raisonnement se charge à mettre en place les taches suivantes : Raisonnement et Inférence.

- Le raisonnement concerne la manipulation des connaissances déjà acquises pour produire de nouvelles connaissances. Il utilise des mécanismes d'inférence permettant la résolution des problèmes pour lesquels il n'existe pas de procédures explicites dans le programme.

Le système de raisonnement des Logiques de Description comprend deux mécanismes d'inférence principaux basés sur des calculs de relations de subsomption :

- La classification de concepts qui permet d'insérer un concept dans la hiérarchie.
- La reconnaissance d'instances donnant pour un individu les concepts les plus spécifiques dont il est instance.

Les raisonnements sur la base de connaissances se font au niveau de de la TBOX (axiomes) et au niveau de la ABOX (faits). L'hypothèse du monde ouvert prévaut : il peut exister des faits qui ne sont pas (encore) dans la ABOX. Ils ne sont pas faux (hypothèse du monde fermé), ils sont inconnus.

-L'inférence est l'opération qui consiste à admettre une proposition en raison de son lien avec une proposition préalable tenue pour vraie. C'est un terme général dont les mots raisonnement, déduction, induction sont des cas spéciaux.

Les inférences sont réalisées par des raisonneurs (moteurs de raisonnement) qui découvrent des connaissances implicites. Il existe deux niveaux d'inférence, ce sont l'inférence au niveau terminologique et l'inférence au niveau d'assertion :

• Inférence au niveau d'assertion : cohérence de la ABOX, vérification d'instance, vérification de rôle, réalisation de la ABOX

• Inférence au niveau terminologique : satisfiabilité, subsomption, trouver les concepts équivalents, trouver les concepts disjoints.

1. **Satisfiabilité :** un concept C est salifiable par rapport à Γ s'il existe un *modèle* J de Γ tel que C^J est non-vide. Dans ce cas, nous pouvons dire que J est *modèle* de C.
2. **Subsomption** : un concept C est subsumé par un concept D par rapport à Γ si $C^\Gamma \subseteq D^\Gamma$ pour chaque *modèle* J de Γ. Dans ce cas, nous écrivons $C \sqsubseteq_\Gamma D$ ou $\Gamma \models C \sqsubseteq D$.
3. **Équivalence** : deux concepts C et D sont équivalents par rapport à Γ si $C^J = D^J$ pour chaque *modèle* J de Γ. Dans ce cas, nous écrivons $C \equiv_\Gamma D$ ou $\Gamma \models C \equiv D$.
4. **Disjonction** : deux concepts C et D sont disjoints par rapport à Γ si $C^J \cap D^J = \phi$ pour chaque *modèle* J de Γ.

Annexe B

Modélisation Ontologique

Nous avons choisi d'utiliser OWL (Web Language Ontology) pour la conception de notre modèle. OWL grâce à son formalisme logique basé sur les logiques de descriptions offre une grande expressivité de représentation des connaissances.

B.1 Ontologies et OWL

Les ontologies se basent sur RDFs et OWL qui sont deux langages principaux pour exprimer des ontologies permettant de définir des vocabulaires RDF. Ce dernier est simple, d'une expressivité réduite et il permet de réaliser des inférences simples. OWL est la dernière norme du W3C. C'est un langage expressif permettant de réaliser des inférences complexes. On utilise le logiciel Protégé pour définir des ontologies de domaines spécialisés et on utilise au maximum les ontologies existantes et reconnues, cela permet un meilleur compromis entre simplicité et expressivité.

Les classes : se sont des ressources qui peuvent être partagées en classes, on précise la classe d'une ressource avec la propriété rdf :type, on peut exprimer qu'une classe est sous-classe d'une autre qui signifie que toutes les instances de la première sont instances de la seconde.

Les propriétés : une propriété est de type rdf : Property qui est une instance de rdfs : Class, on peut exprimer qu'une propriété est sous-propriété d'une autre qui signifie que toutes les paires d'instances vérifiant la première vérifient la seconde, on peut spécifier le type du domaine (l'ensemble des valeurs de sujet possibles) et le type du co-domaine (l'ensemble des valeurs d'objets possibles).

Les individus se sont des instances des classes définies.

Un modèle est évolutif est un domaine où on peut toujours ajouter de nouvelles classes, propriétés et relations entre elles car le Web sémantique est évolutif.

B.1.1 Création des classes

La figure B.1.1 illustre l'ajout d'une nouvelle classe.

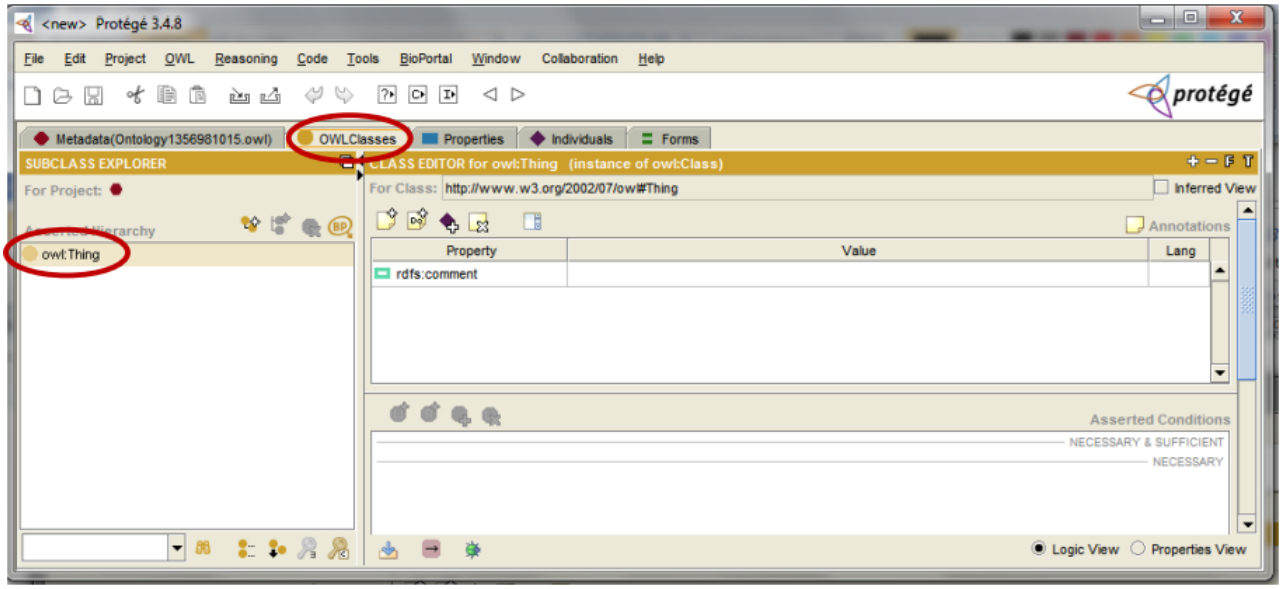

FIGURE B.1.1 – Ajout de classes.

B.1.2 Création des propriétés

La figure B.1.2 illustre l'ajout d'une propriété et elle sert à mettre un lien entre deux classes ou sous classes.

