République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Mohamed El Bachir El Ibrahimi
Bordj Bou Arréridj

Faculté des Mathématiques et d'Informatique
Département d'Informatique

THÈSE DE DOCTORAT EN INFORMATIQUE

Informatique Décisionnelle et Informatique Distribuée

Soutenue publiquement Le : 11 Janvier 2023 par

Manal LAMRI

Issues applicatives de l'Internet des Objets(IoT) au bien être de l'être humain

---

Membres du jury :

Messaoud MOSTEFAI	Président	Professeur	Université Bordj Bou Arréridj
Lyazid SABRI	Directeur de thèse	MCA	Université Bordj Bou Arréridj
Khaled REZEG	Examinateur	Professeur	Université de Biskra
Samir AKROUF	Examinateur	MCA	Université de M'sila
Okba KAZAR	Examinateur	Professeur	Université de Biskra
Sofiane MAZA	Examinateur	MCA	Université Bordj Bou Arréridj

2023-2024

Remerciements

Un projet réussi, grand ou petit, est toujours réalisé grâce à notre Dieu et à l'effort d'un groupe de personnes utiles qui ont toujours donné leurs précieux conseils ou prêté main-forte. J'ai l'honneur et le plaisir d'exprimer ma gratitude et mon appréciation à tous ceux qui m'ont guidé, assisté et supervisé durant l'élaboration de cette thèse.

Je tiens à exprimer ma profonde gratitude à mon directeur de thèse, le docteur Sabri Lyazid pour son soutien continu et ses conseils tout au long de la réalisation de cette thèse et au-delà. Sa disponibilité, ses encouragements constants et sa patience ont créé une excellente relation de travail entre nous pour mener à terme ma thèse. Un grand merci encore une fois à lui de m'avoir donné l'opportunité de suivre mes recherches et de m'avoir offert les meilleures conditions pour réussir ce travail et le faire tel qu'il est aujourd'hui. Il est un leader intelligent et un guide patient.

Je tiens également à remercier les membres du jury qui ont évalué mon travail : le professeur Mostefai Messaoud, le professeur Khaled Rezeg et le professeur Okba Kazar, ainsi que le docteur Akrouf Samir et le docteur Maza Sofiane pour avoir accepté de faire partie du jury et la lecture de ma thèse.

Mes sincères remerciements vont à ma famille pour avoir toujours cru en moi. Je remercie ma mère pour sa bénédiction et son soutien infatigable tout au long de ma vie d'adulte, je n'aurais pas été ce que je suis aujourd'hui. Un merci spécial à mon grand modèle de résilience et de force, mon père qui sacrifie sa vie pour moi en continuant à m'encourager et à me motiver. Je me sens tellement bénie et reconnaissante d'avoir des parents aussi dévoués qui ont toujours exprimé à quel point ils étaient fiers de moi. Je leur serai constamment redevable, sans eux, je n'aurais rien obtenu. Enfin, je dirais à mon mari Amine Mihoub et à ma chère fille Rana Hala Jouri, vous êtes le plus important dans ma vie et vous donnez un sens à tout !.

Résumé

Aujourd'hui il est très reconnu et accepté que les technologies et les applications de l'internet des objets (IdO) et de l'internet des services (IoS) sont dans une phase de prématurité loin de toute maturité. Les défis de recherche se situent pratiquement au niveau de tous les aspects d'une solution allant des dispositifs physiques nécessaires jusqu'aux modèles satisfaisant les besoins spécifiques de l'être humain. En d'autres termes, il y a une grande fissure entre les besoins spécifiques de l'être humain et l'innovation technologique émergeante.

Dans le paradigme de l'internet des objets, plusieurs entités qui nous entourent seront interconnectées. Dans cette direction, plusieurs activités de recherche sont en train de concentrer sur les liens entre les milliers de réseaux de capteurs hétérogènes utilisant une convergence de technologies tels que, RFID (Radio Frequency Identification) qui permet à l'individu de garder trace sur tout objet sur terre et à tout moment. Dans cette recherche nous accordons un intérêt particulier à l'informatique nomadique pour investiguer son intérêt au bien être de l'être humain à l'exemple de la protection de son environnement et la bonne prise en charge de sa santé. Cette thèse met l'accent sur des modèles sémantiques de représentation des connaissances qui garantissent une description sémantique des entités dynamiques, assurent l'intégrité des connaissances et préservent la confidentialité.

Mots clés : Modèles sémantiques, Internet des Objets, intégrité des connaissances, confidentialité, sécurité.

Abstract

Today, it is widely recognized and accepted that the technologies and applications of the Internet of Things (IoT) and the Internet of Services (IoS) are far from any maturity phase. Research challenges are found practically in all aspects of a solution, ranging from the physical devices necessary to the models satisfying the specific needs of the human being. In other words, there is a big gap between the particular needs of human beings and emerging technological innovation.

In the Internet of Things paradigm, many entities around us will be interconnected. In this direction, several research activities focus on the links between the thousands of heterogeneous sensors networks using a convergence of technologies, such as RFID (Radio Frequency Identification) that allow the individual to keep track of any object on earth and at any time. In this research, we take a particular interest in nomadic computing to investigate its interest in the well-being of human beings, such as the protection of their environment and the good support of their health. This thesis focuses on semantic models of knowledge representation that guarantee a semantic description of dynamic entities, ensure knowledge integrity and preserve confidentiality.

Keywords : Semantic models, Internet of Things, knowledge integrity, confidentiality, security.

الملخص

اليوم من المعترف به والمقبول على نطاق واسع أن تقنيات وتطبيقات إنترنت الأشياء (IdO) وإنترنت الخدمات (IoS) في مرحلة سابقة لأوانها بعيدًا عن أي نضج. توجد تحديات البحث في كل جانب من جوانب الحل تقريبًا، بدءًا من الأجهزة المادية اللازمة حتى التصميمات التي تلبي احتياجات الإنسان المحددة. بعبارة أخرى هناك فجوة كبيرة بين الاحتياجات المحددة للإنسان والابتكار التكنولوجي الناشئ.

في نموذج إنترنت الأشياء ستكون أشياء كثيرة من حولنا مترابطة. في هذا الاتجاه، تركز العديد من الأنشطة البحثية على الروابط بين آلاف شبكات الاستشعار الغير المتجانسة باستخدام تقارب تقنيات RFID (تحديد الترددات الراديوية) التي تسمح للفرد بتتبع أي كائن على الأرض وفي أي وقت .في هذا البحث، نولي اهتمامًا خَاصًّا للحوسبة البدوية (l'informatique nomadique) للتحقق من اهتمامها برفاهية الإنسان، على سبيل المثال حماية بيئتها والإدارة السليمة لصحتها. تركز هذه الأطروحة على النماذج الدلالية لتمثيل المعرفة التي تضمن الوصف الدلالي للكيانات الديناميكية، وتضمن سلامة المعرفة وتحافظ على السرية.

الكلمات المفتاحية: النماذج الدلالية ، إنترنت الأشياء ، سلامة المعرفة ، السرية ، الأمن.

Table des matières

Résumé iii

Abstract iv

Liste des tableaux x

Liste des figures xi

Liste des abréviations xiv

Introduction Générale 1

1 Internet des Objets : Principes, défis, technologies 5

1.1 Internet des Objets : Principes 5

1.2 Internet des Objets : domaines d'application 8

1.2.1 Soins de santé intelligents 8

1.2.2 Maison intelligente 9

1.2.3 Systèmes de transport intelligents 9

1.3 Internet des Objets : Défis 10

1.3.1 Architecture 10

1.3.2 Évolutivité passage à l'échelle (en Anglais scalability) 11

1.3.3 Mobilité 11

1.3.4 Interopérabilité 12

1.3.5 Gestion du flux et auto-configuration 13

1.3.6 Fiabilité 13

1.3.7 Contraintes de ressources 14

1.3.8 Sécurité et Protection de la vie privée 14
1.4 Synthèse 17
1.5 Internet des Objets : Technologies associées 18
1.5.1 Blockchain 18
1.5.2 Cryptographie pour Blockchain 20
1.5.3 Blockchain & les algorithmes de consensus 21
1.6 Attribute-based access control (ABAC) 24
1.6.1 XACML : Mise en œuvre du modèle ABAC 26
1.6.2 Principaux composants de XACML 27
1.7 Conclusion 28
1.8 Contexte de la thèse 29
1.9 Notre approche 33

2 IdO pour la protection de l'environnement & le bien-être des usagers : État de l'art 35
2.1 Introduction 35
2.2 Plateformes d'authentification et de contrôle d'accès 35
2.2.1 Approches fondées sur XACML & ABAC 36
2.2.2 Approches fondées sur la technologie Blockchain . . . 43
2.2.3 Approches sémantiques pour la protection de la vie pri-vée & contrôle d'accès 46
2.3 Conclusion 54

3 Modélisation des connaissances à base d'ontologies 56
3.1 Introduction 56
3.2 Dèfinition et Rôle des ontologies 56
3.3 Web Sémantique et langages de représentation de connaissances 60
3.3.1 Modélisation des ontologies avec les langages traditionnels 61
3.3.2 L' apport du RDF(S) pour la modélisation des connaissances 63
3.3.3 Langages de modélisation de connaissances 65
3.4 Représentation des connaissances avec OWL 69

3.4.1 Modélisation des ontologies avec La Logique de Description . . . 72
3.5 Limites du langage OWL . . . 74
3.6 Règles : Alternative pour la modélisation des connaissances . 75
3.7 Moteurs d'inférences pour la Logique de Description . . . 76
3.8 Concilier OWL avec CWA & UNA . . . 77
3.9 Discussion . . . 79
3.10 Conclusion . . . 80

4 Vers une nouvelle approche sémantique pour la protection de l'environnement et le bien-être humain 82
4.1 Introduction . . . 82
4.2 Modèle sémantique pour la gestion d'accès . . . 83
4.3 Mise en correspondance entre LRS avec des politiques XACML 89
4.4 Modélisation des actions via LRS . . . 92
4.4.1 Fondement du raisonnement . . . 94
4.5 Fondement de NKRL . . . 96
4.6 Ontologie HTemp . . . 97
4.7 Représentation des évènements en NKRL . . . 99
4.8 Représentation des connaissances n-aires . . . 102
4.9 Représentation spatio-temporelle et corrélation sémantique entre évènements . . . 105
4.10 Conclusion . . . 106

5 Mise en œuvre 108
5.1 Introduction . . . 108
5.2 Plateforme sémantique pour le contrôle d'accès dans des applications Internet des Objets . . . 109
5.3 SWRL vs LRS : Différences sémantiques . . . 118
5.4 Discussion . . . 118
5.5 NKRL & Blockchain : Améliorer la protection de l'environnement et la gestion sémantique des connaissances distribuées 121
5.5.1 Hyperledger Fabric et les systèmes complexes distribués 122
5.5.2 Environnement d'exécution . . . 124
5.6 Mise en œuvre et résultats . . . 127

5.7 Conclusion 131
5.8 Publications 133

Conclusion Génaral **135**

Bibliographie **137**

Liste des tableaux

2.1 Un résumé des technologies utilisées par les différentes plateformes. *OV=Ontologie OWL 2 et ses variantes, PV=Protection de la vie privée, CS=Contrôle d'accè et x= supporter*. 53

4.1 Structure générale d'une template NKRL. 98
4.2 Structure de la template Produce. 100
4.3 Structure de la template Own. 101
4.4 Quelques exemples d'occurrences de prédicats instanciées selon le principe décrit par l'équation Eq1. 103
4.5 Autres exemples d'occurrences de prédicats. 104

Table des figures

1.1 Éléments de l'Internet des Objets et domaines d'application. Illustre l'ampleur des enjeux de l'IdO et ses effets sur l'humain. 6
1.2 Défis majeurs de l'IdO et la gestion de données pour évaluer une situation et fournir une action adéquate. 17
1.3 Arbre de Merkle. 20
1.4 Principaux composants d'une Blockchain Hyperledger Fabric. Pour des raisons de compréhension nous avons préféré garder les appellations en Anglais. 23
1.5 Modèle ABAC. 26
1.6 Diagramme de flux de données du langage XACML 3.0. . . . 27

2.1 Cadre d'analyse des politiques avec ASP, [Rezvani et al. (2019)]. 39
2.2 Le modèle Pseudonymisation et anonymisation avec XACML (PAX), [Al-Zubaidie et al. (2019)]. 41
2.3 Schéma fonctionnel du modèle de cloud hybride PRSX-AC, [Kanwal et al. (2021)]. 42
2.4 L' architecture de contrôle d'accès proposée, [Shantanu et al. (2019)]. 43

3.1 Domaine d'utilisation des ontologies. [Uschold et al. (1996)] . 57
3.2 Les langages d'ontologie traditionnels. Open Knowledge Base Connectivity (OKBC) [Chaudhri et al. (1998)] fut le premier protocole permettat d'accéder aux ontologies. 61
3.3 Évolution des langages d'ontologies, [Horrocks et al. (2000)]. 66
3.4 Les composants de base OIL, [Fensel et al. (2001)]. 67

3.5 Framework d'évaluation des différents langages de modélisation de connaissances, [Corcho et al. (2000)]. 68

4.1 cω-Model Vs OWL/RDF standard. 84

4.2 Un extrait d'ontologie de politique multi-domaines de consortium. 90

4.3 Vue d'ensemble de la taxonomie DSNO-Ontology. De plus, l'éditeur cω-Model fournit des fonctionnalités intéressantes qui importent l'ontologie OWL et se traduisent en cω-Model. La description des capteurs et des actionneurs est basée sur les concepts et les propriétés du Semantic Sensor Network (SSN) [Compton et al. (2012)]. 91

4.4 Algorithme Temporel NKRL, [Zarri (1997)]. 104

5.1 La plateforme basée sur une ontologie pour le partage des politiques de contrôle d'accès dans des environnements collaboratifs de l'Internet des objets. 109

5.2 Vue d'ensemble de la connexion de SCL en s'appuyant sur des concepts définis dans l'ontologie DSNO dédiée aux environnements collaboratifs de l'Internet des Objets. 113

5.3 Journal d'exécution du noyau de raisonnement et de la couche de communication. 114

5.4 Conception globale de l'éditeur de règles sémantiques. l'idUser, idDevice, startTime sont des paramètres d'entrées et de sorties pour les actions MoveRobot et AssistantDoctor. 116

5.5 Résultats des tests d'évolutivité. 117

119figure.caption.36

5.7 Le diagramme de séquences du scénario. 121

5.8 Vue d'ensemble des couches d'architecture de la fusion des ontologies Blockchain et NKRL. 123

5.9 Annotation des données numériques extraites du capteur en connaissances sémantiques. Cette figure illustre le processus d'annotation des données d'un capteur dans une occurrence de prédicat. Par exemple, lorsque l'utilisateur ou le système ouvre le volet, un évènement est envoyé au module Encodeur pour effectuer l'appariement avec le modèle NKRL afin de le transmettre au composant SRC. 126
5.10 Durée d'approbation de 100 transactions à partir d'un capteur. 130
5.11 Durée d'approbation de la transaction et le déclenchement de l'action correspondante. 130
5.12 Durée d'approbation de 100 transactions à partir de cinq capteurs. 131

Liste des abréviations

Abbréviation	Définition
IoT	Internet of Things
IdO	Internet des Objets
RFID	identification par radiofréquence
AmI	Ambient Intelligence
UbiComp	Ubiquitous computing
IA	Intelligence Artificielle
IoS	Internet of Services
ABAC	Attribute-based access control
XACML	eXtensible Access Control Markup Language
PAP	Policy Administration Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PDP	Policy Decision Point
SM	Smart Contracts
HF	Hyperledger Fabric
MSP	Membership Service Provider
WS	Web Sémantique
XML	eXtensible Markup Language
RDF	Resource Description Framework
RDFS	RDF Schema

Abbréviation	Définition
OIL	Ontology Inference Layer
DAML	Darpa Agent Markup Language
DL	Description Logic
OWL	Ontology Web Language
TBox	Terminological Box
ABox	Assertion Box
SWRL	Semantic Web Rule Language
ASP	Answer Set Programming
CWA	Closed World Assumption
OWA	Open World Assumption
UNA	Unique Name Assumption
cω-Model	closed world assumption model
NKRL	Narrative Knowledge Representation Language
HTemp	Hierarchy of Templates
HClass	Hierarchy of classe
RBAC	Rule Based Access Control
EHR	Electronic Health Record
SNN	Semantic Sensor Network Ontology
SRL	Semantic Rule Language
LRS	Langage de Règles Sémantique
DSNO	Dynamic Security Network Ontology

Introduction Générale

Les avancées et les progrès de l'intelligence artificielle, de la robotique et des diverses technologies multimédias continueront de transformer notre quotidien et rendre l'intelligence d'Internet des Objets (IdO) plus intuitifs. L'IdO permet aux systèmes complexes distribués d'interconnecter des individus, des appareils IdO et des Services (en anglais, Internet of Services (IoS)). Les technologies associées à l'IdO doivent favoriser et simplifier la capacité à percevoir et à s'adapter à la situation des usagers en fournissant des services personnalisés et adaptés. À titre d'exemple, grâce aux appareils IdO, les médecins, les patients et les citoyens devraient recevoir des messages personnalisés sur des problèmes de santé à l'aide de Smartphones, des informations sur la sécurité des citoyens à l'aide de panneaux publicitaires, etc. L' Internet des Objets doit donc veiller au bien-être individuel et protection de l'environnement des usagers. Il s'agit d'assurer la sécurité d'accès physique/virtuel aux différents dispositifs afin de prévenir les menaces potentielles dans un système distribué.