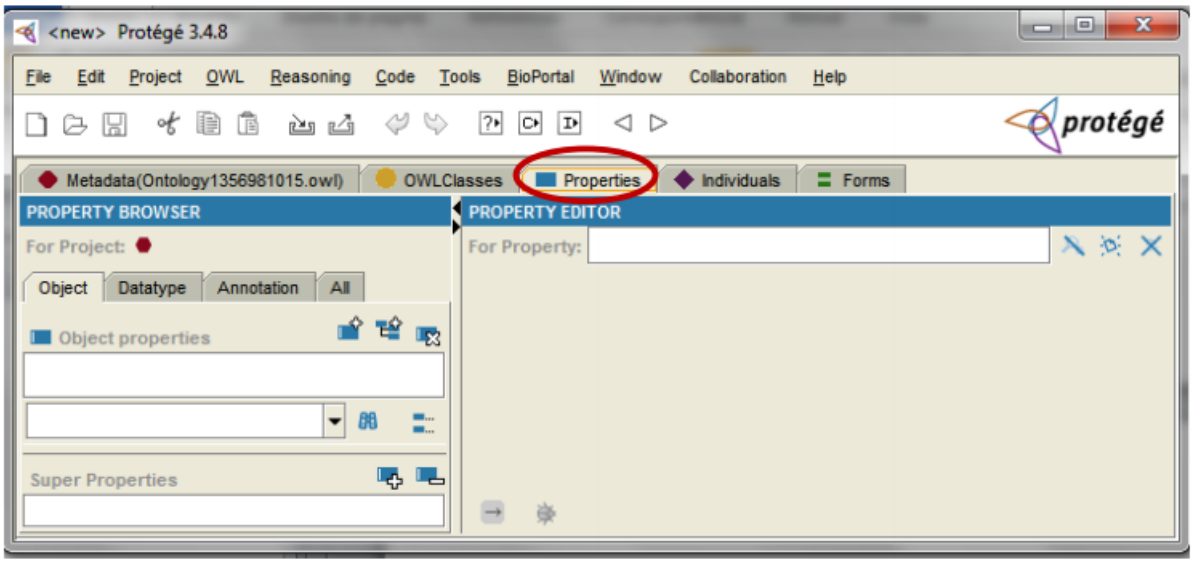

FIGURE B.1.2 – Ajout de propriétés.

B.1.3 Création des instances ou individus

LA figure B.1.3 illustre l'instanciation des individus.

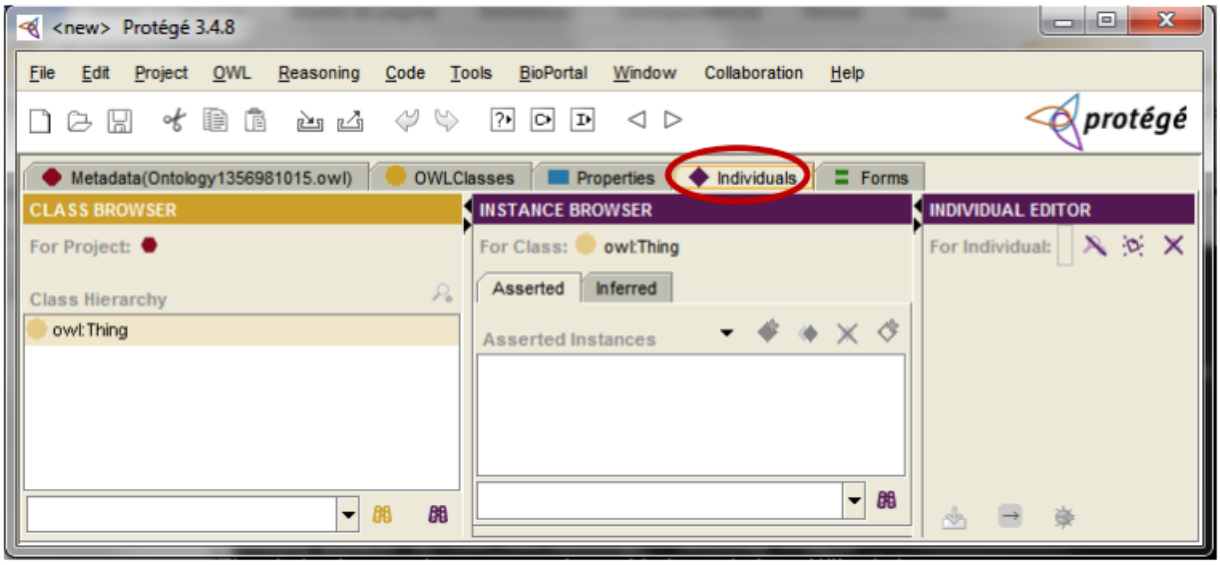

FIGURE B.1.3 – Insertion d'individus.

B.1.4 Modèle ontologique

La figure B.1.4 illustre l'ontologie conçue avec les classes, les propriétés et les individus.

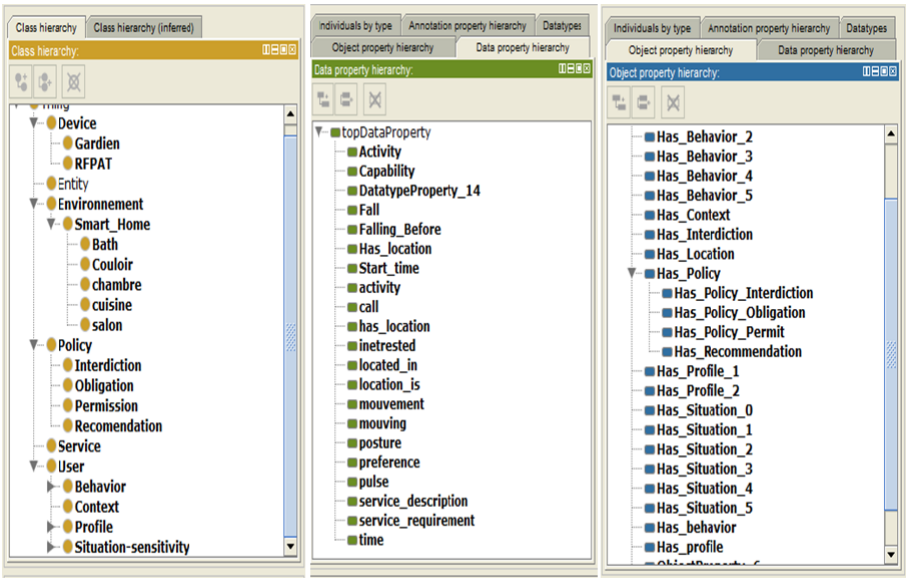

FIGURE B.1.4 – Modèle ontologique

Annexe C

Raisonnement Ontologique

La compréhension et l'utilisation des informations et connaissances représentées dans un langage appartenant aux technologies du web sémantique, leur exploitation exige d'avoir un moteur d'inférence (raisonneur) afin de dériver de nouveaux faits ou connaissances à partir des informations existantes.

C.1 Ontologie et SWRL

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

C.2 SWRL Jess Tab

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

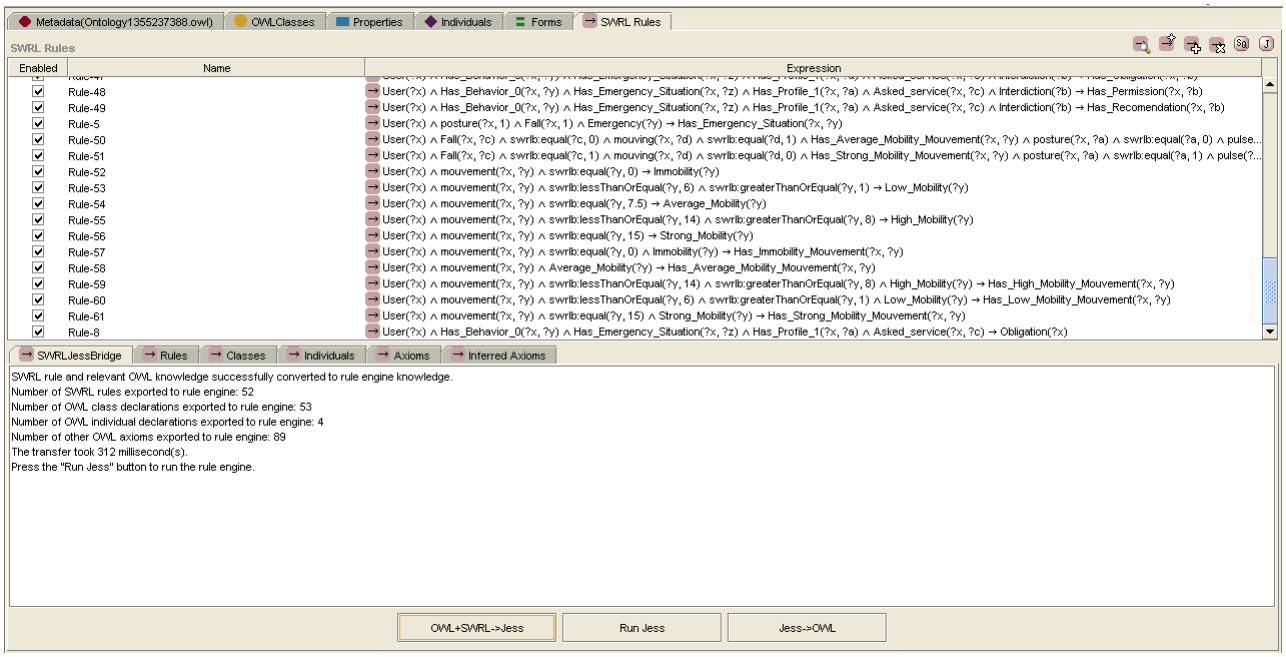

FIGURE C.2.1 – Transformation des faits et des règles SWRL sous Jess.