Les domaines d'application de l'Internet des Objets dédiés au bien-être humain sont donc divers tels que, l'utilisation dans l'industrie, les villes intelligentes et le domaine de la santé. Ainsi, dans le domaine de la santé par exemple, des paramètres vitaux des patients sont mesurés instantanément et transmis automatiquement. L' aspect protection des données personnelles et de la vie privée se révèlent encore être cruciax lorsqu'un personnel de l'hôpital tente d'accéder aux dossiers médicaux des patients, ou accéder à distance à la caméra de sécurité intérieure de la maison ou à une caméra embarquée dans un robot pour évaluer le mental et la santé physique d'un individu. Le système doit traiter toutes les connaissances observées ou inférées et déclenchées des actions proactives en fusionnant des données issues de différents appareils IdO disséminés dans l'environnement. Toutefois, les

dispositifs IdO sont menacés d'être sources de risques de sécurité, car ils peuvent avoir un impact potentiellement dangereux sur le bien-être humain. En effet, une plateforme de communication doit être sécurisée et résistante aux différentes attaques telles que menaces de sécurité sur les sources de données (attaque physique, attaque par injection de données et attaque par manipulation de service). En particulier, nous devons faire face à des vulnérabilités pouvant surgir lors de la manipulation de données privées. Il est donc indispensable de garantir que les appareils IdO soient correctement protégés. La mise en place des applications IdO complexes distribuées capables de comprendre le comportement des différents artefacts (personnes, robots, appareils, etc.), d'améliorer la perception du contexte de l'utilisateur nécessite la protection de la confidentialité des données, la gestion et le partage d'une compréhension commune et intelligible de l'environnement.

L' objectif principal de notre approche est de valider l'architecture cognitive globale et la flexibilité de la méthode proposée. Nous pouvons conclure qu'une couche sémantique, basée sur une ontologie, caractérise le développement récent des propositions de plateformes afin d'améliorer les capacités des applications IdO à collecter, à récupérer, à partager, à manipuler et à analyser les données des capteurs. Il est admis par la communauté de recherche qu'une ontologie permet de définir des concepts pour la description de l'aspect sécurité et confidentialité d'une manière indépendante du domaine.

Nous soulignons ici que le langage du Web Sémantique, Ontology Web Language (OWL) et ses variant sont explicitement conçus pour les besoins du web. Ces langages présentent de grandes difficultés à traiter des problèmes complexes en intelligence artificielle, par exemple, les comportements humains. Les travaux présentés dans cette thèse visent à faciliter la mise en œuvre de la protection de l'environnement et le bien être humain via le contrôle d'accès pour les systèmes distribués. Pour ce faire, nous avons proposé une architecture sémantique qui s'appuie sur un modèle basé sur l'hypothèse du monde fermé, cω-Model (closed-world Model), Narrative Knowledge Representation Language (NKRL), eXtensible Access Control Markup Language (XACML) et Blockchain Hyperledger Fabric. L' objectif est de garantir d'un côté une description sémantique des caractéristiques dynamiques

des entités et d'un autre côté, assurer l'intégrité des connaissances et préserver la confidentialité.

La thèse est organisée comme suit :

Le chapitre 1 présente une synthèse générale sur les concepts de l'Internet des Objets. Plus particulièrement, nous sommes focalisés sur les principes de ce paradigme et les défis et les enjeux associés en termes de sécurité et interopérabilité. Enfin, dans ce chapitre, nous avons présenté les solutions technologiques sur lesquelles notre proposition s'est appuyée. Il s'agit des technologies Blockchain et XACML. Nous avons également discuté le contexte de la thèse et l'approche proposée pour la mise en œuvre des appareils IdO au service du bien-être humain et la protection de leur environnement.

Le chapitre 2 donne un aperçu des systèmes de sécurité et de protection de la vie privée des usagers. Nous discutons les approches de conceptions pensées pour la conception des plateformes pour assurer l'accès sécurisé aux ressources des appareils de l'IdO et sécurisé l'échange de données. Néanmoins, nous avons soulevé des questions en matière de l'applicabilité des langages d'ontologie tels qu'OWL.

Dans le chapitre 3, nous présentons l'évolution des langages de modélisation du web sémantique. L' émergence des outils de raisonnement pour augmenter l'expressivité de modélisation des connaissances de ces langages.

Le chapitre 4 nous avons présenté les formalismes pour répondre aux problématiques liées aux fondements d'OWL. Nous détaillons une nouvelle approche qui consiste en un langage de représentation de connaissances basé sur le monde fermé avec supposition du nom unique et la reconnaissance de contexte à base de règles basées sur la logique non monotone. Dans ce chapitre, nous présentons le formalisme du modèle cω-Model pour la gestion sémantique et le Langage de Règles Sémantique (LRS, en Anglais Semantic Rule Language (SRL)). Enfin, nous présentons le formalisme de la modélisation des informations narratives NKRL basés sur les dimensions spatio-temporelles.

Dans le chapitre 5, nous présentons dans un premier temps la validation de notre approche de politique d'accès sécurisé fondée sur le modèle

XACML et le langage de règles sémantiques proposé dans le chapitre 4. Dans ce chapitre, nous montrons comment les formalismes explorés abordent l'hétérogénéité sémantique des données des capteurs lors du partage des connaissances, concilier les divergences sémantiques à travers plusieurs domaines et maintenir la politique de sécurité locale. Enfin, dans la suite du chapitre, nous montrons, l'apport du raisonnement narratif entrelacer avec la technologie émergente, Blockchain.

Dans la conclusion générale, nous dressons un bilan des contributions et des orientations futures découlant de ces travaux de thèse.

Chapitre 1

Internet des Objets : Principes, défis, technologies

1.1 Internet des Objets : Principes

Le terme "Internet of Things (IoT)" (Internet des Objets (IdO) en Français), fut inventé par Kevin Ashton pour la première fois en 1999. Son objectif était de mettre en évidence la puissance de connecter des étiquettes d'identification par radiofréquence (RFID) à l'Internet dans le cadre de la gestion de la chaîne d'approvisionnement. Le terme IdO est aujourd'hui souvent associé à d'autres paradigmes tels que l'intelligence ambiante (Ambient Intelligence (AmI) en Anglais) et l'informatique ubiquitaire (Ubiquitous computing (UbiComp), en Anglais). Mark Weiser [Weiser (1991)] a décrit l'Informatique ubiquitaire comme une vision futuriste de l'informatique du 21^{e} siècle : "*The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it*". Ainsi, L' objectif d'Ubiquitous Computing comme d'ailleurs celui d'IdO consiste à offrir à l'utilisateur un accès aux différentes fonctionnalités offertes par les divers dispositifs informatiques hétérogènes. En effet, l'IdO est associé aujourd'hui à l'e-santé, la surveillance, la traçabilité, l'Internet industriel des objets (IIdO), etc. Depuis, il demeure encore difficile de parvenir à une définition standard du terme IdO. En fait, les définitions variaient considérablement. Selon les définitions de Union internationale des télécommunications (ITU [1]) et

1. https://www.itu.int/fr/about/Pages/default.aspx

de la société de l'information de la Commission européenne, "*IdO est l'intégration des capacités d'identification, de détection/actionnement, de communication et de traitement, et la connexion de toutes les personnes et de tous les objets selon leurs intérêts, de sorte que n'importe qui et n'importe quoi, à tout moment et de n'importe où, en utilisant n'importe quel chemin/réseau, peut connecter n'importe quel autre objet pour obtenir n'importe quel service*". Par conséquent, UbiComp représente un paradigme dans lequel le traitement de l'information est complètement intégré de manière plus ou moins invisible dans les objets et les activités quotidiennes. Le terme AmI quant à lui, a été inventé par la Commission européenne en 2001, lorsque l'organisation Information Society Technology Advisory Group (ISTAG) [Ducatel et al. (2001)] a lancé le défi AmI, qui a été mis à jour plus tard en 2003.

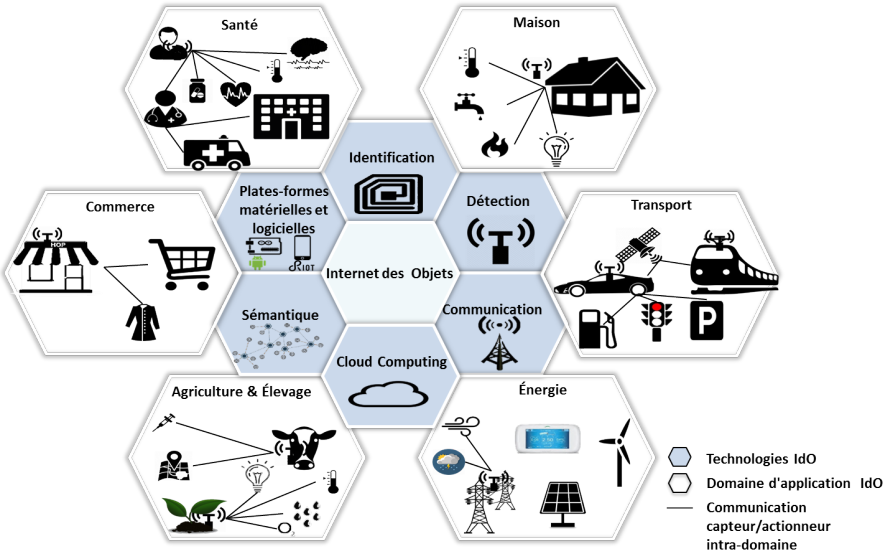


FIGURE 1.1 – Éléments de l'Internet des Objets et domaines d'application. Illustre l'ampleur des enjeux de l'IdO et ses effets sur l'humain.

L' intelligence ambiante est donc la vision d'un avenir dans lequel des environnements électroniques sont sensibles (sensibles aux besoins des personnes) et réactifs (capable d'anticiper leurs besoins et leurs comportements) à la présence des personnes. Cet environnement envisagé est interconnecté, embarqué, intelligent, personnalisé, adaptatif, anticipatif [Emile et al. (2001)], figure 1.1. En pratique, la différence entre ces termes est plutôt de nature académique : ils ont tous en commun l'objectif d'assister des per-

sonnes ainsi que l'optimisation et le renforcement continue des processus économiques et sociaux par de nombreux microprocesseurs et capteurs intégrés à l'environnement. Comme identifié par les auteurs dans [Atzori et al. (2001)], le paradigme IdO ne peut être réalisé que par la convergence de trois visions principales – "Internet Oriented", "Things Oriented" et "Semantic Oriented". Internet Oriented représente Internet et ses technologies associées. Elle agit comme un middleware (ou intergiciel en français) pour connecter des objets intelligents dans le monde entier. Things Oriented est connu sous le nom de "Intelligent Things" fait référence aux capteurs, actionneurs et aux matériels de communications embarqués qui relieront les objets du monde réel au monde numérique. Enfin, Semantic Oriented, représente les processus de connaissance et la prise décision. CASAGRAS [2] [CASAGRAS (2009)] a décrit l'IdO comme une infrastructure de réseau mondial, reliant des objets physiques et virtuels grâce à l'exploitation des capacités de capture de données et de communication. Cette infrastructure comprend les développements Internet et de réseaux existants et évolutifs. Il offrira des capacités spécifiques d'identification d'objets, de capteurs et de connexion comme base pour le développement d'applications et de services coopératifs indépendants. Ceux-ci seront caractérisés par un degré élevé de capture de données autonomes, de transfert d'évènements, de connectivité réseau et d'interopérabilité.

Plus généralement, l'IdO tient la promesse de créer un réseau mondial composé de nombreux objets connectés prenants en charge l'informatique omniprésente et la sensibilité au contexte [Dong et al. (2010), Jara et al. (2010), Bandyopadhyay et al. (2011), Broll et al. (2011)]. L' informatique omniprésente et la sensibilité au contexte sont des exigences clés de l'intelligence ambiante, l'une des principales promesses de l'IdO. L' intelligence ambiante permettrait aux objets du quotidien de comprendre leur environnement, d'interagir avec les gens et de prendre des décisions. Chaque objet intégrant l'identification, l'automatisation, l'intelligence, la détection, le traitement et la communication est considéré comme un objet intelligent qui peut faciliter la prise de conscience autonome du contexte d'un objet. En

2. CASAGRAS (Grant Agreement 216803) is a Coordination and Support Action for Global RFID-related Standardisation Activities involving, in particular, organisations from China, Japan, Korea and the USA

2018, IHS Statista [3] a estimé que le nombre d'objets IdO connectés à Internet atteindra 75 milliards d'ici 2025. Ces objets intelligents peuvent être par exemple des capteurs, des actionneurs, ou des RFID qui sont interconnectés et créent un ensemble de nouveaux services IdO.

1.2 Internet des Objets : domaines d'application

L' émergence de l'IdO ouvre une grande variété d'applications qui visent principalement à améliorer la qualité de vie des citoyens. Ces applications se retrouvent dans divers domaines, tels que la santé, l'environnement, les transports, l'énergie. Il existe ainsi des milliers d'applications et de nouvelles apparaissent chaque jour. Avant de passer en revue les défis majeurs associés l'Internet des objets, dans ce qui suit nous allons esquisser quelques domaines d'application sur lesquelles nous nous focalisons dans cette thèse.

1.2.1 Soins de santé intelligents

La santé est un domaine d'application important de l'IdO [Xu et al. (2014)]. La dépendance croissante des soins de santé à l'IdO est attribuée à un meilleur accès aux soins, à l'amélioration de la qualité des soins et à la réduction du coût des soins. Propulsé par les capacités de l'IdO, tout le système de santé peut être surveillé et suivi à tout moment et toutes les informations relatives aux soins de santé peuvent être recueillies, analysées et utilisées efficacement. Les services de soins de santé basés sur l'IdO se concentrent sur la prévention, la détection précoce des maladies et les soins à domicile au lieu du diagnostic clinique coûteux pour anticiper les besoins des patients et garantir le respect des plans de soins de santé.

Plusieurs applications de santé basées sur l'IdO ont été proposées, couvrant presque tous les aspects des soins de santé tels que la télémédecine [Ullah et al. (2021), Graham et al. (2020), Rokonuzzaman et al. (2021)], la gestion des médicaments [Ayshwarya et al. (2021), Vardhini et al. (2020)],

3. IHS Statista. 2018. Internet of Things (IdO) connected devices installed base worldwide from 2015 to 2025 (in billions). https://www.statista.com/statistics/471264/IoD-number-of-connected-devices-worldwide/

la surveillance des paramètres biophysiques par exemple la gestion des aliments [Sundaravadivel et al. (2018)]. Ces applications peuvent être classées en deux catégories : les « applications à condition unique » qui font référence à une maladie ou une infirmité spécifique, et les « applications à condition groupée » qui traitent un certain nombre de maladies ou conditions associées comme la gestion des médicaments. Les dispositifs biomédicaux (capteurs médicaux et capteurs portables) sont utilisés pour surveiller divers signes vitaux, et pour transmettre leurs données via des interfaces et des réseaux filaires ou sans fil (Bluetooth, NFC, Zigbee, Wi-Fi, WSN, etc.). Les données reçues sont ensuite transmises aux centres médicaux distants pour effectuer les actions appropriées.

1.2.2 Maison intelligente

L' IdO a les capacités nécessaires pour rendre les maisons plus intelligentes, plus interconnectée et automatisées. Cela permet d'offrir la sécurité, le confort, et l'efficience énergétique à tout moment, ce qui se traduit par une meilleure qualité de vie domestique pour les résidents [Almusaylim et al. (2019), Celtek et al. (2017), Guravaiah et al. (2019)]. Une surveillance adéquate des appareils et des systèmes domestiques par le déploiement de capteurs à différents endroits (par exemple, les systèmes de détection d'empiétement, les systèmes de chauffage, les systèmes d'éclairage, les détecteurs de fumée, les compteurs de services publics, les climatiseurs, les réfrigérateurs, etc.) permet d'économiser des ressources, de l'argent, des vies et du temps.

Par ailleurs, plusieurs systèmes d'automatisation de la maison basés sur les technologies IdO ont été conçus et développés pour améliorer le niveau de satisfaction des résidents tels que [Dipankar et al. (2020)].