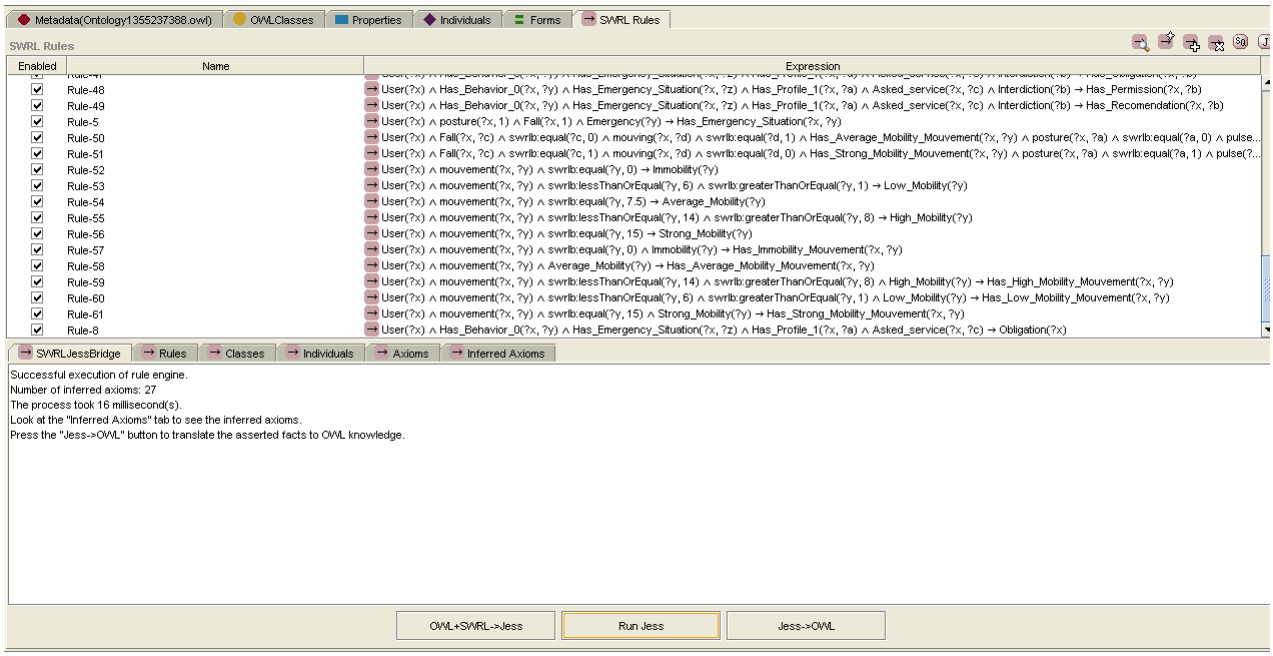

FIGURE C.2.2 – Activation de Jess.

Annexe D

Querying Ontologique

Dans le cadre des travaux de cette thèse, nous avons conçu une ontologie (UBC-ACM) décrivant l'utilisateur et son environnement pour permettre une bonne gestion de ses accès aux services. Cette ontologie est exploitée par le biais du protocole SPARQL pour récupérer les décisions d'accès après avoir établi le processus de modélisation et raisonnement dont les nouvelles connaissances sont stockées dans la base de données. Le querying est implémenté au moyen des outils Protégé et Jena sous Eclipse. Il est possible de faire passer des requêtes de type SQWRL sous Protégé permettant d'intérroger l'ontologie de manière à y détecter anomalies et informations manquantes.

D.1 Ontologie et SPARQL

SPARQL « Simple Protocol And Rdf Query Language » est un protocole de requêtes et un langage de requêtes de bases de données. SPARQL est le langage standardisé d'interrogation de graphes rdf, comme SQL qui est le langage d'interrogation de bases de données relationnelles. Alors que SQL est basé sur la notion de calcul relationnel et les requêtes sont exprimées dans un langage logique de description du résultat : les champs sélectionnés, les jointures, les filtrages, les groupes et les opérations de groupe, le langage SPARQL est basé sur la notion de graphes de triplets et les requêtes sont décrites par des motifs (patterns) et des variables.

Le langage permet d'interroger des descriptions RDF en utilisant des clauses (similaires dans certains cas à celles du langage SQL) telles que PREFIX (spécifie l'adresse exploitée dans la construction de la requête), SELECT ... [FROM] ... WHERE (requête interrogative), CONSTRUCT (requête constructive), UNION, OPTIONNAL (jointures, conditions optionnelles), FILTER (conditions obligatoires).

La figure D.1.1 illustre la position du protocole SPARQL dans le framework du Web sémantique.

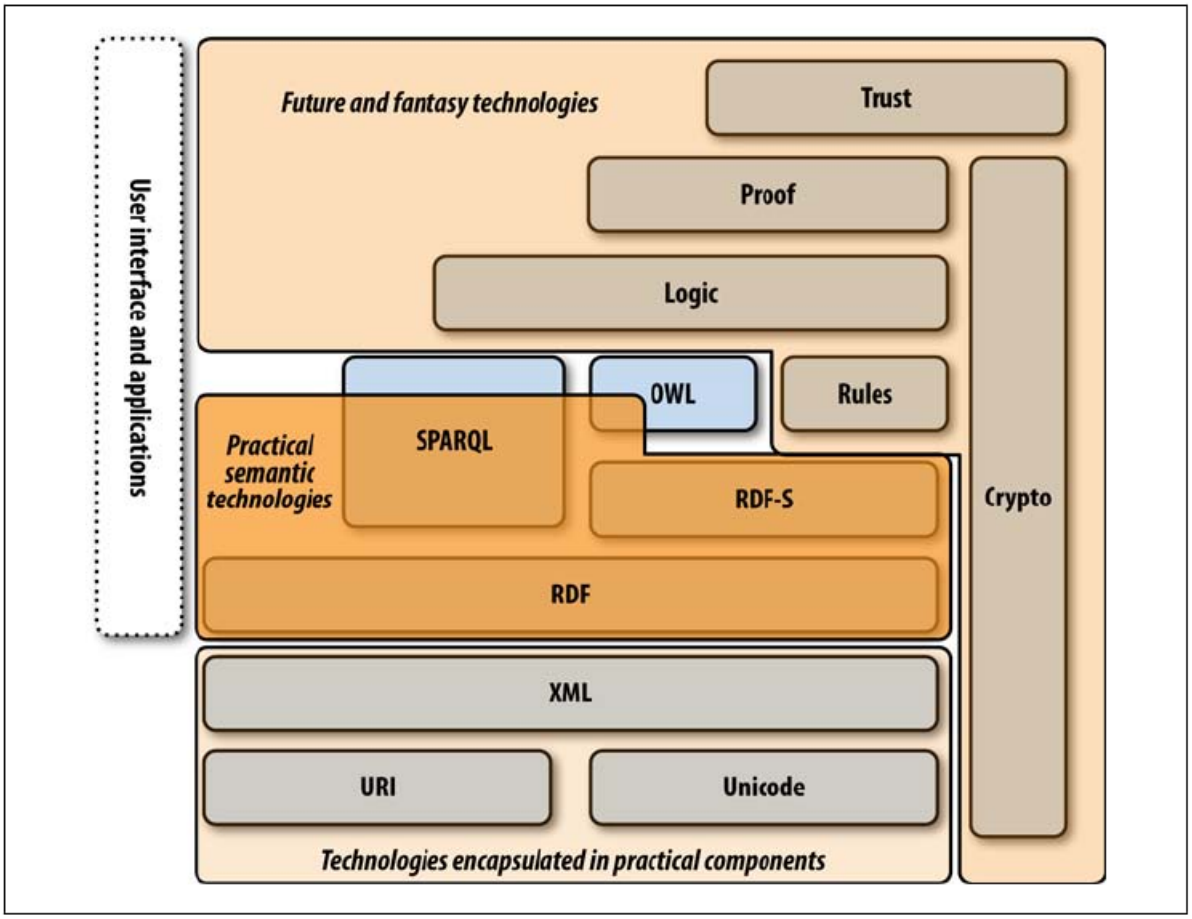

FIGURE D.1.1 – Position du protocole SPARQL.

D.1.1 Forme générale d'une requête SPARQL

Trois requêtes principales : SELECT pour interroger, CONSTRUCT pour ajouter de nouveaux triplets, et ASK pour tester une propriété.

BASE prex :<namespace-uri >
PREFIX prex :<namespace-uri >
SELECT variable-list
FROM source-list
WHERE pattern

On distingue deux parties principales dans une requête SPARQL :
Entête constitué de Base, Prefixe, Select, Construct, Ask.
Corps constitué de From, Where.

D.2 Ontologie et SQWRL

On peut passer des requêtes de type SQWRL comme illustré dans la figure D.2.1. On clique sur le bouton SQ pour que l'onglet SQWRQueryTab soit affiché et ensuite on clique sur « Run » pour exécuter la requête.

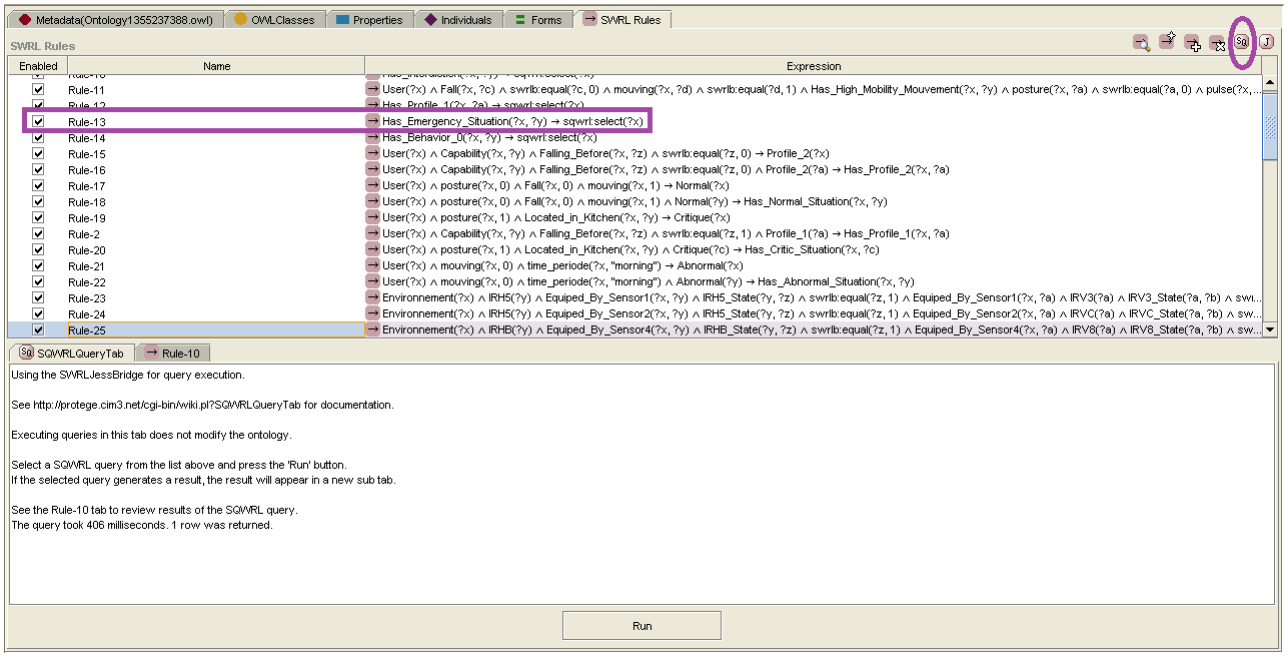

FIGURE D.2.1 – Requête de type SWRL.

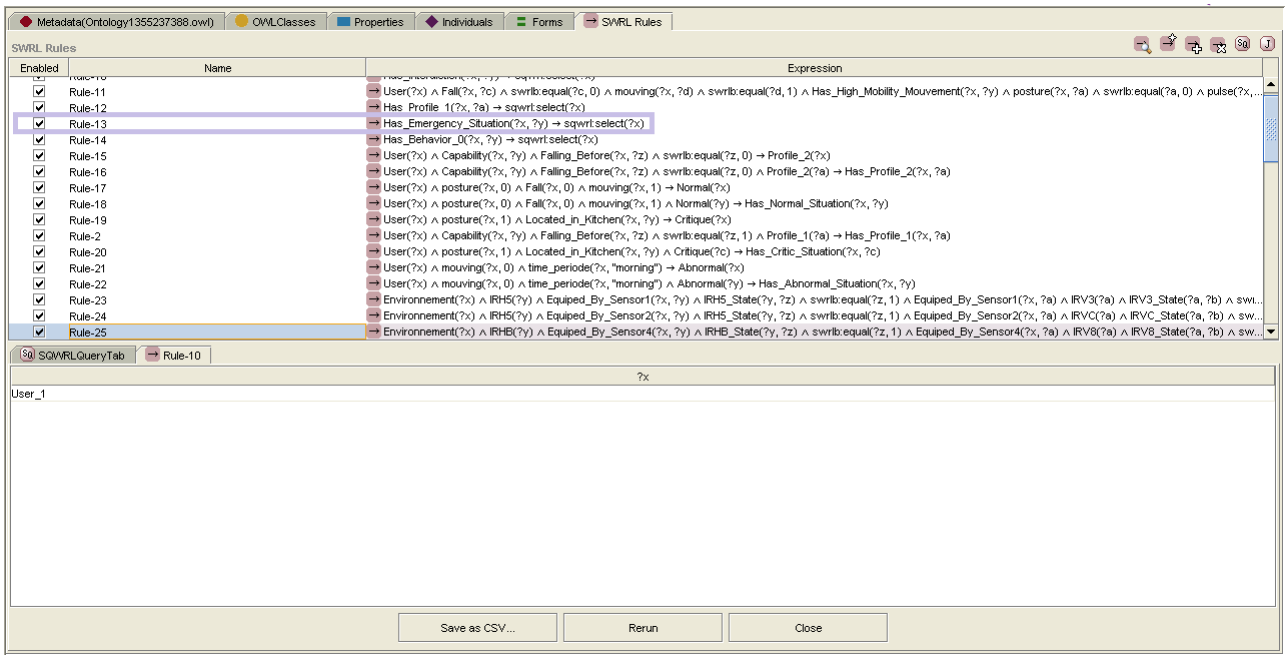

FIGURE D.2.2 – Réponse de la requête.

La figure D.2.2 illustre la réponse de la requête exécutée.