1.2.3 Systèmes de transport intelligents

Les systèmes de transport intelligents (ITS) désignent des systèmes qui utilisent à la fois l'informatique et les technologies des télécommunications, du radiorepérage et de l'automatisation afin d'améliorer la sécurité, la gestion

et l'efficacité des transports terrestres [4]. Les ITS visent à rendre les systèmes de transport actuels plus sûrs, plus efficaces et plus sécurisés. Ils fournissent des plans de trajet multimodaux intelligents et réduisent la congestion du trafic, la consommation l'énergie des voitures, les risques et les émissions de CO_2 [Canale et al. (2016), Yang et al. (2017), Al-Dweik et al. (2017)]. Dans [Hari et al. (2016)], un modèle de système de stationnement automatisé intelligent a été développé à l'aide des capteurs infrarouges. Il faut l'aide d'un mécanisme de feedback pour déterminer la disponibilité des aires de stationnement dans les régions voisines. Des capteurs et des actionneurs infrarouges spéciaux sont intégrés dans la surveillance des zones de stationnement appropriées disponibles. Enfin, Internet of Vehicle (IoV) est l'application concrète de l'IdO dans le domaine du transport intelligent [Chen et al. (2016), Kaiwartya et al. (2016)]. IoV comprend cinq types de communications véhiculaires, à savoir, véhicule à véhicule, véhicule à bord de la route, véhicule à infrastructure, véhicule à appareils personnels et véhicule à capteurs pour rendre la conduite plus fiable, agréable et efficace.

1.3 Internet des Objets : Défis

En général, un système IdO comprend de nombreuses normes liées à l'identification, l'architecture, la sécurité, les protocoles de communications, le traitement de l'information, etc. Bien que diverses recherches aient été menées dans l'IdO, il reste encore des défis techniques majeurs à relever tels que l'évolutivité, la mobilité, l'interopérabilité, la gestion, la fiabilité, la disponibilité, l'accessibilité, etc. Dans ce qui suit nous passons en revue les différents défis soulevés par les académiciens et industriels :

1.3.1 Architecture

L' IdO englobera un très large éventail de technologies. Par conséquent, l'architecture de référence unique ne peut pas être utilisée comme modèle pour toutes les implémentations concrètes possibles. Si un modèle de référence peut probablement être identifié, il est probable que plusieurs architec-

4. https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-49-2021-PDF-F.pdf

tures de référence coexisteront dans l'IdO. Les architectures IdO doivent être ouvertes, basées sur des normes et flexibles.

1.3.2 Évolutivité passage à l'échelle (en Anglais scalability)

L' évolutivité peut être définie comme la capacité du réseau à répondre aux demandes croissantes du réseau [Bondi et al. (2000)]. C'est une exigence fondamentale de tout système IdO pour gérer la capacité de la quantité croissante de travail. Il peut être catégorisé comme suit : mise à l'échelle verticale et mise à l'échelle horizontale. La mise à l'échelle verticale est destinée à mettre à niveau les périphériques réseaux existants. Par exemple, ajouter de la puissance de traitement à un serveur pour augmenter sa vitesse. De plus, un système peut évoluer en l'étendant et en ajoutant plus de traitements, de mémoire principale, de stockage et d'interfaces réseau au nœud pour adapter le système afin de gérer plus de demandes. La mise à l'échelle horizontale, quant à elle, consiste à étendre le réseau en introduisant plus de nœuds. Cela peut être réalisé en ajoutant plus de machines dans le groupe de ressources et en ajoutant plus d'appareils IdO à un réseau. Conformément aux prédictions faites par IHS Statista, l'IdO évolue et se développe continuellement pour répondre aux demandes toujours croissantes. Par conséquent, les technologies futures devraient être très flexibles pour traiter des milliards d'objets intelligents qui sont inévitablement connectés à Internet.

1.3.3 Mobilité

La mobilité est l'un des principaux défis techniques pour les implémentations de l'IdO. En effet, une plateforme IdO est vue comme une multitude de services, nommée également Internet de services (ou en Anglais Internet of Services (IoS)). Ils permettent de collecter, stocker, corréler, analyser et exploiter les données. Ce qui constitue un défi majeur en économie numérique puisqu'il s'agit ici aux industriels et gouvernements de gérer le transfert de données (à l'intérieur d'un pays comme à l'extérieur, le Covid-19 en est un exemple marquant pour le partage d'informations entre les pays) y compris

des données personnelles et confidentielles des usagers. Par conséquent, le principe de base de l'IdO est de connecter en permanence les utilisateurs mobiles aux services souhaités. Le service des appareils mobiles dans les systèmes IdO peut devenir indisponible lorsque ces appareils passent d'une passerelle à une autre, ce qui nécessite des solutions efficaces qui garantissent la continuité du service. Dans ce contexte, [Ganz et al. (2012)] ont proposé un schéma de mobilité des ressources qui introduit un mode de mise en cache et un mode tunnel pour permettre aux applications d'accéder aux données sensorielles lorsque les ressources deviennent temporairement indisponibles. En outre, le nombre d'appareils mobiles aux ressources limitées dans les systèmes IdO nécessite également des mécanismes efficaces pour prendre en charge la gestion de la mobilité dans l'environnement IdO. Un schéma de gestion de la mobilité réalisable a été présenté dans [Fu et al. (2014)]. Ce schéma gère la mobilité du groupe en fonction des similitudes dans les modèles de mobilité des appareils. Un autre schéma où la gestion de la mobilité des capteurs et la continuité du service sont tous deux abordés en fournissant un mécanisme de gestion du cycle de vie du service distribué est proposé dans [Elsaleh et al. (2011)]. Ce mécanisme gère le cycle de vie des instances de services Web qui représentent un capteur en utilisant une superposition pair-à-pair entre les passerelles.

1.3.4 Interopérabilité

L' interopérabilité peut être définie comme la capacité des logiciels et des objets à communiquer entre eux pour un échange et un traitement efficaces des informations [Jussi et al. (2014)]. Chaque objet dans l'environnement IdO a des capacités de traitement, de collecte d'informations et de communication. De plus, les objets seraient également soumis à diverses conditions, notamment la disponibilité de l'énergie, les capacités de calcul et de sécurité, ce qui soulève de nombreux problèmes d'interopérabilité dans l'IdO. Par conséquent, la solution d'interopérabilité doit être garantie pour offrir une interaction transparente entre les différentes entités IdO. L' interopérabilité doit également être abordée par les développeurs d'applications et les fabricants d'appareils pour fournir des services peu importe les spécifications

de la plateforme (i.e., divers protocoles de communication) utilisée par les clients. Les descriptions de service, la publication, les pratiques courantes, les normes et les mécanismes de découverte font partie des nombreux autres défis qui doivent également être pris en compte avant de permettre des interactions interopérables entre des objets.

1.3.5 Gestion du flux et auto-configuration

La gestion efficace de milliards ou de billions d'appareils IdO hétérogènes est un autre défi de l'IdO. Selon l'organisation internationale de normalisation (ISO), l'objectif principal de la gestion de réseau est de mieux comprendre les principales fonctions des systèmes de gestion de réseau en matière de faute, configuration, comptabilité, performance et sécurité (ou en Anglais FCAPS (fault, configuration, accounting, performance and security)). Ces capacités de gestion aident à réduire les coûts et à accélérer de nombreuses tâches de maintenance [Elkhodr et al. (2016)]. Par conséquent, de nouvelles solutions de gestion qui devraient combiner toutes ces fonctionnalités sont nécessaires pour gérer le cauchemar de gestion potentiel qui résultera du nombre croissant d'appareils IdO dans les prochaines années.

1.3.6 Fiabilité

La fiabilité est un problème critique dans l'environnement IdO, en particulier dans des cas d'urgence où une réponse immédiate et appropriée doit être fournie. Comme dans les applications critiques telles que la gestion des risques en industrie, le transport et les applications de soins de santé [Wang et al. (2017)]. En effet, en ce qui concerne la fonctionnalité du système, une perception, une collecte, une transmission et un traitement des données peu fiables peuvent entraîner de longs retards, des pertes de données et éventuellement de mauvaises décisions. Par conséquent, cela peut causer d'énormes dommages ou des conditions potentiellement mortelles. Il est essentiel de concevoir des systèmes fiables transversalement à toutes les couches de l'architecture IdO qui fonctionnent correctement en toutes circonstances, puis de construire un système IdO efficace.

1.3.7 Contraintes de ressources

Les contraintes de ressources font référence aux appareils IdO qui ont été spécifiquement conçus avec une puissance limitée, des capacités de stockage limitées et un traitement limité. Les systèmes IdO génèrent de grandes quantités de données, générant une forte demande de ressources réseau [Siow et al. (2018)]. Les appareils IdO ont tendance à être petits et équipés de batteries pour maintenir l'équilibre entre la durée effective de leur durée de vie et les coûts potentiels de remplacement de l'appareil.

En conséquence, ces appareils sont généralement soumis à des contraintes strictes sur leur consommation électrique et les ressources matérielles disponibles. Des utilisations efficaces de l'énergie des appareils IdO maintiendraient une durée de vie prolongée du réseau. Une solution possible est que les appareils IdO doivent être auto-alimentés pour récupérer l'énergie ambiante (nous parlons dans ce cas du principe du Energy harvesting). Le mécanisme de déchargement des calculs et la gestion du cycle veille-sommeil sont des techniques importantes qui sont efficaces pour réduire la consommation d'énergie des dispositifs IdO [Haimour (2019), Elsts et al. (2018), Klinefelter et al. (2015)].

1.3.8 Sécurité et Protection de la vie privée

L' acceptation sociale des services et des technologies IdO dépendra de la protection des données et de la véracité des informations. Le bien-être [Dimitrios et al. (2021)], la sécurité et la protection de la vie privée représentent donc des défis majeurs pour l'IdO qui doivent être relevés. Comme la communication dans de tels environnements est assurée par des canaux sans fil, les principaux éléments de l'IdO tels que la RFID, les dispositifs de détection, les éléments de réseau, le cloud computing et le stockage de données peuvent subir divers types d'attaques, notamment écoute clandestine, l'accès non autorisé, la modification des données et les problèmes de la protection de la vie privée, etc. De plus, les applications IdO se caractérisent par leur nature distribuée et leurs appareils connectés à grande échelle qui imposent plus de défis en matière de sécurité et de la protection de la vie privée [Nivedita et al. (2021), Nivedita et al. (2021)]. À ce niveau, les challenges sont

menés de manière indépendante et prudente pour répondre à chaque exigence de l'application. Comme en témoignent les travaux de [Johannes et al. (2020), Nivedita et al. (2021)], ces dernières années les applications IdO telles que les voitures intelligentes, les systèmes de contrôle industriels et les systèmes IdO équipés de dispositifs médicaux sont également devenus la cible des attaquants. Dans ce contexte vital, des chercheurs industriels et universitaires ont souligné que les principales préoccupations du paradigme de l'IdO sont les problèmes d'hétérogénéité, de sécurité et de confidentialité. Ainsi, le renforcement des services publics sur la sécurité des citoyens empêche la diffusion de messages et l'échange de données au sein du réseau urbain, protège la vie privée des utilisateurs et sécurise l'accès aux différents appareils IdO. La coordination des sociétés de sécurité privées, des services d'ambulance, des hôpitaux et des supermarchés sont de plus en plus nécessaires, voire vitaux, pour des missions allant de la prévention et de la sécurité au quotidien, à la gestion d'évènements exceptionnels (urgences ou crises majeures), figure 1.2. Bien que plusieurs projets aient été développés pour relever les défis de la sécurité et de la protection de la vie privée de l'IdO, il est nécessaire de déployer beaucoup plus d'efforts pour créer un mécanisme de protection de sécurité fiable et de garantir que les utilisateurs se sentent à l'aise de participer à l'IdO. Par conséquent, des plateformes dédiées sont plus que nécessaire pour éliminer des vulnérabilités de sûreté et d'authentification pour préserver le bien-être humain [Hassija et al. (2019), Leonardo et al. (2021)]. En particulier, la sécurité d'un système IdO repose sur plusieurs exigences de sécurité fondamentales et spécifiques de la sécurité informatique : confidentialité, intégrité, disponibilité, authenticité et non-répudiation que l'on décrit comme suit [Abomhara et al. (2015), Aumasson et al. (2013)] :

1. Confidentialité : Est l'une des mesures de sécurité les plus importantes d'un système IdO. La confidentialité est le processus de dissimulation d'informations privées aux objets IdO ;
2. Intégrité : Signifie que les données transférées ne peuvent pas être modifiées par un tiers accidentellement ou volontairement. Cela permet de garantir la véracité, l'honnêteté, la fiabilité, ainsi que l'absence de manipulation non autorisée des données pendant la transmission. Par

conséquent, comme le nombre d'objets IdO devient très élevé, fournir des services de sécurité réutilisables, tels que l'intégrité, devient un problème central en matière de sécurité IdO. Le hachage est le mécanisme principal utilisé pour contrôler l'intégrité des données ;

3. Disponibilité : Implique que tous les services et objets IdO du système IdO sont disponibles à tout moment, et accessibles par les utilisateurs authentiques en cas de besoin. Cela signifie la continuité des services de sécurité et la prévention de toute défaillance de l'appareil et de toute interruption de fonctionnement. Les mécanismes utilisés pour le maintien de la disponibilité sont les moyens de protection contre les attaques physiques (attaques de privation de sommeil pour épuiser rapidement la batterie des appareils IdO à faible puissance), les attaques de déni de service (DoS : Denial of Service) et les attaques de déni de service distribué (DDoS : Distributed Denial of Service) ;

4. Non-répudiation : Garantit que l'expéditeur ne peut pas nier une action qui a déjà été faite dans les systèmes IdO. En effet, il permet de protéger contre un faux déni d'implication dans une communication. Par conséquent, le service de non-répudiation est un service de sécurité efficace qui doit être mis en œuvre et construit sur l'IdO pour fournir une véritable confiance élevée dans les données transmises. Cela peut être réalisé en utilisant la cryptographie à courbe elliptique (ECC : Elliptic Curve Cryptography) et la cryptographie à courbe hyperelliptique (HECC : Hyper-Elliptic Curve Cryptography) ;

5. Protection de la vie privée : Comprend la dissimulation d'informations personnelles et la capacité de contrôler ce qu'il advient de ces informations. De plus, il assure la non-traçabilité des comportements de l'utilisateur et des actions effectuées dans le système IdO. Par conséquent, la protection de la vie privée, définie comme les droits des individus, des groupes et des institutions, est considérée comme un grave problème de sécurité ;

FIGURE 1.2 – Défis majeurs de l'IdO et la gestion de données pour évaluer une situation et fournir une action adéquate.

1.4 Synthèse

En raison de la forte prévalence de l'IdO dans l'industrie et la vie quotidienne en plus les défis de l'IdO mentionnées précédemment, nous devons déterminer les exigences de sécurité afin de développer un système IdO sécurisé. Les problèmes de sécurité de l'IdO ont été couverts en détail par plusieurs chercheurs. Par exemple, dans [Leloglu et al. (2017)]. Les auteurs analysent les exigences de sécurité pour l'IdO, y compris l'autorisation et l'authenticité. En outre, d'autres auteurs ont classé les services de sécurité requis pour les différentes applications IdO en fonction de leur importance, comme dans le réseau intelligent, la disponibilité est le service le plus critique, tandis que pour les soins de santé, l'authentification est un service capital [Kouicem et al. (2018)]. Par conséquent, le paradigme IdO impose de nombreuses inquiétudes sur la sécurité des données en raison de l'espionnage économique, de l'infection de systèmes informatiques sensibles, de l'usurpation d'identité, etc. À ce niveau, les infrastructures IdO sécurisées doivent fournir des services de sécurité réutilisables tels que la confidentia-

lité, l'intégrité, l'authentification, l'autorisation, la disponibilité et la protection de la vie privée.

Nous adhérons donc à l'idée que la conception de mécanismes d'authentification et de contrôle d'accès est indispensable pour répondre aux exigences des services de sécurité cités-dessus. En effet, l'authentification est le processus de validation si une identité donnée correspond à la prétendue entité IdO [Makhdoom et al. (2019)]. Il vient après l'identification qui consiste à identifier une entité par l'utilisation d'un élément d'identification. Un élément d'identification est une information permettant l'identification formelle et distinctive d'une entité. En particulier, l'authentification est nécessaire entre deux ou un groupe de parties afin de sécuriser la communication dans le système IdO. L' authentification garantit que seuls les utilisateurs autorisés peuvent accéder aux appareils IdO et assure la non-répudiation des communications. De plus, le contrôle d'accès est un mécanisme qui permet de protéger l'accès aux objets et aux ressources IdO (données, applications, services) en limitant l'accès aux utilisateurs qui ne disposent pas des autorisations requises [Sowmya et al. (2019)]. L' autorisation est obtenue après la réussite de l'authentification de l'utilisateur d'identité de confiance. Par conséquent, l'établissement de mécanismes d'authentification et d'identité efficaces est nécessaire pour les mécanismes de contrôle d'accès. Dans ce qui suit, nous expliquons les technologies de bases sur lesquelles sont fondés les travaux de cette thèse.

1.5 Internet des Objets : Technologies associées

1.5.1 Blockchain

En tant que technologie émergente, Blockchain est livré avec des outils pour protéger les données personnelles sensibles et résoudre les problèmes de fiabilité en fournissant une architecture de communication sécurisée dans la conception d'applications distribuées (par exemple, Industrie 4.0, Santé, etc.).

L' architecture de réseau traditionnelle et de nombreux schémas traditionnels de protection de la vie privée stockent les données dans le serveur

centralisé pour garantir que les données ne sont pas divulguées.