Références

[**Abburu 2012**] Abburu, S. : A Survey on Ontology Reasoners and Comparison. In International Journal of Computer Applications, Volume 57, N° 17, pp.33-39, 2012.

[**Abou El Kalam et al. 2006**] Abou El Kalam, A., Deswarte, Y. : Multi-OrBAC : A New Access Control Model for Distributed, Heterogeneous and collaborative systems. In IEEE Symp. on Systems and Information Security, Sao Paulo, Brazil, 2006.

[**Abou El Kalam et al. 2009**] Abou El Kalam, A., Deswarte, Y., Kaaniche, B A M. : PolyOrBAC : a Framework for Critical Infrastructure Security, In International Journal on Critical Infrastructure Protection, Elsevier, Report LAAS N° 09087, 28 pages, Mars 2009

[**Abowd et al. 1999**] Abowd, D-A.K., Dey, A K., Brown, P J., Davies, N., Smith, M., Steggles,P. : Towards a Better Understanding of Context and Context-Awareness. In HUC '99 Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing, pp. 304-307, 1999.

[**Almulhem 2008**] Almulhem, A., Security Policies, Computer Engineering Department, KFUPM (2008)

[**Al Kukhun et al. 2007**] Al Kukhun, D., Sedes, F. : Steps Towards Pervasive Software : Does Software Engineering Need Reengineering ?, pp 143-150, 2007.

[**AL Kukhun 2012**] AL Kukhun, D., :Steps towards adaptive situation and context-aware access : A contribution to the extension of access control mechanisms within Pervasive Information Systems. Rapport de thèse de doctorat, Institut de Recherche en Informatique de Toulouse, France, Novembre 2012.

[**Aloulou 2013**] Aloulou, H. : Plateforme pour l'Assistance à l'Autonomie à Domicile : Gestion de la Dynamique et de l'Incertitude pour la Fourniture Sémantique en Temps Réel de Services d'Assistance. Thèse de doctorat. Evry, Institut national des télécommunications, Paris, Juin 2013.

[**Amini 2010**] Amini, M., : Normative Logic Based Semantic-Aware Authorization Model. Rapport de thèse de doctorat. Sharif University of Technology, Téhéran, Iran, Janvier 2010.

[**Ark et al. 1999**] Ark, W. S., Selker, T. : A look at human interaction with pervasive computers. IBM Systems Journal 38, pp. 504–507, 1999.

[**Asmidar et al. 2009**] Asmidar, A,. Roslan, I., Jamilin, J. : A Review on Extended Role Based Access Control (E-RBAC) Model in Pervasive Computing Environment. In Networked Digital Technologies, 2009. NDT '09. First International Conference on, IEEE, pp. 533-535, 2009.

[**Apprentissage_Wiki 2015**] `http://www.cs.waikato.ac.nz/ml/weka/`, Dernier accès : 25/05/2015.

[**Auth 2015**] `http://fr.wikipedia.org/wiki/Authentification` Dernier accès : 31/03/2015.

[**Amara-Hachimi et al. 2006**] Amara-Hachimi, N., and El Fallah-Seghrouchni A., Modélisation d'informations contextuelles pour des agents mobiles sensibles au contexte. NOTERE'06 : nouvelles technologies de la répartition : 6eme

Conférence internationale sur les nouvelles technologies de la répartition, Toulouse, France, 2006.

[**Augusto 2008**] Augusto, J-C., :Ambient Intelligence : Concepts and Applications. In Software and Data Technologies Communications in Computer and Information Science Volume 10, pp 16-26, 2008.

[**Autonomie et dépendance 2009**] Autonomie et dépendance, Support de Cours, Université Médicale Virtuelle Francophone, 2008-2009, `http://campus.cerimes.fr/geriatrie/enseignement/geriatrie8/site/html/cours.pdf`

[**Bonino et al. 2010**] Bonino, D., Corno, F. : Rule-based intelligence for domotic environments. Automation in Construction Volume 19, Issue 2, pp. 183-196, Mars 2010.

[**Baldauf et al. 2007**] Baldauf, M., Dustdar, S., Rosenberg, F. : A Survey on Context-Aware Systems. International Journal of Ad Hoc and Ubiquitous Computing, Volume 2, N° 4, pp. 263–277, Juin 2007.

[**Bettini et al. 2010**] Bettini, C., Brdiczka, O., Henricksenc, K., Indulskad, J., Nicklase, D., Ranganathanf, A., Ribonia, D. : A survey of context modelling and reasoning techniques. In Pervasive and Mobile Computing Volume 6, Issue 2, pp. 161–180, Avril 2010.

[**Balbo et al. 2009**] Balbo, F., Tarpin, C., Uster, G., Seidowsky, R. : Comment l'intelligence ambiante peut-elle contribuer aux transports intelligents ?. Colloque, Objets nomades et mobilité intelligente, Paris, France, 2009

[**Bick et al 2008**] Bick, M., Kummer, T.-F. : Ambient Intelligence and Ubiquitous Computing. In Handbook on Information Technologies for Education and Training, Publié par Springer pp. 79-100, Heidelberg, Berlin, 2008.

[**Bock et al. 2008**] Bock, J., Haase, P., Ji, Q., Volz, R. : Benchmarking OWL Reasoners. In ARea2008 - Workshop on Advancing Reasoning on the Web : Scalability and Commonsense, Juin 2008.

[**Baader et al. 2003**] Baader, F., Calvanese, D., McGuinness, D.L., Nardi, D., Patel-Schneider, P.F. : The description logic handbook : theory, implementation, and applications, Cambridge University Press, 2003.

[**Brown et al. 1997**] Brown, P.J., Bovey, J.D., Chen, X. : Context-aware applications : From the Laboratory to the Marketplace. In IEEE Personal Communications, Volume 4, N 5, pp. 58-64, 1997.

[**Bertino et al. 2000**] Bertino, E., Bonatti, P A., Ferrari, E., TRBAC : a temporal role-based access control model. In Proceedings of the 5th ACM Workshop on Role-Based Access Control, pp. 21–30, Berlin, Allemagne, Juillet 2000.

[**Bertino et al. 2005**] Bertino, E., Catania, B., Damiani, M. L., Perlasca, P., : GEO-RBAC : A Spatially Aware RBAC. In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies, Stockholm, Sweden, pp. 29-37, 2005.

[**Bacon et al. 2005**] Bacon, J., Moody, K., Yao, W., : A model of OASIS role based access control and its support for active security. ACM Transactions on Information and System Security (TISSEC), Volume 5, N° 4, pp. 492–540,

2002.

[**Cheaito 2012**] Cheaito, M. :Un cadre de spécification et de déploiement de politiques d'autorisation. Thèse de doctorat, Université de Toulouse III, 2012.

[**Culnan 2000**] Culnan, M. J. : Protecting Privacy Online : Is Self-Regulation Working ? ournal of Public Policy & Marketing : Spring, Volume 19, N° 1, pp. 20-26, 2000.

[**Cuppens et al. 2003**] Cuppens, F., Miege, A., : Modelling contexts in the OrBAC model. In 19th annual Computer Security Applications Conference, pp. 416–425, 2003.

[**Chen et al. 2008**] Chen, L., Crampton, J., : On Spatio-Temporal Constraints and Inheritance in Role-Based Access Control. In Proceedings of the ACM Symposium on Information, Computer and Communications Security, pp. 205-216, 2008 .

[**Chen et al. 2004**] Chen, H., Finin, T., Joshi, A. : A Context Broker for Building Smart Meeting Rooms. Proceedings of the Knowledge Representation and Ontology for Autonomous Systems Symposium, pp. 53-60, Stanford, California, Mars 2004.

[**Chana et al. 2009**] Chana, M., Campoa, E., Estève, D., Fourniols, J-Y. : Smart homes — Current features and future perspectives. In Maturitas, Volume 64, Issue 2, pp. 90–97, Octobre 2009.

[**Cavalcante 2012**] Cavalcante, P, Réseaux Évidentiels pour la fusion de données multimodales hétérogènes : application à la détection de chutes", Institut Mines Télécom SudParis, 2012 (Rapport de thèse) .

[**Chen et al. 2004**] Chen H., Finin, T., Joshi A. :An Ontology for Context Aware Pervasive Computing Environnements. In Special Issue on Ontologies for Distributed Systems, Knowledge Engineering Review, Volume 18, N° 3, pp. 197–207, 2004.

[**Carroll et al. 2004**] Carroll, J., Dickinson, I., Dollin, C., Reynolds, D., Seaborne, A., Wilkinson, K. : Jena : implementing the semantic web recommendations. In WWW Alt. '04 Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters, pp. 74-83, 2004.

[**Chahuara Quispe 2013**] Chahuara Quispe, P. : Contrôle intelligent de la domotique à partir d'informations temporelles multisources imprécises et incertaines. Thèse de doctorat, Laboratoire d'Informatique de Grenoble, 2013.

[**Charlet et al. 2004**] Charlet, J., Bachimont, B., Troncy. R. : Ontologies pour le Web sémantique. In Information – Interaction – Intelligence Hors Série 2004.

[**Coutaz et al. 2005**] Coutaz, J., James, L., Crowley, Dobson, S., Garlan, D. : Context is key. In Communications of the ACM - The disappearing computer, Volume 48, Issue 3, pp. 49-53, NY, USA, Mars 2005.

[**Chaari 2007**] Chaari T. : Adaptation d'applications pervasives dans des environnements multicontextes. Thèse de doctorat, Institut National des Sciences Appliquées, Lyon, France, 2007.

[**Cook et al. 2007**] Cook, D-J., Augusto, J-C., Jakkula, V-R. : Ambient

intelligence : Technologies, applications, and opportunities. 2007.

[**Dey 2000**] Dey A, Understanding and using context. Journal of Personal and Ubiquitous Computing, volume 5 numéro 1, pp 4–7, 2000.

[**Dibitonto 2012**] Dibitonto, M. : New Challenges in HCI : Ambient Intelligence for Human Performance Improvement. Thèse de doctorat, université de Cagliari, Italy, Mars 2012

[**Dafa-Alla et al. 2005**] Dafa-Alla, A-F., Kim, E-H., Ryu, K-H., Heo, Y-J., : PRBAC : an extended role based access control for privacy preserving data mining. Computer and Information Science, 2005. Fourth Annual ACIS International Conference on. pp. 68-73, Juillet 2005.

[**Dictionary 2015**] Dictionary.com LLC, "Thesaurus.com," .
`http://thesaurus.com/`, Dernier accès : 19/05/2015.

[**Friedewald et al. 2011**] Friedewald, M., Raabe, O., : Ubiquitous computing : An overview of technology impacts. Journal Telematics and Informatics, Volume 28, Issue 2, pp. 55-65, NY, USA, Mai 2011.

[**Foldoc 2015**] Foldoc.org, "Free on-line dictionary of computing", `http://foldoc.org/context`, Dernier accès : 19/05/2015.

[**Ferraiolo et al. 2001**] Ferraiolo, D., Sandhu, RS., Gavrila, S., Kuhn, D., Chan-dramouli, R. : A proposed standard for role-based access control. In ACM Transactions on Information and System Security Volume 4, N° 3, pp.224-274, 2001.

[**Finin et al. 2008**] Finin, T., Joshi, A., Kagal Massachusetts, L., Niu, J., Sandhu, R., Winsborough, W., Thuraisingham, B. : ROWLBAC - Representing Role Based Access Control in OWL. In SACMAT'08 Proceedings of the 13th ACM symposium on Access control models and technologies, pp. 73-82, 2008.

[**Favela 2012**] Favela, J. : Activity, Behavior and Context : The ABC of Pervasive Healthcare Research. In Workshop Proceedings of the 8th International Conference on Intelligent Environments, Volume 13, pp. 4-13, 2012.

[**Fortineau et al. 2012**] Fortineau, V., Paviot, T., Louis-Sidney, L., Lamouri, S. : SWRL as a rule language for ontology-based models in power plant design. Dans le livre : Product Lifecycle Management : Towards Knowledge-Rich Enterprises, pp. 588-597, 2012.

[**Gallissot 2012**] Gallissot, M., :Modéliser le concept de confort dans l'habitat intelligent : du multisensoriel au comportement. Thèse de doctorat, Université de Grenoble, France, Avril 2012.

[**Gambetta 2000**] Gambetta, D. Can We Trust Trust ? Deptement of Sociology, University of Oxford, , chapter 13, pp. 213–237, 2000.

[**Grandison et al. 2000**] T. Grandison and M. Sloman. A Survey of Trust in Internet Applications. In Journal IEEE Communications Surveys & Tutorials archive, Volume 3, Issue 4, pp. 2-16, Octobre 2000. [**Gross et al. 2003**] Gross, T., Klemke, R. : Context Modelling for Information Retrieval - Requirements and Approaches. In IADIS International Journal on WWW/Internet 6, No.1, pp.29-42, 2003.

[**Gray et al. 2001**] Gray, P., Salber, D. : Modelling and Using Sensed Context Information in the Design of Interactive Applications. In Engineering for Human-Computer Interaction, Volume 2254, pp. 317-335, 2001.

[**Giri et al. 2013**] Giri, N., Zope, V. : Personalized Ontology Based Context Aware Recommender System. International Journal of Advanced Computational Engineering and Networking, Volume 1, Issue 6, pp. 4-10, Aout 2013.

[**Gu et al. 2004**] Gu, T., Pung, H. K., Zhang, D. Q. : A Middleware for Building Context-Aware Mobile Services. IEEE Vehicular Technology Conference (VTC-Spring 2004), Volume 5, pp. 2656 - 2660, Milan, Italy, 2004.

[**Giudicelli 2011**] Giudicelli, V., :Ontologies Langage OWL. Université Montpellier 1, Laboratoire d'ImmunoGénétique Moléculaire (LIGM), 2011.

[**Garlatti et al. 2004**] Garlatti, S., Prié, Y. : Adaptation et personnalisation dans le Web sémantique. In Revue I3 Information-Interaction - Intelligence, Numéro Hors-série Web sémantique, pp. 24 , 2004.

[**Gruber 1993**] Gruber.T. R., A Translation Approach to Portable Ontologies. Knowledge Acquisition, 5(2) :199–220, 1993.

[**Hansmann et al. 2001**] Hansmann, U., Merk, L., Nicklous, M., Stober, T. : Pervasive Computing Handbook. Berlin Heidelberg New York : Springer, 2001.

[**Henricksen et al. 2002**] Henricksen, K., Indulska, J. : Modelling and Using Imperfect Context Information. Workshop Proceedings of the 2nd IEEE Conference on Pervasive Computing and Communications, Edition F. Mattern and M. Naghshineh, Springer, pp. 167–180, Zurich, Switzerland, 2002.

[**Hofer et al. 2002**] Hofer T., Schwinger W., Pichler M., Leonhartsberger G., Altmann J., "ContextAwareness on Mobile Devices – the Hydrogen Approach", Proceedings of the 36th Annual Hawaii International Conference on System Sciences, pp 292–302, Hawaii 2002.

[**Hu et al. 2013**] Hu, B., Wang, Z-X., Dong, Q-C. : A Novel Context-aware Modeling and Reasoning Method based on OWL. Journal of Computers, Volume 8, N° 4, pp. 943-950, 2013.

[**handicap 2015**] Définition du handicap : `http://www.handicap-info.fr/definition-du-handicap/`, Dernier accès : 23/05/2015.

[**Jess 2015**] `http://www.jessrules.com/jess/`
Dernier accès : 03/06/2015.

[**Kofod-Petersen 2007**] Kofod-Petersen, A. : A Case-Based Approach to Realising Ambient Intelligence among Agents. Thèse de doctorat, Department of Computer and Information Sciences, Norwegian University of Science and Technology, 2007.