Tandis que les technologies Blockchain proposent le concept de Smart Contracts 'SM' (règles et actions basées sur des scénarios prédéfinis). Le SM s'exécute automatiquement à l'aide d'informations contextuelles répliquées sur le réseau, offrant une plus grande autonomie requise dans de nombreux environnements IdO ouverts et dynamiques, la domotique, l'industrie 4.0, la robotique, la santé, et supprime, par conséquent, le besoin d'un tiers de confiance centralisé pour agir comme intermédiaire. D'un point de vue de gestion des données, la Blockchain est considérée comme une base de données immuable et décentralisée conservant une liste sans cesse croissante d'enregistrements ordonnés, horodatés et signés, appelés blocs. Ces derniers sont protégés contre la falsification et partagés entre les membres participants. Chaque bloc contient une version du bloc (indiquant les règles de validation à suivre), un horodatage de sa génération, un nonce commençant à 0 et augmentant pour chaque calcul de hachage, une liste de transactions valides nommée MerkleRoot (c'est-à-dire la valeur de hachage de la racine d'un arbre Merkle avec concaténation des valeurs de hachage de toutes les transactions du bloc lui-même (unique identifier)) et la valeur de hachage de son bloc précédent appelé bloc parent, qui sert de lien cryptographique au bloc parent, formant une Blockchain. L' arbre de Merkle est un arbre binaire dans lequel chaque nœud possède exactement deux nœuds enfants et tous les nœuds feuilles sont au même niveau, figure 1.3. Les arbres de Merkle ont adopté la fonction de hachage pour former un composant du bloc. Chaque feuille est étiquetée avec le hachage cryptographique de transaction et chaque nœud non-feuille est essentiellement une valeur de hachage de deux valeurs concaténées de ses deux enfants. Le premier bloc d'une Blockchain est appelé le bloc «genesis» n'ayant pas de bloc parent.

L' unité de base des enregistrements dans Blockchain est la transaction. Les transactions sont des opérations individuelles et indivisibles qui impliquent l'échange ou le transfert d'actifs numériques. Ces derniers peuvent être des informations, des biens, des services, des fonds ou un ensemble de règles pouvant déclencher une autre transaction. Chaque fois qu'une nouvelle transaction est générée, elle est diffusée à l'ensemble du réseau Blockchain. Les nœuds recevant la transaction peuvent vérifier la transaction en

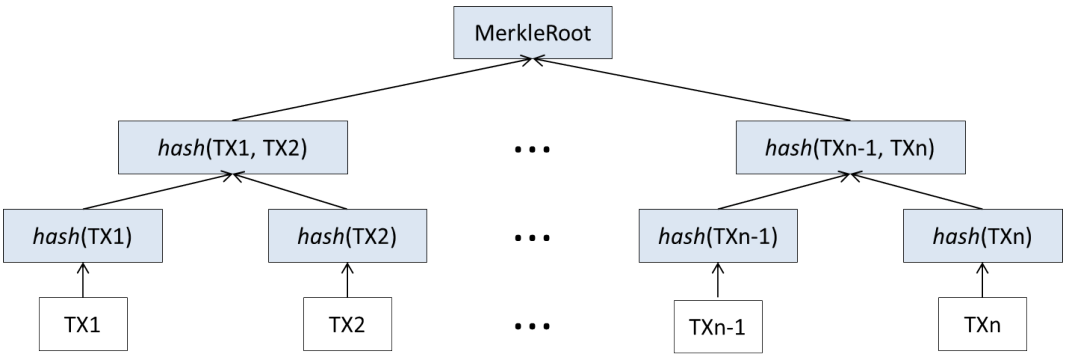


FIGURE 1.3 – Arbre de Merkle.

validant la signature attachée à la transaction, et inclure (en Anglais mine) les transactions vérifiées dans des blocs sécurisés par chiffrement. Ces nœuds sont connus sous le nom de « miners » de blocs. Pour permettre à un miner de créer un bloc, un problème de consensus doit être résolu de manière distribuée. Les miners qui parviennent à résoudre le problème du consensus diffusent leurs nouveaux blocs sur tout le réseau.

À la réception d'un nouveau bloc, les miners qui n'ont pas encore été en mesure de résoudre le problème du consensus ajoutent le bloc à leurs propres chaînes de blocs maintenus localement par les miners, après que toutes les transactions incluses dans le bloc sont vérifiées et que le bloc est également prouvé, la bonne réponse au problème du consensus est fournie. Un bloc validé sera automatiquement ajouté à la fin de la Blockchain via la référence inverse pointant vers le bloc parent. De cette manière, toute modification non autorisée sur le bloc généré précédemment peut être facilement détectée puisque la valeur de hachage du bloc falsifié est significativement différente de celle du bloc inchangé. De plus, étant donné que la Blockchain est distribuée sur l'ensemble du réseau, le comportement de falsification peut également être facilement détecté par d'autres nœuds du réseau.

1.5.2 Cryptographie pour Blockchain

La Blockchain utilise différents types de cryptographie sans aucun intermédiaire pour assurer la sécurité du système. La cryptographie à clé publique, la fonction de hachage, l'arbre de Merkle et la preuve de connaissance

zéro (en Anglais Zero-Knowledge Proofs) sont des cryptographies courantes dans le système Blockchain [Santos et al. (2021)].

1.5.3 Blockchain & les algorithmes de consensus

Un système de Blockchain utilise un algorithme de consensus pour établir la confiance et stocker correctement les transactions sur les blocs. Ainsi, les algorithmes de consensus peuvent être considérés comme le cœur de toutes les transactions de Blockchain. Un protocole de consensus est essentiellement un ensemble de règles à suivre par chaque participant. En tant que technologie distribuée sans confiance universelle, la Blockchain a besoin d'un mécanisme de consensus distribué pour que tous les participants s'accordent sur l'état actuel de la Blockchain. Un certain nombre de mécanismes de consensus uniques ont été conçus pour les Blockchains, notamment Proof of Work (PoW), Prof of State (PoS), Delegated Proof of State (DPoS), Proof of Elapsed Time (PoET) , Practical Byzantine Fault Tolerance (PBFT), Directed Acyclic Graph (DAG), Proof of Authority (PoA), Tendermint , Ripple, Scalable Byzantine Consensus Protocol (SCP), Proof of Bandwidth (PoB), Proof-of-Importance (PoI) , Proof of Burn , Proof of Capacity, en fonction de leurs besoins uniques. Une étude sur ces différents consensus est détaillée par [Kapil et al. (2019)].

Une Blockchain peut être classée en deux catégories en fonction des contrôles d'accès, telles que la Blockchain sans autorisation et avec autorisation (autorisée). Dans une Blockchain sans autorisation, n'importe qui peut accéder au réseau de la Blockchain. La Blockchain publique est le meilleur exemple de ce type de Blockchain.

— **Blockchain publique :** La Blockchain publique est une Blockchain qui fonctionne de manière complètement distribuée et sans autorisation. Il n'y a aucune restriction sur l'adhésion, l'extraction ou l'envoi de transactions sur le réseau Blockchain. Il est open source et les blocs de transaction sont visibles publiquement, bien que les transactions se déroulent sous une forme anonyme. Chaque nœud à la même copie de la Blockchain, donc personne ne peut modifier les données de la Blockchain. Bitcoin et Ethereum sont des exemples populaires de Blo-

ckchain publique ;

Dans une Blockchain avec autorisation, certaines opérations telles que l'extraction d'un bloc, la publication d'une transaction ou même la lecture de la Blockchain peuv-ent être soumises à des autorisations. Par conséquent, seuls les nœuds qui ont l'autorisation fournie par le réseau peuvent accéder au réseau Blockchain et effectuer certaines tâches. Ils fournissent un système de sécurité Blockchain supplémentaire. Il est classé en Blockchain privée et consortium ;

- **Blockchain privée :** La Blockchain privée est applicable aux petites organisations. Ce type de réseau contrôle l'accès aux services de Blockchain. Seuls les participants autorisés peuvent rejoindre Blockchain et effectuer des opérations dessus. La Blockchain privée est plus centralisée et nécessite un administrateur qui s'occupe des opérations liées au contrôle d'accès ;
- **Blockchain du consortium :** La Blockchain consortium est une Blockchain avec autorisation gérée par plus d'une organisation. Tous les nœuds provenant d'organisations autorisées sont autorisés à accéder aux données de la Blockchain, et seul le groupe de nœuds présélectionnés a le droit à participer au protocole de consensus ;

Dans le cadre de cette thèse, nous avons opté pour la Blockchain Hyperledger Fabric (HF [5]). En effet, Hyperledger Fabric est une plateforme distribuée open source de la Fondation Linux. Elle établit une confiance décentralisée dans un réseau. Seules les données que nous voulons partager sont partagées entre les participants concernés (c'est-à-dire, assurer des contrôles de confidentialité avancés). Hyperledger Fabric est une Blockchain autorisée et habilitée à créer un consortium, ce qui signifie que les participants (c'est-à-dire les organisations) sont identifiés et peuvent ne pas se faire confiance. De plus, il fournit des protocoles de consensus permettant aux organisations (multipartites) de personnaliser leur protocole de consensus. Chaque participant contrôle un ou plusieurs pairs (c'est-à-dire un nœud dans la chaîne) et doit traiter un code Blockchain comme non fiable et malveillant puisque n'importe qui peut déployer dynamiquement un contrat in-

5. https://www.hyperledger.org/use/fabric

telligent. Dans ce qui suit, nous décrivons chaque composant décrit dans la figure 1.4.

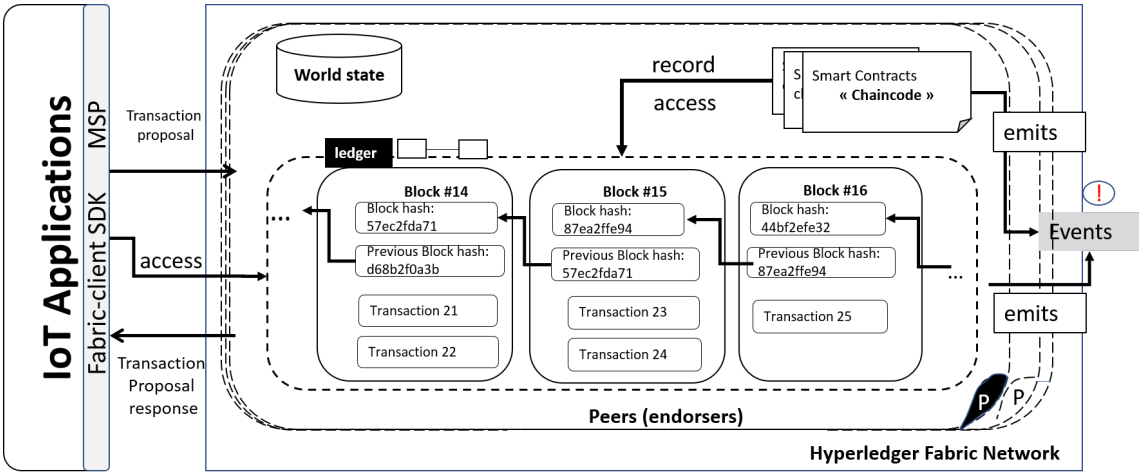


FIGURE 1.4 – Principaux composants d'une Blockchain Hyperledger Fabric. Pour des raisons de compréhension nous avons préféré garder les appellations en Anglais.

- Ledger : est un enregistrement inviolable de toutes les transitions d'état. Il stocke les blocs immuables et l'état actuel. Chaque pair conserve une copie du registre. L' état du monde est une base de données ordinaires, stocke les sorties combinées de toutes les transactions. L' état est physiquement implémenté sous forme de base de données pour fournir un stockage et une récupération simple et efficace des états du grand livre distribué. Une fonction de hachage cryptographique (algorithme) prend n'importe quelle donnée binaire en entrée et génère une sortie de longueur fixe en octets (valeur de hachage), par exemple 57ec2fda71, figure 1.4. La valeur de hachage sert d'empreinte numérique de ces données ;
- Chaincode (Smart Contract) : est signé encodé dans le langage de programmation. De plus, il s'agit d'un conteneur générique pour déployer du code sur un réseau Blockchain Hyperledger Fabric. Il s'exécute sur un grand livre distribué pour encoder les actifs et les instructions de transaction pour modifier les actifs ;
- Peer network : terme frontière qui englobe l'ensemble du flux transactionnel, qui génère un accord sur la commande et confirme l'exactitude

de l'ensemble des transactions constituant un bloc. Les pairs sont les composants fondamentaux de tout réseau fabric. Les pairs stockent le registre de la Blockchain et valident les transactions avant qu'elles soient engagées dans le registre. Les pairs exécutent les contrats intelligents qui contiennent la logique métier utilisée pour gérer les actifs sur le registre de la Blockchain. Chaque pair du réseau doit appartenir à un membre du consortium ;

- Membership (MSP) : l'authentification des services d'adhésion autorise et gère les identités sur un réseau Blockchain autorisé. Ainsi, le MSP est l'épine dorsale de tous les systèmes puisqu'il permet à chaque entité d'être reconnue et approuvée par les membres du réseau. En effet, le MSP contient toutes les identités autorisées et intègre la chaîne de confiance des membres de l'organisation qui ont rejoint le réseau ;
- Events handlers : créer une notification des opérations importantes sur la Blockchain et des notifications liées aux contrats intelligents. Tous les évènements incluent l'ID de transaction, permet aux applications d'agir lorsqu'une transaction se produit ;
- Fabric SDK : la gestion du système permet de créer, de modifier et de surveiller les composants de la chaîne de blocs. Le client fabric (mis à disposition via le SDK Fabric) fournit l'API queryByChaincode() permettant aux développeurs de transmettre une demande de requête à un homologue. Cette méthode est disponible sur un objet canal instancié et prend deux entrées. Outre l'utilisation d'une requête de code Blockchain (requêtes implémentées dans le code Blockchain), une application cliente peut envoyer une requête directement au grand livre distribué, ce qui est utile pour récupérer des informations de métadonnées (par exemple, un code Blockchain instancié) ou pour récupérer une transaction ou un bloc spécifique de la Blockchain ;

1.6 Attribute-based access control (ABAC)

Le modèle Attribute-based Access Control (ABAC) a été développé par [Eric et al. (2005)] afin de remédier aux difficultés rencontrées par les archi-

tectures web services en termes de sécurité. En effet, l'idée principale du modèle d'ABAC consiste à utiliser des politiques qui combinent des attributs au lieu d'identités, de rôles ou de dégagements pour les autorisations d'accès. Contrairement aux autres modèles de contrôle d'accès, la prise de décision des politiques ABAC est basée sur la divulgation des informations d'identification émises par des certificateurs d'attributs tiers (par exemple, des organisations, des entreprises, des institutions). Par conséquent, le privilège d'accès peut être obtenu par des sujets sans être préalablement connu de l'administrateur système (ou du propriétaire de la ressource). Comme l'illustre la figure 1.5, il existe quatre types d'attributs :

1. Attributs du sujet : les sujets sont les entités demandant l'accès aux objets. Chaque sujet peut être caractérisé via un attribut atomique ou un ensemble d'attributs sans référence explicite à son identité. Presque toutes les informations associées à un sujet peuvent être considérées comme un attribut tel que le nom, le rôle, l'affiliation et l'adresse ;

2. Attributs des actions : les actions sont les opérations que l'utilisateur souhaite effectuer. Les attributs d'action courants dans les demandes d'autorisation sont "lecture" et "écriture". Dans des scénarios plus complexes, l'action peut être décrite par une combinaison d'attributs ;

3. Attributs d'objet : les objets sont des ressources que le sujet souhaite manipuler. Les attributs d'objet peuvent affecter le type d'autorisation accordée. Ils peuvent inclure le nom de la ressource, son type (par exemple, texte, image). Le propriétaire et les informations d'un objet peuvent être automatiquement extraits de ses métadonnées ;

4. Attributs d'environnement : l'environnement peut être décrit par des informations techniques, opérationnelles, liées à la situation ou au contexte dans lequel l'accès à l'information se produit. La spécificité du modèle ABAC est la considération du contexte. Les attributs de contexte peuvent être l'heure, la date, le lieu, etc.

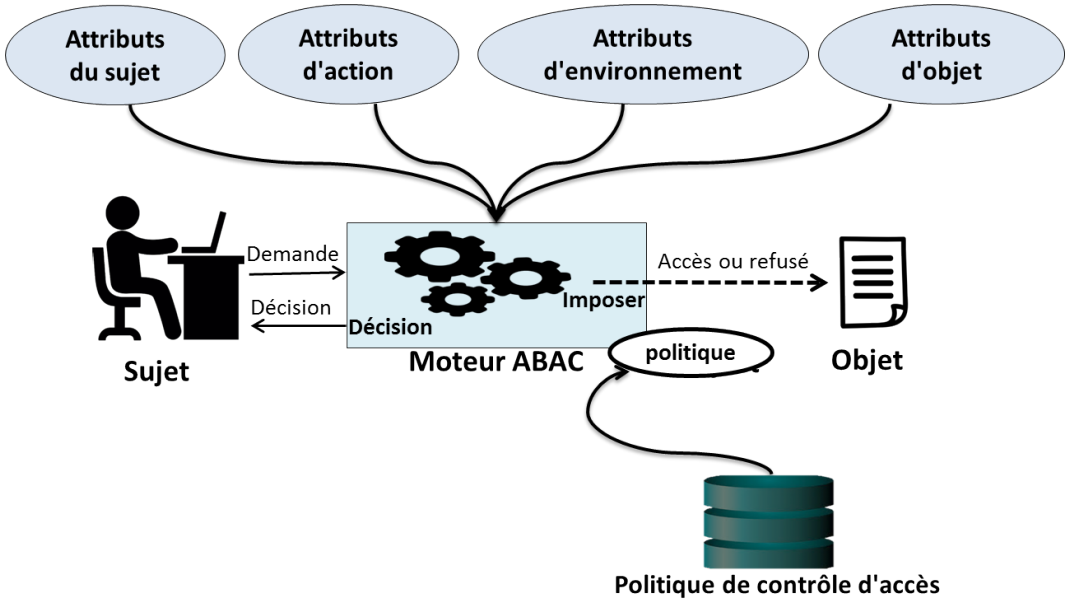


FIGURE 1.5 – Modèle ABAC.