[**Krumm 2009**] Krumm, J., : Ubiquitous Computing Fundamentals. Edité par Chapman and Hall/CRC. Première édition, 2009.

[**Kumar et al. 2002**] Kumar, A., Karnik, N., Chafle, G., : Context sensitivity in role-based access control. Operating systems review, Volume 36, N° 3, pp. 53–66, 2002.

[**Kim et al. 2005**] Kim, Y-G., Mon, C-J., Jeong, D., Lee, J-O., Song,

C-Y., Baik, D-K., : Context-aware access control mechanism for ubiquitous applications. Journal Advances in Web Intelligence, Volume. 3528, pp. 236–242, 2005.

[**Kobsa 2001**] Kobsa,A. : User Modeling and User-Adapted Interaction.In User modeling and user-adapted interaction, Volume 11, N° 1-2, pp. 49-63, Mars 2001.

[**Kobsa 1993**] Kobsa, A. : User Modeling : Recent Work, Prospects and Hazards, 1993.

[**Kadouche 2007**] Kadouche, R. : "Modélisation du profil utilisateur et personnalisation dans les espaces de vie intelligents", Institut Mines Télécom SudParis, 2007 (Rapport de thèse).

[**k-means 2015**] `http://fr.wikipedia.org/wiki/K-moyennes`, Dernier accès : 25/05/2015.

[**Kadouche et al. 2008**] Kadouche, R., Mokhtari, M., Giroux, S., Abdulrazak, B. : Semantic approach for modelling an assistive environment using description logic. In iiWAS '08 Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services, pp. 222–231, 2008.

[**Longman 2015**] Longman dictionary of contemporary english advanced learner's dictionary. `http://www.ldoceonline.com/dictionary/context`, Dernier accès : 19/05/2015.

[**Li et al. 2008**] Li, X., Yoo, S-B., : Extended Role-Based Security System using Context Information. Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on, Volume 2, pp. 7-12, Décembre 2008.

[**Le Duc 2004**] Le Duc, C. : Transformation d'Ontologies basées sur la Logique de Description Application dans le Commerce Electronique. Thèse de doctorat. Laboratoire d'Informatique, Signaux, et Systèmes de Sophia Antipolis. France, 2004.

[**Mayrhofer et al. 2004**] Mayrhofer, R., Radi, H., Ferscha, A. : Recognizing and predicting context by learning from user behavior. In Radiomatics : journal of Communication Engineering, special issue on Advances in Mobile Multimedia, Volume 1, N°1, pp. 30–42, 2004.

[**Medjahed 2010**] Medjahed, H. "Distress situation identification by multimodal data fusion for home healthcare tele monitoring", Institut Mines Télécom - Télécom SudParis, 2010, (Rapport de thèse).

[**Miraoui et al. 2008**] Miraoui, M., Tadj, C., Amar, C.B. : Context Modeling and Context-Aware Service Adaptation for Pervasive Computing Systems. International Journal of Computer and Information Science and Engineering, Volume 2, N° 3, pp. 148-157,2008.

[**Miraoui 2009**] Miraoui, M. : Architecture logiciel pour l'informatique diffuse : Modélisation du contexte et adaptation dynamique des services. Thèse de doctorat, Montréal, Canada, 2009.

[**Mcheick et al. 2014**] Mcheick, H., Sbeity, H., Hazimeh, H., Naim, J.,

Alameh, M. : Context Aware Mobile Application Architecture (CAMAA) for Health Care Systems - Standardization and abstraction of context aware layers. IEEE Canada International Humanitarian Technology Conference (IHTC), Montreal, Canada, 2014.

[**Miège 2005**] Miège, A. : Definition of a Formal Framework for Specifying Security Policies : The Or-BAC Model and Extensions. Thèse de doctorat, Computer Security, ENST - INFRES Computers and Networks, ENST, 2005.

[**M'hamed et al. 2013**] M'hamed, A., Zerkouk, M., El Husseini, A., Messabih., B., El Hassan, B., Towards a Context Aware Modeling of Trust and Access Control Based on the User Behavior and Capabilities, in Proc ICOST 2013, LNCS 7910, pp. 69–76, 2013.

[**Najar 2014**] Najar, S. : Adaptation des services sensibles au contexte selon une approche intentionnelle. Thèse de doctorat, Université Panthéon-Sorbonne - Paris I, France, 2014.

[**Nathiya et al. 2010**] Nathiya, G., Punitha, S. C., Punithavalli, M. : An Analytical Study on Behavior of Clusters Using K Means, EM and KMeans Algorithm. In International Journal of Computer Science and Information Security, Volume 7, N° 3, pp. 185-190, Mars 2010.

[**Nixon et al. 2004**] Nixon, P A., Wagealla, W., English, C., Terzis, S., : Security, Privacy and Trust Issues in Smart Environments. University of Strathclyde, Glasgow, Scotland, 2004.

[**Noorollahi Ravari et al 2008**] Noorollahi Ravari, A, Amini, M., Jalili, R. : A Temporal Semantic-Based Access Control Model. In 13th International CSI Computer Conference, CSICC 2008 Kish Island, Iran, Mars 2008

[**Nurmi et al. 2004**] Nurmi, P., Floréen, P. : Reasoning in context-aware systems. Article présenté à Helsinki Institute for Information Technology (HIIT), 2004.

[**OMS 2015**] OMS : http ://www.who.int/fr/ Dernier accès : 23/05/2015.

[**Onto_OWL 2015**] Tutoriel pour construire une ontologie OWL en Protégé 3.4.8 (Ontologie des Pizzas)
`http://python.espe-bretagne.fr/master-hst-ue9-2/wp-content/uploads/2013/03/Tutoriel-Pizza-gloria-1.pdf`

Dernier accès : 03/06/2015.

[**PAD 2015**] Personnes âgées dépendantes : Annuaire France : `http://www.le-guide-sante.org/Annuaire/Geriatres/Personnes-agees-dependantes.html`, Dernier accès : 23/05/2015.

[**Paganelli et al 2007**] Paganelli, F., Giuli, D. : An ontology-based context model for home health monitoring and alerting in chronic patient care networks. In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Volume 2, pp. 838–845, 2007.

[**Park et al. 2006**] Park, S., Han, Y., Chung, T., : Context-role based access control for context-aware application. High Performance Computing and Com-

munications, Volume 4208, pp. 572-580, Berlin/Heidelberg, Septembre 2006.

[**Pellet 2015**] http://clarkparsia.com/pellet/
Dernier accès : 03/06/2015.

[**Pellier 2015**] Pellier, D. : Introduction à l'intelligence artificielle et à la robotique (Douzième partie). Deptement Informatique, UPMF, 374-415, 2015

[**Perera et al. 2014**] Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. Context Aware Computing for The Internet of Things : A Survey. Communications Surveys & Tutorials, IEEE, Volume 16, Issue 1, pp. 414 - 454, Février 2014.

[**Perttunen et al. 2009**] Perttunen, M., Riekki, J., Lassila, O. : Context Representation and Reasoning in Pervasive Computing : a Review. In International Journal of Multimedia and Ubiquitous Engineering, pp. 1-28, 2009

[**Protégé 2015**] http://protege.stanford.edu/
Dernier accès : 03/06/2015.

[**Rashidi et al. 2013**] Rashidi, P., Mihailidis, A. : A Survey on Ambient-Assisted Living Tools for Older Adults (AAL). In Biomedical and Health Informatics, IEEE Journal of, Volume 17 , Issue 3, pp. 579 - 590, Mai 2013.

[**Reignier 2010**] Reignier, P., : Intelligence Ambiante Pro-Active : de la Specification a l'Implementation. Thèse HDR, INRIA Grenoble Rhône-Alpes / LIG Laboratoire d'Informatique de Grenoble - PRIMA, 2010.

[**Riboni et al. 2011**] Riboni, D., Bettini, C. : OWL 2 modeling and reasoning with complex human activities. Journal Pervasive and Mobile Computing archive, Volume 7 Issue 3, pp. 379-395 , Juin 2011.