1.6.1 XACML : Mise en œuvre du modèle ABAC

eXtensible Access Control Markup Language (XACML [6]) est un standard OASIS (Organization for the Advancement of Structured Information Standard [7]), qui définit un langage pour le contrôle d'accès, l'administration des règles et la politique de sécurité des systèmes d'information. XACML définit un langage capable d'exprimer les déclarations de politique pour une grande variété de systèmes et d'appareils d'information.

L' approche adoptée par XACML consiste à rassembler des techniques établies de longue date pour le contrôle d'accès, puis à étendre un langage indépendant de la plateforme (XML) avec une syntaxe et une sémantique appropriées pour exprimer ces techniques sous la forme d'énoncés de politique. XACML décrit à la fois un langage de politique de contrôle d'accès et un langage de requête/réponse. Le langage de politique est utilisé pour exprimer les politiques de contrôle d'accès (qui peuvent faire quoi et quand) tandis que le langage de requête/réponse exprime des requêtes pour savoir si un accès particulier doit être autorisé (demandes) et décrit les réponses à ces requêtes (réponses).

6. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
7. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

1.6.2 Principaux composants de XACML

Un moteur XACML typique se compose des principaux composants suivants, figure[8] 1.6 :

1. **Policy Administration Point (PAP)** : définit, stocke et gère les politiques ;
2. **Policy Enforcement Point (PEP)** : responsable de l'acte réel d'autoriser ou d'empêcher l'accès à la ressource. Il coordonne également l'exécution des obligations, qui sont des opérations supplémentaires qui doivent être effectuées lorsqu'une décision a été prise ;
3. **Policy Information Point (PIP)** : fournit des informations externes, telles que, les valeurs d'attribut sur le sujet, la ressource et l'action ;
4. **Policy Decision Point (PDP)** : évalue les politiques et émet les décisions d'autorisation finales ;
5. **Context Handler** : convertit les demandes d'accès du format de demande natif au format XACML et convertit également les décisions d'autorisation XACML au format de réponse natif. En même temps, il collecte les valeurs d'attribut et les renvoie au PDP ;

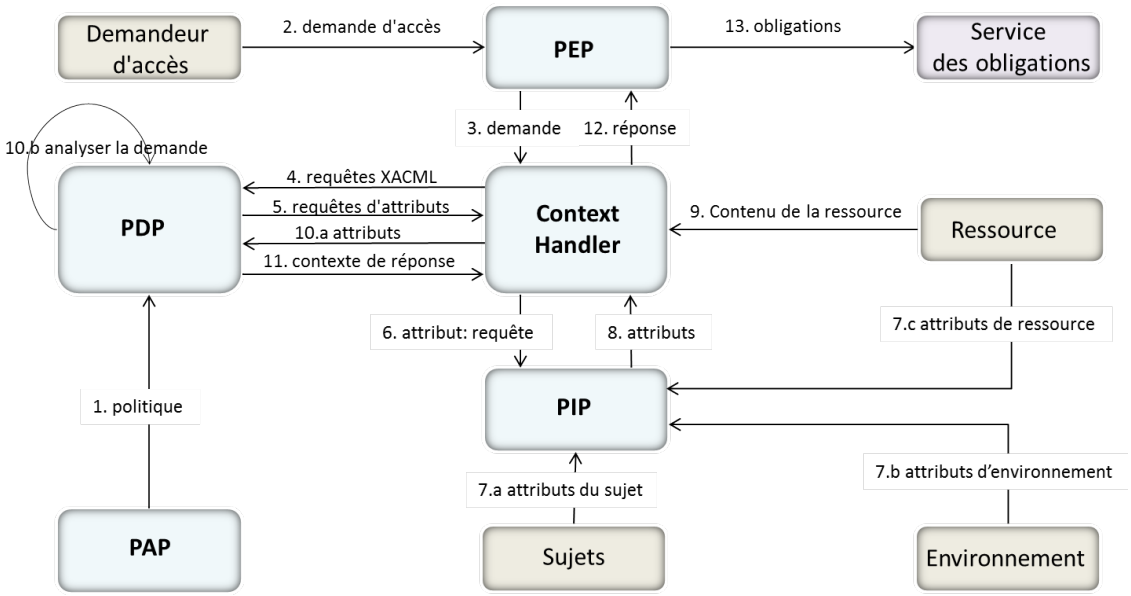


FIGURE 1.6 – Diagramme de flux de données du langage XACML 3.0.

8. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

XACML a des capacités de prévention et de détection qui sont utilisées pour prendre la décision d'accès. Les principaux composants de la politique sont «rule», «policy», et « PolicySet ». «rules» sont les composantes minimales d'une politique qui se compose de trois éléments : cible, effet et condition. La cible est un ensemble de demandes de décision, qui joue un rôle important dans la réduction de plusieurs politiques en place à celles applicables uniquement grâce à la correspondance de cible avec ses composants internes. L' effet est le résultat attendu (autoriser ou refuser) à fournir lorsqu'une «rule» est satisfaite. La condition est la fonction à exécuter lorsqu'une cible de «rule» est applicable, conduisant à un résultat "Vrai" ou "Faux". «policy» est un ensemble de règles regroupées à l'aide d'un algorithme de combinaison de règles avec des paramètres de combinaison sélective. Alors que « PolicySet » est un ensemble de politiques.

Le moteur XACML évalue une demande XACML donnée par rapport à plusieurs politiques. Ce moteur utilise deux entrées et renvoie une sortie. Les deux entrées sont les politiques XACML et la demande d'accès, tandis que la sortie est la décision d'accès. Dans l'évaluation, l'effet indique la conséquence d'une règle («rules» dans le jargon XACML). «rules» peuvent éventuellement contenir une condition, qui consiste en une expression booléenne qui limite d'avantage l'applicabilité de «rule». Il existe quatre valeurs de décision de contrôle d'accès : «Permit» (l'action demandée est autorisée), «Deny» (l'action demandée est refusée), «NotApplicable» et «Indeterminate». Les deux dernières valeurs sont renvoyées lorsqu'une erreur se produit et qu'aucune décision ne peut être prise ou lorsque la demande ne peut pas être satisfaite par le service interrogé.

1.7 Conclusion

La sécurité et la gestion sémantique des connaissances dynamiques sont au cœur du processus de développement d'applications IdO. Le manque d'interopérabilité et de surveillance de l'accès physique/virtuel à l'environement ou aux données sensibles peut mettre en danger une adoption large et uniforme du paradigme IdO dans nos systèmes techno- et socio-économiques. Néanmoins, de nombreuses applications IdO sont limitées en éner-

gie, ce qui nécessite une auto-alimentation pour récupérer l'énergie ambiante sans fournir de puissance de calcul. Ainsi, il n'est pas facile d'adopter des mécanis-mes de sécurité et de confidentialité conçus pour les systèmes traditionnels tels que le Contrôle d'Accès Discrétionnaire.

Dans le monde de l'Internet des Objets, comme dans celui du Web, il est nécessaire d'identifier des objets de manière unique. Il s'agit bien de définir un objet physique ou une entité abstraite par rapport à l'environnement auquel est supposé appartenir. Ces questions fondamentales sont souvent posées par des concepteurs de l'ingénierie des connaissances. L' objectif est de trouver un formalisme permettant de donner un sens aux informations véhiculées en sorte qu'elles soient compréhensibles par un programme et non pas seulement par un humain. Dans ce contexte, les ontologies comme un composant indispensable aux plateformes des applications de l'Internet des Objets visent à décrire des concepts qui sont des représentations mentales plus ou moins partagées [Nonita et al. (2021), Paulo et al. (2021), Xing et al. (2021), Khan et al. (2018), Gheisari et al. (2021)].

1.8 Contexte de la thèse

La confidentialité des données et la surveillance de l'accès physique/virtuel à l'espace ou aux connaissances sensibles font partie des nombreux défis auxquels sont confrontés les concepteurs de systèmes distribués. Par conséquent, la sécurité et la gestion dynamique des connaissances sont au cœur du processus de développement d'applications IdO. Le manque d'interopérabilité et de protection de la vie privée peuvent mettre en danger l'adoption du paradigme IdO.

La coordination des sociétés de sécurité privées, des services d'ambulance, des hôpitaux et des supermarchés est de plus en plus nécessaire, voire vitale, pour des missions allant de la prévention et de la sécurité au quotidien à la gestion d'évènements exceptionnels (urgences ou crises majeures). Le principe de la politique d'accès dans les environnements omniprésents soulève une question fondamentale : doit-on fusionner toutes les politiques pour tous les domaines (c'est-à-dire les organisations) ? En effet, chaque domaine utilise différents concepts pour spécifier des politiques

de sécurité définies selon différents vocabulaires et interprétations des actions de contrôle de sécurité. Nous considérons qu'une politique centrale n'est pas pratique car chaque organisation a sa propre politique de sécurité privée en termes de rôles, d'autorisations et de règles d'accès. Plusieurs technologies ont été proposées pour améliorer le contrôle d'accès. eXtensible Access Control Markup Language (XACML2), tout comme XML, est considéré comme le langage de balisage le plus populaire pour spécifier les mécanism-es de contrôle d'accès pour la gestion des politiques. En s'appuyant sur XACML, les systèmes de sécurité devraient atténuer les conflits et l'hétérogé-néité entre les politiques de contrôle. Néanmoins, puisque XML n'est pas un langage de représentation d'ontologies, XACML ne peut pas répondre aux connaissances sémantiques nécessaires pour autoriser les applications à améliorer les effets interprétables par ordinateur.

En tant que technologie émergente, Blockchain est livré avec des outils pour protéger les données personnelles sensibles et résoudre les problèmes de fiabilité en fournissant une architecture de communication sécurisée dans la conception d'applications distribuées (par exemple, Industrie 4.0, Santé, etc.). De nombreux systèmes traditionnels de protection de la vie privée stockent les données dans le serveur centralisé pour s'assurer que les données ne sont pas divulguées. De plus, la cryptographie à clé publique ne peut pas être appliquée à toutes les couches en raison des contraintes de puissance de calcul imposées par les appareils IdO. Tandis que les technologies Blockchain proposent le concept de Smart Contracts 'SM' (règles et actions basées sur des scénarios prédéfinis). Le SM s'exécute automatiquement à l'aide d'informations contextuelles répliquées sur le réseau, offrant une plus grande autonomie requise dans de nombreux environnements IdO ouverts et dynamiques, tels que la domotique, l'industrie 4.0, la robotique, la santé, et supprime, par conséquent, le besoin d'un tiers de confiance centralisé pour agir comme intermédiaire. Étant donné que les appareils sont soumis à des contraintes énergétiques, utiliser la technologie Blockchain Hyperledger Fabric (HF) autorisée [9] devient plus adaptée. Des applications Blockchain autorisées accordent des autorisations d'écriture à un pair prédéfini ou à un ensemble de pairs. Ce qui peut apporter certains avantages aux

9. https://www.hyperledger.org/use/fabric

mécanismes d'autorisation et d'authentification, tels que la récupération de clé, et peut également contribuer à simplifier le problème de la confidentialité et à réduire la latence des transactions. En effet, HF permet d'accéder et de traiter les données en temps réel, permettant ainsi de prendre instantanément les mesures adéquates pour faire face à une urgence telle qu'une action malveillante, même involontaire, peut causer des dommages au patient, et permettant une détection précoce des changements de comportement (chute, fréquence cardiaque, etc.). HF est un consortium, ce qui signifie que les participants (c'est-à-dire les organisations) sont identifiés et peuvent ne pas se faire confiance. De même, il promet une architecture d'information décentralisée, sécurisée et transparente. Cependant, la création de ces applications basées sur la Blockchain s'accompagne de nombreux défis : traiter et fusionner des informations hétérogènes provenant de divers artefacts et humains. En fait, de nombreuses recherches montrent que le partage d'informations à travers la Blockchain et le XACML et le manque d'interopérabilité peuvent compromettre l'adoption de la Blockchain dans nos systèmes socio-économiques.

La corrélation entre les évènements élémentaires est un autre aspect fondamental et décisif pour avoir une meilleure interprétation de contexte/-situation et lever toute ambiguïté avant la prise de décision (e.g., éviter de déclencher une fausse alarme) afin de s'adapter aux changements. Concevoir de tel système sensible au contexte exige une représentation conceptuelle générique à la fois des évènements statiques et dynamiques déclenchés dans le monde réel et des mécanismes de raisonnements robustes. Il n'est pas étrange que ces objectifs coïncident avec la question de la représentation des connaissances et des inférences en Intelligence Artificielle (IA), considérés pour très longtemps comme la clé pour construire un système intelligent. En effet, le traitement symbolique des connaissances est parmi les premiers objectifs recherchés par IA. Les techniques de la représentation des connaissances utilisées en IA pour décrire le monde réel via des structures symboliques sont vastes et variées : Les règles de productions, frame, réseaux sémantiques, logique des prédicats, etc. L' utilisation de l'une de ces techniques dépend à la fois de l'application et des préférences de l'utilisateur. La question est de savoir quel est le modèle de représentation à utiliser

et quel est le mécanisme de raisonnement adéquat ?

Comme en témoignent de nombreux travaux, les ontologies sont aujourd'hui parmi les meilleures solutions pour partager les connaissances, assurer une communication sécurisée qui préserve la confidentialité et les mécanismes d'authentification. De plus, elles prennent en charge l'interopérabilité sémantique à travers des réseaux hétérogènes. Récemment, la communauté scientifique souligne que la meilleure méthode pour mieux interpréter et partage les données hétérogènes doit s'appuyer sur des définitions de concepts d'ontologies. Ces dernières vont permettre une représentation des données plus expressive et un enrichissement des données brutes des capteurs avec des annotations sémantiques. Par conséquent, l'ontologie entrelacée avec des modèles et des technologies de sécurité offre un niveau d'autonomie efficace et plus élevé en partageant les données associées, résout les problèmes d'interopérabilité sémantique. Par conséquent, la meilleure approche pour améliorer la gestion sécurisée et sémantique des connaissances distribuées consiste à créer un lien sémantique entre les données numériques de bas niveau issues des systèmes de perception avec des représentations sémantiques de haut niveau de l'ontologie. Pour remplir ces objectifs, cette thèse se focalise essentiellement sur :

1. Le post-traitement des informations du capteur. Un modèle ontologique doit considérer à la fois l'aspect « statique » (objets physiques) et « dynamique » (évènements et situations). Il s'agit ici de mettre en œuvre un processus d'ancrage des concepts définis dans des ontologies avec les entités présentes dans l'environnement réel.
2. La conception d'architecture pour les systèmes de raisonnement et de décisions. L' objectif est d'offrir une interopérabilité et une abstraction élevées des entités, avec des mécanismes de transmission sécurisée d'évènements/de connaissances, et de garantir leur confidentialité. Plus précisément, il s'agira d'un système intégré de surveillance intelligente des actifs physiques et numériques et de la sécurité et de la sûreté personnelle.
3. Assurer l'intégrité des données : Grâce à la plateforme HF, chaque entité possède sa propre identité Blockchain, qui assure l'intégrité du message et de l'authentification, et préserve les connaissances privées.

Comme sera présenté dans le chapitre suivant, le langage d'ontologie (OWL) est de facto une solution la plus couramment utilisée pour exprimer des connaissances dans applications IdO. Ainsi, de nombreuses applications distribuées, reposant sur OWL, ont été implémentées. Même si ces approches offraient quelques extensions et un module intégré pour enrichir la sémantique standard du web, leur principale faiblesse consistait à générer des descriptions de connaissances redondantes. De nombreux scénarios, tels que ceux implémentés en cours de cette thèse, nécessitent une structure n-aire qui exprime les actions/évènements et les propriétés temporelles. Cependant, OWL et ses variantes n'ont répondu à aucune proposition concernant la notion n-aire. Ainsi, l'ensemble du langage Web sémantique devient inadapté pour intégrer des dispositifs IdO hétérogènes et répondre aux exigences de gestion dynamique des connaissances dans les applications IdO.