[**Ronzani 2009**] Ronzani, D., : The Battle of Concepts : Ubiquitous Computing, Pervasive Computing and Ambient Intelligence in Mass Media. Ubiquitous Computing and Communication Journal., Volume 4, N° 2, Janvier 2009.

[**Rouse 2015**] Rouse, M. : Pervasive Computing (Ubiquitous Computing) Definition.
http://searchnetworking.techtarget.com/definition/pervasive-computing,

Dernier accès : 19/05/2015.

[**Ryan et al. 1997**] Ryan, N.S., Pascoe, J., Morse, D.R. : Enhanced reality fieldwork : the contextaware archeological assistant. In Computer Applications in Archeology, British Archaelogical Reports, Gaffney, Leusen and Exxon edition, Oxford, UK 1997.

[**Saha et al. 2003**] Saha, D., Mukherjee, A. : Pervasive computing : A paradigm for the 21st century. IEEE Computer, Volume 36, N° 3, pp. 25–31, Mars 2003.

[**Samarati et al. 2001**] Samarati, P., De Capitani di Vimercati, S. : Access Control : Policies, Models, and Mechanisms. In Foundations of Security Analysis and Design, Volume 2171, pp. 137-196, 2001.

[**Schilit et al. 1994**] Schilit, B., Adams, N., Want, R. :Context-aware computing applications. In Workshop on Mobile Computing Systems and Applications, pp. 85- 90, Santa Cruz, CA,1994.

[**Schmidt 2002**] Schmidt, A., : Ubiquitous Computing – Computing in Context. Thèse de Doctorat, Lancaster University, UK, 2002.

[**Sellam 2008**] Sellami, Z. : Intelligence ambiante : étude d'une approche par auto-organisation coopérative et mise en oeuvre d'une plate-forme de conception générique. Rapport de Master 2 Recherche, Université Paul Sabatier (UPS) – Toulouse III, France, 62 pages, 2008

[**Skillen et al. 2012**] Skillen, K.L., Chen, L., Nugent, C.D., Donnelly, M.P., Burns, W., Solheim, I. : Ontological User Profile Modeling for Context-Aware Application Personalization. Ubiquitous Computing and Ambient Intelligence, Volume 7656, pp 261-268, 2012.

[**Strang 2004**] Strang, T., Linnhoff-Popien, C. : A context modeling survey," In : Workshop on advanced context modelling, reasoning and management, UBICOMP 2004 - The sith international conference on ubiquitous computing, Nottingham/England, 2004.

[**Spiekermann et al. 2009**] Spiekermann, S. , Cranor, L.F. :Engineering privacy. IEEE Ttransactions on Software Engineering, Volume 35, N°1, 2009.

[**Studer et al 1998**] Studer, R., Benjamins, R., Fensel.,., Knowledge engineering : Principles and methods. Data & Knowledge Engineering, 25(1–2) :161–198, 1998.

[**Sirin et al. 2007**] Sirin, E., Parsia, B., Cuenca Grau, B., Kalyanpur, A., Katz, Y. : Pellet : A practical OWL-DL reasoner. In Journal Web Semantics : Science, Services and Agents on the World Wide Web archive, Volume 5, Issue 2, pp. 51-53, Juin 2007.

[**Shehzad et al. 2004**] Shehzad, A., Ngo, H., Pham, K., Lee, S. : Formal modeling in context aware systems. In Proceedings of the First International Workshop on Modeling and Retrieval of Context. Septembre 2004

[**Tentori et al. 2008**] Tentori, M., Favela. J. : Activity aware computing for healthcare. IEEE Pervasive Computing, Volume 7, N°2, pp. 51-57, 2008.

[**Tiberghien 2013**] Tiberghien, T., : Strategies pour le raisonnement sur le contexte dans les environnements d'assistance pour les personnes âgees. Thèse de doctorat, Institut national des télécommunications, Paris, Novembre 2013.

[**Tigli et al. 2009**] Tigli, J-Y., Lavirotte, S., Rey, G., Hourdin, V., Riveill, M., : Context-aware Authorization in Highly Dynamic Environments. IJCSI International Journal of Computer Science Issues, Volume 4, N° 1, pp. 24-35, 2009.

[**Toahchoodee et al. 2009**] Toahchoodee, M., Abdunabi, R., Ray, I., Ray, I., :A Trust-Based Access Control Model for Pervasive Computing Applications. Journal Data and Applications Security XXIII, Volume 5645, pp. 307-314, 2009.

[**Toninelli 2006**] Toninelli, A., A semantic context-aware access control framework for secure collaborations in pervasive computing environments. In

ISWC '06 : Fifth International Semantic Web Conference, pp. 473-486, 2006.

[**Topcu 2011**] Topcu, F. : Context Modeling and Reasoning Techniques. Technical University of Berlin, At SNET Seminar Expert Talks, 2011.

[**Vieillissement 2015**] Comprendre le vieillissement : `http://www.info-seniors.com/info-article/2/30/181/comprendre-le-vieillissement.html`, Dernier accès : 23/05/2015.

[**Vieill2015**] http ://enjeux-senior.org/2014/08/24/population-vieillissante-une-faiblesse-pour-leconomie/

[**Von et al. 2006**] Von, V., Heckmann, D. : Ubiquitous User Modeling. 2006.

[**Wang et al. 2004**] Wang, X.H., Zhang, D., Gu, T., Pung, H. : Ontology based context modeling and reasoning using owl. In Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on, pp. 18–22, 2004.

[**Wang et al. 2006**] Wang, E., Kim, Y-S. : A Teaching Strategies Engine Using Translation from SWRL to Jess. Intelligent Tutoring Systems, Volume 4053, pp. 51-60, 2006.

[**Wang 2014**] Wang, X., Dong, J S., Chin, C Y., Hettiarachchi, S R., Zhang, D. : Semantic Space : An Infrastructure for Smart Spaces. In Pervasive Computing, IEEE, Volume 3, Issue 3, pp. 32 - 39, 2014.

[**Weiser 1993**] Weiser, M. : Hot topics : Ubiquitous computing. IEEE Computer, Volume 26, numéro 10, pp. 71–72, 1993.

[**Weiser et al. 1997**] Weiser, M., Brown, J.S. : The coming age of calm technology. Denning P. J. and Metcalfe R. M., Eds., Beyond Calculation : The Next Fifty Years of Computing, New York, 1997.

[**Weiser 1999**] Weiser, M., : The computer for the twenty-first century. ACM SIGMOBILE Mobile Computing and Communications Review, Volume 3, Issue 3, pp. 3-11, NY, USA, Juillet1999.

[**TMD 2015**] `http://fr.wikipedia.org/wiki/T%C3%A9l%C3%A9m%C3%A9decine`

[**WS 2015**] `http://fr.wikipedia.org/wiki/Web_sémantique`
Dernier accès : 03/06/2015.

[**Wootton et al. 1999**] R., Craig J. Introduction to Telemedicine, Londres, Royal Society of Medicine Press, 1999.

[**Xu 2013**] Xu, T. : The context-aware middleware in ambient intelligence. Thèse de doctorat, LIRIS - Laboratoire d'InfoRmatique en Image et Systèmes d'information, Ecole Centrale de Lyon, 2013.

[**Zerkouk et al. 2014**] Zerkouk, M., Cavalcante, P., M'hamed, A. Boudy, J., Messabih, B. : Behavior and Capability based Access Control Model for Personalized TeleHealthCare Assistance. In Mobile Networks and Applications, Volume 19, Issue 3, pp. 392-403, Juin 2014.

[**Zhang et al. 2013**] Zhang, D., Huang, H., Lai, CF., Liang, X., Zou, Q., Guo, M. : Survey on context-awareness in ubiquitous media. Multimedia Tools and Applications. Multimedia Tools and Applications, Volume 67, N°1, pp. 179–211, 2013.