1.9 Notre approche

Pour faire face à ces problèmes, nous proposons de combiner le Modèle de politique de sécurité basé sur XACML avec des règles sémantiques fondées sur le modèle cω-Model (modèle basé sur l'hypothèse du monde fermé). Ce modèle a été développé durant le projet SembySem ([10]). De plus, le paradigme Unique Name Assumption (UNA) sur lequel est fondée cω-Model permet à n'importe quel objet dans le monde réel d'être ancré de manière unique dans la base de connaissances en tant qu'objet en utilisant une seule instance d'un modèle cω-Model décrivant cet objet. Par exemple, supposons qu'il y ait trois caméras intelligentes à l'intérieur de la maison. Dans ce cas, trois instances du concept SmartCamera seront instanciées dans l'ontologie, et chaque sortie SmartCamera est également unique. Contr-airement à OWL, le système ne peut pas différencier entre ces caméras du fait qu'OWL ne permet pas d'idtentfier de manière unique des objets. C'est-à-dire que deux noms différents peuvent faire référence à la même caméra. Ainsi, l'identifiaction qu'est une caractéristique importante en IdO n'est pas garantie par OWL.

10. https://itea4.org/project/sembysem.html

Par ailleurs, le modèle XACML offre un bon niveau d'abstraction et fournit des structures restreintes pour exprimer des politiques de sécurité.

Néanmoins, l'accès XACML à des systèmes de contrôle présentent de nombreux défis, comme par exemple, aucune sensibilité aux paramètres d'exécution de l'authentification et n'aborde pas la question sémantique. Pour ces raisons et pour une meilleure performance du langage XACML, nous proposons de s'appuyer sur une ontologie pour améliorer la gestion des accès et intégration des politiques dans chaque domaine sans créer de dépendances entre les domaines en termes du contrôle d'accès. Pour ce faire, nous mettons en place une ontologie qui représente les concepts de niveau supérieur de chaque domaine. Nous explorons le potentiel d'une représentation symbolique de haut niveau modèle appelé cω-Model et le langage de règles sémantique.

La seconde contribution consiste à entrelacer un modèle d'ontologie avec la technologie Blockchain. Ainsi défini, ce modèle permet une représentation narrative des évènements et établit des relations sémantiques implicites (e.g., causalité) entre les évènements observés dans l'environnement. Plus précisément, il modélise les interdépendances entre contextes et exprime des connaissances telles que : qui est l'initiateur de l'évènement/action ?

L' objectif est d'enrichir l'interprétation du contexte pour assurer une meilleure adaptation. Cette approche repose sur deux types d'ontologies du langage de représentation des connaissances narratives (NKRL) : une ontologie binaire connue sous le nom de HClass et une structure n-aire connue sous le nom de hiérarchie temporelle (HTemp), [Zarri (1997)]. Cette dernière utilise des prédicats et des rôles sémantiques pour représenter des connaissances dynamiques portant sur les évènements liés au contexte qui ont été observés. Ainsi, un concept défini dans une ontologie HClass devient identifiable à partir des données fournies par les capteurs. De plus, basé sur des principes de cryptographie, la Blockchain sécurise par exemple l'accès à la caméra embarquée du robot pour permettre au personnel hospitalier d'évaluer l'état de santé du patient pendant l'attente des ambulanciers.

Chapitre 2

IdO pour la protection de l'environnement & le bien-être des usagers : État de l'art

2.1 Introduction

Nous présentons dans ce chapitre un état de l'art sur les systèmes de sécurité et de protection de la vie privée des usagers. Nous discutons les approches de conceptions pensées pour la conception des plateformes pour assurer l'accès sécurisé aux ressources des appareils de l'IdO et sécuriser l'échange de données. N'empêche que, nous avons soulevé des questions en matière de l'applicabilité des langages d'ontologie tels qu' OWL. En effet, Le processus d'autorisation dans des environnements IdO distribués hétérogènes est plus complexe que l'autorisation d'utilisateurs dans des environnements homogènes [Riad et al. (2021)]. Néanmoins, des dispositifs IdO sont limités en énergie et ne fournissent pas la puissance de calcul. Cela rend les applications IdO plus difficiles à adopter pour la sécurité, la confidentialité et les mécanismes de contrôle d'accès existants conçus pour les systèmes distribués.

2.2 Plateformes d'authentification et de contrôle d'accès

Une authentification efficace et un schéma d'autorisation basé sur les technologies ABAC et la technologie Blockchain pour des applications IdO

ont été proposés. Dans ce qui suit, nous allons présenter les approches fondées sur XACML/ABAC, les technologies Blockchain et nous allons terminer avec les plateformes sémantiques basées sur les ontologies.

2.2.1 Approches fondées sur XACML & ABAC

Pour maintenir la cohérence dans des environnements dynamiques, les auteurs [Daniel et al. (2015)] proposent un moyen de gérer les politiques XACML distribuées. Ils identifient qu'un domaine de sécurité peut se voir accorder un niveau d'autonomie pour gérer ses ressources localement. Les politiques d'un autre domaine qui se concentrent sur les ressources locales devraient être restreintes d'une certaine manière. Les auteurs réutilisent l'architecture XACML pour gérer les privilèges sur les politiques distribuées via des Meta-Policies qui peuvent économiser du temps et des efforts dans la mise en œuvre et le déploiement d'une nouvelle architecture de contrôle d'accès. De plus, grâce à l'expressivité de XACML et de ses profils (appliqués dans les Meta-Policies), il est possible de définir correctement les privilèges et de garantir la vie privée des politiques et des attributs dans chaque domaine de sécurité. Les auteurs étendent XACML avec un mécanisme basé sur Security Assertion Markup Language (SAML) qui inclut des protocoles et des assertions, et inclut en même temps un mécanisme de sécurité lié à l'authenticité et à la validité des requêtes et des réponses. Tandis que [Panende et al. (2018)] comparent deux modèles de contrôle d'accès utilisés comme solutions pour le contrôle d'accès Digital Evidence Storage (DES), à savoir Rule Based Access Control (RBAC) and Attribute-Based Access Control(ABAC). Les auteurs utilisent XACML comme langage de programmation pour spécifier la politique RBAC et ABAC à l'aide du format XML. Les deux modèles de contrôle d'accès sont des solutions de l'autorisation limitée et de l'authentification des utilisateurs qui ont été appliquées au système DES. Les tests fonctionnels qui ont été effectués à l'aide d'outils spéciaux conçus pour tester RBAC et ABAC montrent que le modèle de contrôle d'accès qui convient pour être appliqué au DES est le modèle ABAC en raison de sa nature extrêmement granulaire et flexible.

Afin d'introduire la surveillance en temps réel de paramètres importants

tels que la température, la luminosité, l'humidité et la concentration de gaz dans les chambres froides, les auteurs dans [Afreen et al. (2021)] ont présenté un système intelligent nommé Real-Time Monitoring and Notification System (RT-MNS). L' aide à la décision est mise en œuvre dans le RT-MNS à l'aide d'un réseau de neurones artificiels (ANN) avec propagation vers l'avant pour classer l'état du produit dans l'une des trois classes, c'est-à-dire bon, insatisfaisant ou alarmant. Sur la base des certificats d'attribut utilisateur, un droit d'accès est accordé par l'autorité de contrôle d'accès. Cependant, la spécification d'une définition cohérente des attributs au sein d'un domaine ou dans différents domaines pourrait augmenter considérablement l'effort et la complexité de la gestion des politiques à mesure que le nombre d'appareils augmente, et par conséquent, la proposition n'est pas adaptée aux applications distribuées à grande échelle.

D'autres propositions basées sur ABAC, XACML ont donné naissance à de nombreuses plateformes [Javier (2017), Morisset et al. (2019), Gang et al. (2021), Nimalaprakasan et al. (2018)]. Certainement le paradigme ABAC attire de plus en plus l'attention des chercheurs et des industriels en raison de sa flexibilité, de son évolutivité et de son expressivité. Toutefois, l'approche de traitement des informations manquantes adoptée par les mécanismes ABAC standards existants (par exemple, basée sur XACML) est défectueuse, ce qui rend l'évaluation des politiques ABAC vulnérable aux attaques par dissimulation d'attributs. [Javier (2017)] ont proposé un système conçu pour une authentification mutuelle efficace basée sur un protocole d'établissement de clé sécurisée. De plus, l'accès aux données dans cette approche est basé sur des certificats d'attributs d'utilisateur qui assurent un contrôle d'accès précis. Néanmoins, ce modèle implique une gestion complexe, où chaque entité doit mettre à jour les attributs pour maintenir une autorisation continue avant, pendant et après l'autorisation d'exécution d'accès, ce qui n'est pas adapté pour être appliqué à des dispositifs contraints. Pour résoudre le problème des informations manquantes, les auteurs dans [Morisset et al. (2019)] ont appliqué des structures de données basées sur Binary Decision Diagram (BDD) pour la représentation des politiques ABAC. Les auteurs ont analysé leur travail avec trois politiques, à savoir la politique CONTINUE, la politique KMarket et la politique SAFAX. Les politiques CONTINUE

et SAFAX sont spécifiées en XACML v2 (OASIS 2005) tandis que la politique KMarket est exprimée en XACML v3 (OASIS 2013). La cible de la politique CONTINUE est définie sur 14 attributs allant du rôle des utilisateurs au sein du système de gestion de conférence, l'action pour laquelle l'accès est demandé aux attributs utilisés pour caractériser l'existence de conflits d'intérêts et l'état du processus d'examen. La politique SAFAX est utilisée pour réglementer les actions que les utilisateurs peuvent effectuer sur l'interface Web. La politique de KMarket est utilisée pour vérifier si un achat est autorisé. [Nimalaprakasan et al. (2018)] proposent quant à eux, une extension du langage de politique de contrôle d'accès fondée sur XACML, avec des types de données et des fonctions spécifiques au Building Information Model (BIM) basés sur la spécification IFC (Industry Foundation Classes), appelée "BIM-XACML". Un modèle sémantique (il ne s'agit pas d'une ontologie) est fourni pour les types de données et les fonctions nécessaires à un système de contrôle d'accès utilisant des modèles d'informations sur le bâtiment. Enfin, [Gang et al. (2021)] pensent que la plupart des méthodes de détection de conflits ne pouvaient pas détecter statiquement les conflits implicites en raison de l'absence des attributs dans les règles. Afin de résoudre ce problème, une méthode pour transformer les règles conflictuelles implicites en règles conflictuelles explicites par la complétion d'attributs est proposée. Les auteurs utilisent l'algorithme de détection de règles en conflit probable amélioré pour détecter toutes les règles en conflit probable dans la politique XACML et analysent la probabilité du conflit. Dans la même perspective sémantique que [Nimalaprakasan et al. (2018)], les auteurs dans [Rezvani et al. (2019)] ont proposé un mécanisme structuré pour traduire une politique XACML en un programme Answer Set Programming (ASP) qui prend en charge à la fois XACML 2.0 et 3.0 et exploite un outil d'analyse de politique mis en œuvre au-dessus de l'ASP Clingo. Leur objectif est de vérifier les propriétés d'une politique XACML, y compris l'analyse des requêtes, la détection des anomalies (redondance et conflit), l'accessibilité, l'utilité, la complétude, la subsomption, le morphisme et la disjonction. La figure 2.1 montre le cadre d'analyse des politiques. La couche supérieure de ce cadre contient trois modules pour traduire les composants XACML en programmes ASP. Une approche de traduction modulaire qui aide à spécifier les politiques XACML,

les requêtes et les algorithmes de combinaison dans des programmes ASP séparés sont développés. Comme résultats de la traduction de la couche supérieure, trois programmes ASP contenant la traduction d'une politique XACML ont été définies. Notez que la transformation définit une sémantique formelle de XACML en termes de sémantique ASP. Dans la couche intermédiaire de ce cadre, chaque propriété de politique en tant que programme ASP est spécifiée. Le programme de propriété ainsi que les résultats de la traduction sont envoyés à un solveur ASP pour vérifier la satisfaisabilité de la propriété sur la politique. Les résultats finaux fournissent des preuves de la satisfaisabilité de chaque propriété sous la forme d'ensemble de réponses générées par le solveur.

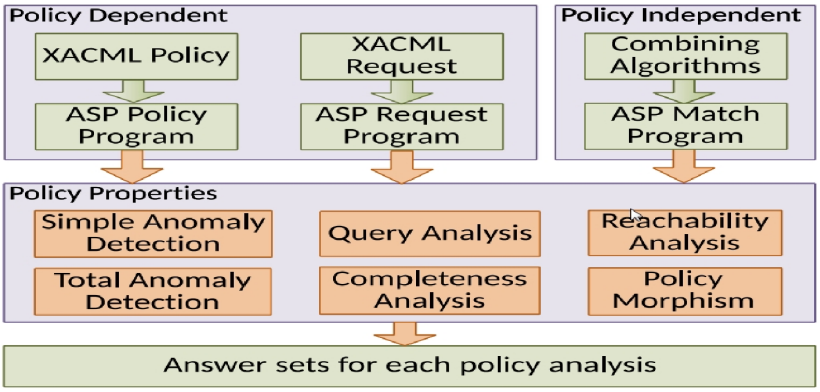


FIGURE 2.1 – Cadre d'analyse des politiques avec ASP, [Rezvani et al. (2019)].

De surcroît au contrôle d'accès, d'autres propositions s'intéressent également à la protection de la vie privée [Al-Zubaidie et al. (2019), Shantanu et al. (2019), Turkmen et al. (2017), Rezvani et al. (2019), Kanwal et al. (2021), Damiano et al. (2019), Arunkumar et al. (2017), Panende et al. (2018), Daniel et al. (2015)]. De nombreuse propositions pour la conception de systèmes dédiés en santé pour la gestion de la vie privée dans Electronic Health Record (EHR) et les problèmes de décision d'accès sécurisé pour les données des patients ont été proposées par exemple par [Al-Zubaidie et al. (2019), Kanwal et al. (2021)]. Le système Pseudonymization and Anonymization with the XACML (PAX) est proposé par [Al-Zubaidie et al. (2019)]. Les auteurs utilisent un pseudonyme aléatoire pour séparer les informations personnelles des données des patients, l'anonymat pour masquer les informations des

sujets et le XACML 3.0 pour créer des politiques de contrôle d'accès distribuées pour autoriser les demandes des sujets aux dossiers des objets dans l'EHR. Les auteurs adoptent le schéma Shamir avec les signatures Elliptic Curve Digital Signature Algorithm (ECDSA) pour augmenter le niveau de sécurité pour les utilisateurs indirects. Ils créent un ensemble de quatre bases de données pour améliorer la vie privée. Deux bases de données sur Attributes Server (AS), le premier contient les attributs des patients et le second contient les pseudonymes ; le troisième contient les politiques des utilisateurs et le dernier sur le Data Server (DS) qui contient les données des utilisateurs. Lorsqu'un nouvel utilisateur est ajouté au système, son pseudonyme contient un rôle d'utilisateur et un numéro d'utilisateur interne généré de manière aléatoire. Ceux-ci ne sont pas transmis et sont plutôt utilisés à des fins de vérification. Étant donné que ces pseudonymes sont liés aux utilisateurs, ils peuvent être utilisés pour afficher les données des utilisateurs sans dépasser les privilèges. Il existe 7 différents types de protocoles d'autorisation dans ce modèle, 4 protocoles pour les utilisateurs directs et 3 protocoles pour les utilisateurs indirects, figure 2.2. AS évalue la demande d'accès par les modules PDP (PDP1 et PDP2), vérifie les signatures, les pseudonymes et autres paramètres de sécurité. Si toutes les évaluations et tous les tests sont valides, AS envoie une demande à DS pour récupérer les données du patient. Après une vérification réussie des signatures (Sigs) et des Privacy Parameters (PP), DS envoie les données requises avec des pseudonymes et des Sigs à AS qui à son tour envoie la réponse «permis» au client pour autoriser l'accès à l'ensemble de données.

Comme illuster par la figure 2.3, le modèle PRSX-AC proposé par [Kanwal et al. (2021)] quant à lui, fonctionne selon les étapes suivantes : Tout d'abord, health-care organization (HCO) télécharge les données EHR d'origine sur le cloud privé. Les utilisateurs de domaine (ODU, PRDU, PBDU) envoient une demande d'accès EHR au PEP. Les auteurs s'appuient également sur des réseaux de Petri de haut niveau (HLPN) et le langage Z [1] pour la modélisation et l'analyse du modèle proposé. Les résultats expérimentaux montrent que dans le modèle proposé, les politiques d'accès basées sur les relations et

1. La langage Z a été développé à l'Université d'Oxford par Jean René Abrial. Z est un langage formel qui utilise les notions ensemblistes, le calcul des propositions, des prédicats, des fonctions, les séquences.

l'anonymisation des dossiers de santé électroniques peuvent bien fonctionner en termes de temps de réponse des politiques d'accès et d'espace de stockage.

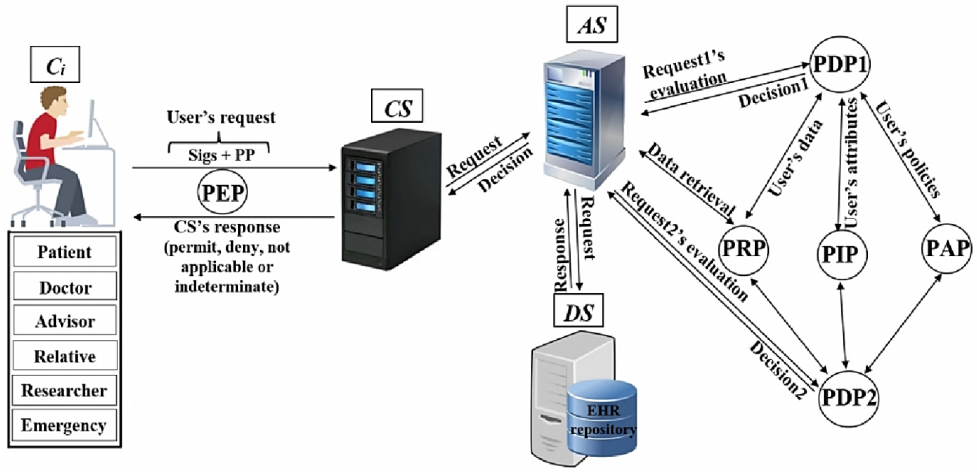


FIGURE 2.2 – Le modèle Pseudonymisation et anonymisation avec XACML (PAX), [Al-Zubaidie et al. (2019)].

[Shantanu et al. (2019)] quant à eux, proposent un modèle d'architecture de contrôle d'accès partiellement décentralisé pour les ressources médicales restreintes dans des applications IdO. Pour ce faire, ils utilisent une approche hybride en combinant les attributs, les rôles et les capacités pour leur conception. Dans cette proposition, les appareils IdO peuvent prendre eux-mêmes des décisions d'autorisation sans dépendre d'une autorité centralisée. Lorsqu'un utilisateur demande l'accès à une ressource, il doit fournir certains attributs pour prouver son identité. Une fois satisfait, l'accès est accordé aux entités autorisées pour accéder aux ressources avec un minimum de spécification de politique, figure 2.4. Le CMS se compose des modules de base suivants : RM est responsable de l'appariement de l'appartenance au rôle en fonction des attributs ; CG est chargé de générer des capacités pour les réponses XACML positives ; PMU dispose de l'architecture XACML standard pour fournir une solution multiplateforme tout en satisfaisant l'interopérabilité ; et Database Servers incluent l'UAD qui stocke les attributs de l'utilisateur, le PD qui stocke les politiques sous la forme de politiques XACML sérialisées et les métadonnées associées, le CD qui stocke les modèles de capacité et le TD qui stocke les attributs des TH activés et déployés.

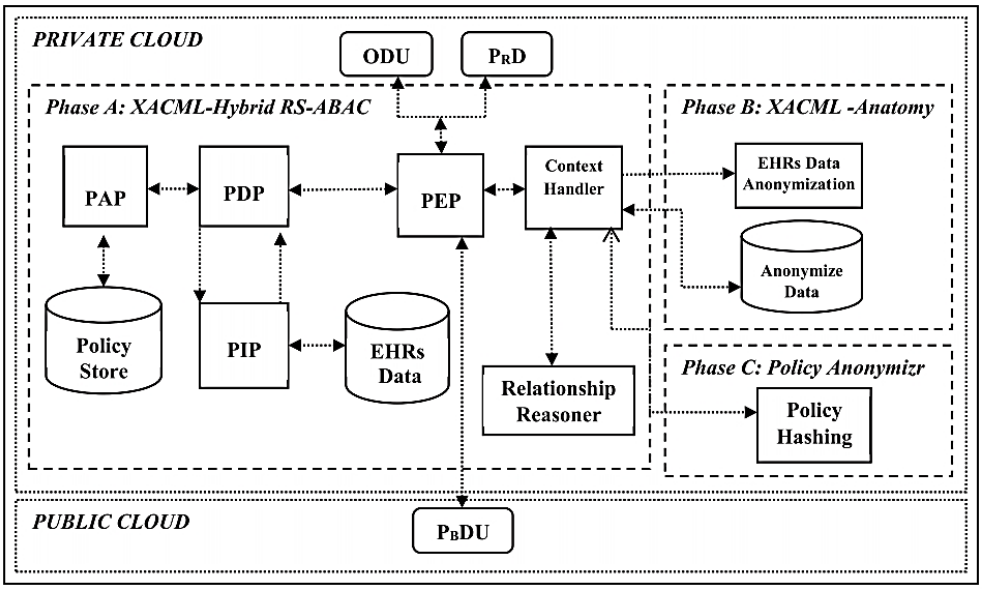


FIGURE 2.3 – Schéma fonctionnel du modèle de cloud hybride PRSX-AC, [Kanwal et al. (2021)].

Pour finir avec des approches fondées sur XACML et ABAC étudiées dans cette thèse, nous présentons respectivement les deux propositions [Deng et al. (2020), Arunkumar et al. (2017)]. Dans la première proposition, les auteurs proposent un moteur d'évaluation de politique pratique, à savoir CSRM (Clustering and Supervised Response Mechanism), pour éliminer les goulots d'étranglement causés par des ensembles de politiques à grande échelle et des requêtes intensément abondantes. Les auteurs utilisent CK-means pour obtenir un meilleur résultat de regroupement dans la couche de politique. La seconde proposition quant à elle, propose Geospatial XACML (GeoXACML) pour le contrôle d'accès géospatial. Deux extensions d'attribut principales sont utilisées : GeoPoint et GeoPolygon. Un attribut GeoPoint représente un point particulier qui stocke une latitude et une longitude tandis qu'une instance GeoPolygon représente une région ou des limites géospatiales, par exemple, un bâtiment ou une chambre, en stockant plusieurs GeoPoints. En plus de ces extensions d'attributs, une fonction geo-contains est chargée de vérifier si l'emplacement du demandeur se trouve dans une région définie par l'objet geoPolygon et un GeoHashing. Avec ces extensions d'attribut, le demandeur peut envoyer l'emplacement actuel avec la demande d'accès au PDPvia XACML. Le PDP vérifie les politiques géospatiales pour décider si

le demandeur est autorisé à l'accès demandé ou non. Une fois l'accès autorisé, Policy Enforcement Point (PEP) fournit la ressource demandée. Les auteurs décrivent également une étude de cas dans le contexte des services de santé où le contrôle d'accès aux appareils portables est modéré en fonction de l'emplacement de l'appareil.

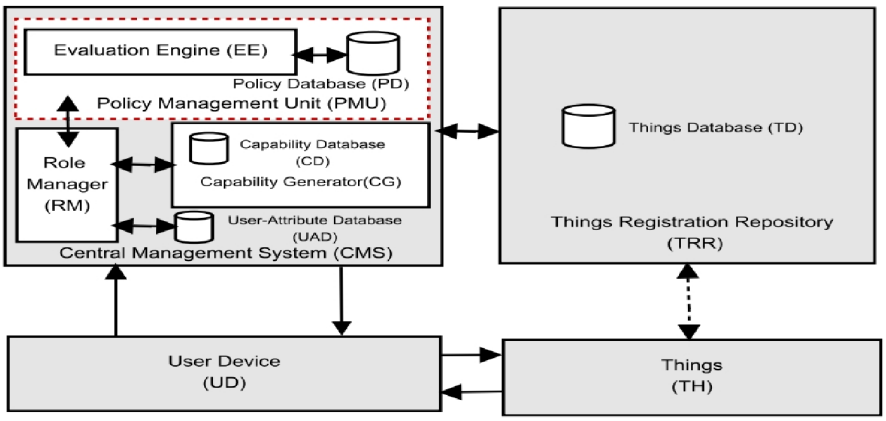


FIGURE 2.4 – L' architecture de contrôle d'accès proposée, [Shantanu et al. (2019)].

2.2.2 Approches fondées sur la technologie Blockchain

Les chaînes de blocs ont gagné en popularité auprès des chercheurs universitaires et industriels travaillant dans la conception d'applications distribuées. Dans ce contexte, nous pouvons citer les travaux de [Li et al. (2019), Reyna et al. (2018), Abunadi et al. (2021), Nguyen et al. (2019), Huang et al. (2019), Bodkhe et al. (2020)].

Les technologies Blockchain garantissent la disponibilité sécurisée des informations sur les réseaux peer-to-peer sans intermédiaire. Malgré ces travaux, [Kim et al. (2018)] ont souligné qu'il n'y a pas eu beaucoup de travaux qui examinent la Blockchain et les ontologies. Ils ont décrit et analysé certains résultats de recherche sémantique utilisés pour construire une Blockchain sémantique. Dans le cadre des soins médicaux, les auteurs [Dwivedi et al. (2019)] proposent un nouveau framework (ou infrastructure logicielle en français) de modèles de Blockchain modifiés adaptés aux appareils IdO.

Cette approche repose sur des primitives cryptographiques avancées. L' objectif est de répondre aux exigences des soins médicaux indispensables basées sur les appareils IdO pour le bien être humain. Les auteurs estiment que les technologies associées à l'IdO posent de graves risques pour la vie privée et des problèmes de sécurité concernent le transfert de données et l'enregistrement des transactions de données. Ces problèmes de sécurité et de confidentialité des données médicales pourraient mettre en danger la vie du patient.

Les auteurs [Mitrevski et al. (2020), Tahir et al. (2020)] présentent une approche intelligente distribuée qui pourrait être utile dans différents scénarios IdO. [Mitrevski et al. (2020)] proposent une approche MADIT (Mobile-Agent Distributed Intelligence Tangle-Based). Tout d'abord, plusieurs agents mobiles sont employés pour répondre aux communications au niveau du nœud et collecter les données de transaction à un niveau inférieur. La principale nouveauté de l'approche est un modèle de haut niveau pour gérer les transactions, qui améliore l'évolutivité de la distribution des données pour les applications mobiles distribuées. Pour assurer l'intégrité de l'utilisateur, une plateforme légère d'authentification et d'autorisation pour le réseau IdO activé par Blockchain a été proposé [Tahir et al. (2020)]. Le protocole proposé se compose de deux services nommés applications et réseaux. Les applications IdO sont des services basés sur le cloud, comme l'assistance à la mobilité publique. Chaque entité du réseau est définie et associée à un certificat de clé publique pour authentifier l'ensemble des informations de service et obtenir l'accès aux données. L' analyse des résultats expérimentaux montre que ce cadre est robuste et hautement sécurisé, et fiable par rapport aux autres. Un autre schéma d'agrégation de données pour préserver la vie privée basée sur la Blockchain dans un réseau intelligent est proposé par [Zhitao et al. (2018)]. L' identité de l'utilisateur est masquée à l'aide du pseudonymat afin de préserver la vie privée interne au sein d'un groupe. Quant à [Akkaoui (2021)] a proposé un schéma d'authentification décentralisée pour les systèmes de santé IdO afin de minimiser l'impact des attaques par déni de service distribué sur les environnements IdO en tirant parti des fonctionnalités décentralisées de la Blockchain. L' auteur a testé le mécanisme sur la plateforme Ethereum pour l'analyse de la sécurité et de la confidentialité.

Afin de pallier au caractère centralisé des architectures, [Hang et al. (2019)] proposent une plateforme IdO intégrée utilisant la technologie Blockchain pour garantir l'intégrité des données de détection. L' objectif est de supporter une surveillance en temps réel et un contrôle entre l'utilisateur final et l'appareil. Le logique métier de l'application est définie par le contrat intelligent, qui contient des règles et des conditions.

Combiner les deux technologies Blockchain et XACML a fait objet d'études de nombreux chercheurs [Damiano et al. (2019), Liu et al. (2020), Beomseok et al. (2021), Yan et al. (2018), Xiaofeng et al. (2021), Yingwen et al. (2021), Sara et al. (2021), Afnan et al. (2020)]. Un système complet de contrôle d'accès basé sur la Blockchain implémentant ABAC a été présenté dans cet article. Cette approche adopte XACML comme langage politique et exploite la Blockchain Ethereum pour mettre en œuvre toutes les phases du processus d'évaluation des politiques. En fait, le moteur qui évalue la politique de sécurité par rapport à la demande actuelle et les gestionnaires des attributs requis pour l'évaluation de la politique sont implémentés en tant que contrats intelligents interopérables et, par conséquent, sont exécutés sur la Blockchain. Seule la phase d'écriture et de création des politiques sont effectuées hors chaîne, car la traduction des politiques de XACML en contrats intelligents Ethereum serait trop coûteuse pour être exécutée en chaîne. Dans cette approche, une politique XACML est correctement traduite en un contrat intelligent, appelé Smart Policy (SP), qui est créé par le propriétaire de la ressource et stocké sur la Blockchain par une transaction appropriée. Ainsi, les SP sont responsables du processus d'évaluation de la politique, intégrant le PDP pour une politique de contrôle d'accès spécifique et les PIP requis pour collecter les valeurs des attributs de cette politique. À chaque fois, une demande d'accès doit être évaluée pour prendre une décision d'accès, et la Blockchain l'exécute de manière distribuée. Le principal avantage de cette proposition est que les processus de gestion et d'évaluation des politiques sont exécutés sur une Blockchain, ce qui fait que leur système hérite les avantages de la technologie Blockchain, c'est-à-dire qu'il est transparent, immuable, distribué (donc pas de point unique de défaillance ou d'attaque), etc. L' aspect mobilité des appareils IdO rend difficile la prise en charge du contrôle d'accès par les méthodes traditionnelles de contrôle

d'accès centralisé dans l'environnement IdO actuel à grande échelle.

Ce constat est soulevé par de nombreux auteurs tels que [Liu et al. (2020)]. Pour relever ces défis, les auteurs proposent un système de contrôle d'accès dans l'IdO nommé fabric-iot basé sur Hyperledger Fabric et ABAC. Le système contient trois types de contrats intelligents, à savoir le contrat de périphérique (Device Contract (DC)), le contrat de politique (Policy Contract (PC)) et le contrat d'accès (Access Contract (AC)). DC fournit une méthode pour stocker l'URL des données de ressources produites par les appareils, et une méthode pour l'interroger. PC fournit des fonctions pour gérer les politiques ABAC pour les utilisateurs administrateurs. AC est le programme de base pour mettre en œuvre une méthode de contrôle d'accès pour les utilisateurs normaux.

2.2.3 Approches sémantiques pour la protection de la vie privée & contrôle d'accès

Les ontologies sont aujourd'hui le pivot dans de nombreuses applications, comme la description sémantique de ressources multimédias et d'objets physiques (selon le paradigme du Web des Objets) [Maamar et al. (2020), Wirawit et al. (2016), Nakul et al. (2021)]. Comme l'a démontré [Choudhury et al. (2018), Li et al. (2019)], les ontologies sont désormais le fondement d'un système distribué visant à répondre à l'hétérogénéité sémantique qui survient lors de l'extraction dynamique des connaissances et de l'authentification et de la gestion des accès aux ressources. Tous les auteurs visent à faciliter les processus de recherche d'informations et d'exploration de données, la mise en œuvre de services Web Sémantiques et la conception de systèmes ubiquitaires. Dans [Rafal et al. (2020), Sharma et al. (2021), Safyan et al. (2019)], les auteurs ont souligné que les ontologies pourraient servir de modèles de connaissances sémantiques dans les applications distribuées qui nécessitent de traiter des informations contextuelles, de faire un raisonnement formel et de faciliter l'échange de connaissances entre utilisateurs et utilisateurs-systèmes et entre les systèmes eux-mêmes. Les ontologies sont également associées à des mécanismes d'inférence pour automatiser le raisonnement sur ces connaissances. Par conséquent, plusieurs ontologies

ont été proposées pour implémenter la gestion sémantique des connaissances dans les applications d'intelligence ambiante et prendre en charge le raisonnement contextuel basé sur la logique.

L' aspect sécurité qui dépend des ontologies a été étudié il y a plus d'une décennie [Denker et al. (2005), Conti et al. (2018), Bradshaw et al. (2013)]. Tous les auteurs décrivent les principales questions concernant la représentation des connaissances et le raisonnement pour la sécurité dans le web sémantique. Ils insistent fortement sur le fait que les applications ont besoin d'un langage de politique déclaratif (c'est-à-dire d'ontologies et de capacités d'inférence) pour préserver la confidentialité et la confiance.

Parmi les approches pour la gestion sémantique des enregistrements médicaux des patients Electronic Medical Records (EMRs), l'approche fondée sur Web Ontology Language (OWL) proposée par [Junjian et al. (2014)]. Les auteurs avaient comme objectifs la représentation et le stockage des connaissances médicales dans un formalisme sémantiquement riche en vue de surveiller en temps réel l'état du patient et d'afficher des rappels sur les activités médicales. Le fondement sur les ontologies a fait objet récemment de nombreuses études telles que [Elsaleh et al. (2020), Kuster et al. (2020), Sai et al. (2020)]. Le modèle d'annotation sémantique des flux de données IdO proposé par [Elsaleh et al. (2020)] s'appuie sur l'ontologie Semantic Sensor Network Ontology (SNN [2]) et de son noyau léger Sensor, Observation, Sample, and Actuator (SOSA). Leur modèle d'information se concentre sur la modélisation des observations de flux et leur analyse. Ce flux est encapsulé par quatre classes : les classes IotStream, StreamObservation, Analyticsprocess et Event. IoT-Stream comprend des modules pour l'annotation, la consommation et l'interrogation des données. Comme IoT-Stream s'appuie sur SSN/SOSA, il prend également en charge la géolocalisation. IoT-Stream fournit une implémentation de leur norme, qui est disponible en ligne [3]. Quant à [Kuster et al. (2020)] ont proposé un modèle de données sémantiques pour éliminer l'hétérogénéité entre les différentes données de capteurs. Ils ont suggéré que ce modèle de données sémantiques prend en charge la durabilité urbaine presque en temps réel. L' ontologie proposée par les auteurs a la

2. https://www.w3.org/TR/vocab-ssn/
3. http://iot.ee.surrey.ac.uk/iot-crawler/ontology/iotstream

capacité d'identifier divers indicateurs de performance clé, critères, thèmes et sous-thèmes de durabilité dans un système urbain, ainsi que des capteurs et des observations de perception. Conformément à ces questions de compétence, ils ont utilisé le langage de requête SPARQL [4] pour récupérer des informations pertinentes à partir de la base de connaissances de l'ontologie. Cette nouvelle approche combine des ontologies différentes et qui sont spécifiques à un domaine dans une ontologie de haut niveau qui peut prendre en charge la création d'un logiciel d'évaluation de la durabilité urbaine en temps réel. L' ontologie proposée réutilise les ontologies existantes dans la littérature, telles que les ontologies SSN, QUDT [5] et le langage de requêtes GeoSPARQL.

Sans doute, assurer la protection de la vie privée est une préoccupation non seulement organisationnelle, mais à un niveau mondial. Cette inquiétude est révélée par les orientations relatives à la protection des données dans les villes intelligentes fournies par General Data Protection Regulation(GDPR-[6], [7]). Ces lignes directrices sont véhiculées par la norme ISO/IEC TS 27570 [8]. Cette norme ne couvre pas toutes les exigences du GDRP en ce qui concerne le cycle complet des données, elles se sont concentrées uniquement sur les phases de collecte et de partage des données. Dans le même contexte de GDPR, les auteurs [Serrano et al. (2018)] ont mis à jour l'ontologie FIESTA-IoT pour inclure des concepts permettant l'interopérabilité, la fédération et l'expérimentation et se conformer à la nouvelle version de l'ontologie SSN.

L' ontologie [9] proposée améliore l'aspect respect de la vie privée, permet l'interopérabilité sémantique et prend en charge le développement d'applications IdO préservant la vie privée. Qaunt aux auteurs dans [Bríoring et al. (2017)] n'ont pas précisé quel langage d'ontologie utilisé, toutefois, ils ont proposé une interface de programmation d'application nommée Bridging the Interoperability Gap of the IoT (API BIG IoT). Cette dernière définit une structure de base générique, qui peut être instanciée par annotation avec des

4. https://www.w3.org/TR/rdf-sparql-query/
5. https://www.qudt.org/pages/QUDToverviewPage.html
6. https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
8. https://www.iso.org/fr/news/ref2631.html
9. https://github.com/fiesta-iot/ontology/blob/master/fiesta-iot.owl

termes d'un vocabulaire sémantique. Selon les auteurs, contrairement à un langage, une API reste mince et facile à comprendre tout en étant générique et applicable dans différents domaines.

Les approches de sécurité entrelacées avec les ontologies ont été proposées par de nombreux auteurs, tels que [Sai et al. (2020),Toumia et al. (2020)]. [Sai et al. (2020), Shulong et al. (2016), Gheisari et al. (2021)] ont proposé un écosystème de ferme intelligente avec trois modules fondés sur une ontologie pour le contrôle d'accès. Le premier module présente une architecture à trois couches pour l'agriculture intelligente : couche d'entité physique, couche de jumeau numérique et couche d'interactions. La couche d'entité physique se compose d'une Farm Based Unit (FBU) avec des dispositifs fixes tels que des capteurs placés sur le terrain, d'une On Board Unit (OBU) avec des dispositifs mobiles sur le terrain, d'une Worker Based Unit (WBU) qui représente les ressources humaines sur le terrain et d'une Home Based Unit (HBU) qui connecte toutes les unités au cloud via un hub de passerelle. Le module de jumeau numérique se compose des représentations virtuelles de toutes les entités physiques pour surveiller le flux de données. Le module interactions définit toutes les interactions possibles entre les entités physiques et les stocke dans un graphe de représentation. Sur la base de cette architecture, un certain nombre de cas d'utilisation pour les autorisations de lecture, d'accès et d'exploitation sont définis pour le contrôle d'accès qui est décidé dynamiquement en fonction des attributs de l'entité.

L' ontologie ColPri, développée avec OWL et utilise le vocabulaire Simple Knowledge Organization System (SKOS [10]) proposé par [Toumia et al. (2020)]. Cette ontologie vise à fournir une base de connaissances des appareils IdO collaboratifs permettant de configurer des politiques d'accès et le respect de la vie privée. De plus, l'ontologie permet de spécifier si la divulgation d'informations à des entités telles que des développeurs et des tiers est autorisée. En ce qui concerne les données personnelles, ColPri suit SKOS et modélise différentes catégories de données telles que les données personnelles, pseudo-anonymes et anonymes. Les données personnelles pourraient en outre être spécifiées comme sensibles (par exemple, des criminelles, de santé, d'habitude et d'identité) et non sensibles. ColPri diffère des autres

10. https://www.w3.org/2004/02/skos/

ontologies en utilisant à la fois OWL et SKOS. L' ontologie peut être utilisée pour modéliser les préférences de la vie privée des données dans les villes intelligentes, en particulier dans les maisons intelligentes.

[Shulong et al. (2016)] ont proposé Ontology-based Resource Description Model (ORDM) afin de décrire les ressources dans l'environnement IdO. La classe Attribut définit les informations inhérentes à l'appareil, telles que le type d'appareil, le modèle et la plage des valeurs détectées. La description des données est faite dans la classe State, qui fournit les données courantes capturées par le capteur avec leur unité de données associées. La classe de la vie privée protégeait l'appareil contre tout accès ou contrôle illégal. Une application bureautique intelligente basée sur l'ORDM est implémentée pour l'évaluation. Cependant, l'ORDM n'offrait pas de contrôle d'accès précis aux données détectées. En effet, les utilisateurs pouvant accéder à la ressource IdO sont fixés dans l'ontologie proposée sans aucun raisonnement ni critère clair. De plus, les auteurs n'ont pas traité du partage des ressources de données pendant la phase de traitement des données.

Les auteurs [Gheisari et al. (2021)] ont proposé un cadre de Ontology-based Privacy-Preserving (OBPP) pour assurer la préservation de la vie privée des appareils IdO, fournir des services de haut niveau et traiter l'hétérogénéité entre les différents appareils en même temps. Le premier module comprend une ontologie, un modèle de stockage de données, pour résoudre le problème d'hétérogénéité tout en conservant les informations de confidentialité des appareils IdO et en apportant une sensibilité au contexte. Le second « Reasoning Engine» contient des règles de raisonnement sémantique pour trouver des modèles anormaux tout en abordant la qualité des services fournis et en prenant des décisions de haut niveau. Le troisième module «OBPP Procedure» fournit un gestionnaire de règles de confidentialité pour relever les défis de préservation de la vie privée des appareils IdO réalisés en modifiant dynamiquement les comportements de la vie privée des appareils. Les auteurs [Schwee et al. (2019)] ont proposé une méthode pour identifier les risques potentiels pour la vie privée lors du traitement des flux de données de capteurs et pour informer sur les possibilités spécifiques d'inférence et de liaison de données avant de partager les données. Cette méthode introduit une ontologie avec les concepts nécessaires pour modéliser les risques

de la vie privée pour les données d'entrée. L' ontologie peut être utilisée par un expert du domaine pour modéliser un ensemble de données. Identifier les transformations pouvant être appliquées sur ces classes de données, et enfin, déduire d'autres types de flux de données associés. Quant aux auteurs dans [Mitrevski et al. (2021)] ont proposé et analysé une stratégie pour généraliser des modèles d'exécution paramétrés d'actions de manipulation sur différents objets basés sur l'ontologie des objets. Ils utilisent une ontologie O = (T ; A) pour la généralisation sur les objets, où T est la TBox, qui encode les définitions de classes d'objets, les relations entre ces classes, ainsi que les définitions de propriétés d'objets, et A est l'ABox, qui consiste en des assertions de classes et de propriétés, à savoir les objets terrestres qui appartiennent à des classes d'objets spécifiques et les propriétés de ceux-ci, respectivement. Les auteurs ont vérifié leur algorithme pour deux actions – saisir et ranger des objets du quotidien – de sorte qu'ils ont montré que le robot peut déduire des cas où une politique existante peut se généraliser à d'autres objets et où des connaissances d'exécution supplémentaires doivent être acquises.

Dans le contexte des villes intelligentes, les auteurs [Drozdowicz et al. (2020)] proposent un cadre de contrôle d'autorisation et de la vie privée basée sur des technologies sémantiques. Ce cadre permet à l'utilisateur de maintenir des politiques de contrôle d'accès aux données. Ils proposent un système autogéré pour garantir les préférences de la vie privée de l'utilisateur. Ils ont dérivé un nouveau vocabulaire sémantique basé sur d'autres ontologies de domaine (suivi de la condition physique, soins de santé, données de capteurs, etc.). De plus, ils ont intégré certains des vocabulaires clés dérivés dans les politiques XACML avec un raisonnement sémantique pour offrir une approche ABAC raffinée et flexible pour les applications de suivi de la condition physique. De ce fait, les utilisateurs ont la possibilité de formuler des préférences de la vie privée en utilisant le vocabulaire sémantique dérivé (domaine) pour contrôler l'accès dans des environnements intelligents. Cette dernière décrit et relie les concepts importants de sécurité et de vie privée dans le domaine de la santé en ligne. Le Semantic PIP fonctionne comme suit : lorsque le gestionnaire de contexte demande des valeurs d'attributs, le SemanticPIP crée des concepts OWL et des individus OWL pour les attributs

de sujet, d'objet, d'action et d'environnement qui existent dans la requête. Il convertit également les valeurs d'attribut existant dans la demande en axiomes de propriété de données des types appropriés. En d'autres termes, il traduit une demande d'accès en une ontologie. Ensuite, il fusionne l'ontologie construite avec l'ontologie de domaine et utilise un raisonneur sémantique pour obtenir des informations supplémentaires (attributs sémantiquement pertinents). Après cela, il récupère les valeurs d'attributs en émettant des requêtes SPARQL sur l'ontologie pour les propriétés reconnues par le raisonneur. Enfin, il renvoie les valeurs d'attribut récupérées au context handler. Ce context handler met à jour la demande en ajoutant les informations déduites et l'envoie au PDP, qui prend une décision basée sur les politiques XACML et la demande est mise à jour. Bien que la stratégie de résolution des conflits n'ait pas été déterminée, nous supposons que le schéma de Drozdowicz et al. abordent la résolution des conflits de la même manière que la norme XACML.

Nous terminons notre étude de l'état de l'art par le langage Knowledge-Aware Operational Support (KAoS) [Bradshaw et al. (2013)] et Rei [11].

Par ailleurs, le tableau 2.1 résume les langages et les technologies utilisés en recherche pour la protection de la vie privée et le contrôle d'accès. KAoS est un langage de représentation de politique basé sur OWL. Il applique les politiques établies dans plusieurs domaines par la gestion des spécifications et la résolution des conflits. Les ontologies de politique KAoS décrivent les situations, les actions et la ressource à protéger (c'est-à-dire la cible) associée à l'acteur (c'est-à-dire le sujet). Pour agir en tant que point de décision politique, KAoS fournit un moyen de déterminer si un agent est autorisé à rejoindre un domaine externe. Rei est une ontologie de sécurité et de confidentialité OWL-Lite utilisée pour décrire à la fois les autorisations négatives et les obligations dans le domaine de la politique. Chaque stratégie décrit les règles utilisées pour définir le comportement des entités dans le domaine. Le système doit décrire un moteur de politique qui peut comprendre la politique et évaluer les propriétés d'une entité pour décider comment l'entité doit agir. S'appuyant sur une approche basée sur des règles, Rei surmonte l'incapacité de définir des variables dans le langage OWL.

11. https://www.csee.umbc.edu/~lkagal1/rei/

Auteurs	OV	PV	ABAC XACML	Blockchain	CS
[Junjian et al. (2014)], [Gheisari et al. (2021)], [Schwee et al. (2019)]	x	x			
[Sai et al. (2020)], [Toumia et al. (2020)], [Serrano et al. (2018)]	x	x			x
[Gang et al. (2021)], [Nimalaprakasan et al. (2018)], [Rezvani et al. (2019)]			x		x
[Al-Zubaidie et al. (2019)], [Shantanu et al. (2019)], [Kanwal et al. (2021)]		x	x		x
[Nguyen et al. (2019)], [Huang et al. (2019)], [Bodkhe et al. (2020)]				x	x
[Damiano et al. (2019)], [Liu et al. (2020)]		x	x	x	x
[Kim et al. (2018)]	x			x	x
[Drozdowicz et al. (2020)], [Kim et al. (2018)]	x	x	x		

TABLE 2.1 – Un résumé des technologies utilisées par les différentes plateformes. *OV=Ontologie OWL 2 et ses variantes, PV=Protection de la vie privée, CS=Contrôle d'accè et x= supporter*.

2.3 Conclusion

Les industriels et les chercheurs ont souligné que les problèmes d'hétérogénéité, de sécurité et de confidentialité font partie des principales préoccupations du paradigme de l'IdO qui restent à résoudre. Limite l'amélioration des outils d'autorisation et des modèles de contrôle d'accès bien connus [Hu et al. (2014)]. En effet, la sécurité, la confidentialité et la gestion dynamique des connaissances sont au cœur du processus de développement d'applications IdO [Nisha et al. (2019), Rafal et al. (2020), Conti et al. (2018), Zarpelão et al. (2017)]. Le manque d'interopérabilité et de surveillance de l'accès physique/-virtuel à l'espace ou aux données sensibles peut mettre en danger l'adoption du paradigme IdO, en particulier par les personnes âgées.

Les ontologies sont désormais le fondement d'un système distribué visant à répondre à l'hétérogénéité sémantique qui survient lors de l'extraction dynamique des connaissances et de l'authentification et de la gestion des accès aux ressources. La communauté de recherche a souligné que les ontologies pourraient servir de modèles de connaissances sémantiques dans les applications distribuées qui nécessitent de traiter des informations contextuelles, de faire un raisonnement formel et de faciliter l'échange de connaissances entre utilisateurs, utilisateurs-systèmes et entre les systèmes eux-mêmes. Les ontologies sont également associées à des mécanismes d'inférence pour automatiser le raisonnement sur ces connaissances. Ainsi, plusieurs ontologies ont été proposées pour implémenter la gestion sémantique des connaissances dans les applications d'intelligence ambiante et prendre en charge le raisonnement contextuel basé sur la logique. De plus, pour faciliter les processus d'exploration de données, la mise en œuvre de services Web Sémantiques pour la protection de la vie privée ou de contrôle d'accès. Nous avions présenté que l'aspect sécurité qui dépend des ontologies a été étudié il y a plus d'une décennie par exemple [Denker et al. (2005). Tous les auteurs décrivent les principales questions concernant la représentation des connaissances et le raisonnement pour la sécurité dans le web sémantique. Ils insistent fortement sur le fait que les applications ont besoin d'un langage de politique déclaratif (c'est-à-dire d'ontologies et de capacités d'inférence) pour préserver la confidentialité et la confiance.

Il est également clair que le modèle XACML offre un bon niveau d'abstraction et fournit des structures restreintes pour exprimer les politiques de sécurité. Néanmoins, les systèmes de contrôle d'accès XACML présentent de nombreux défis comme par exemple, aucune sensibilité aux paramètres d'exécution de l'authentification et n'aborde pas la question sémantique.Pour ces raisons et pour une meilleure performance du langage XACML, nous pensons que s'appuyer sur une ontologie est indispensable pour améliorer la gestion des accès et intégrer des politiques dans chaque domaine sans créer de dépendances entre domaines en termes de contrôle d'accès. Comme nous allons le constater dans les prochains chapitres que le langage OWL ne pourra jamais être utilisé dans des applications mettant en danger le bien-être humain. En réponse, nous explorons le potentiel d'un modèle de représentation symbolique de haut niveau appelé cω-Model et un langage de règles de production. Ce même principe est adopté dans cette thèse pour entrelacer les ontologies n-aires telles que NKRL avec la technologie Blockchain. Ces deux solutions sont détaillées dans les chapitres suivants.

Chapitre 3

Modélisation des connaissances à base d'ontologies

3.1 Introduction

On présentera dans ce chapitre, l'évolution des langages de modélisation du web sémantique. L' émergence des outils de raisonnement pour augmenter l'expressivité de modélisation des connaissances de ces langages. Ce chapitre illustre la nécessité d'avoir un modèle plus expressif en plus des systèmes à base de règles. On terminera par une analyse détaillée pour mieux exposer notre approche.

3.2 Dèfinition et Rôle des ontologies

Dans la littérature, de nombreuses définitions ont été données au terme "ontologie". Ces différentes définitions et l'émergence du grand nombre d'ontologies sont le résultat des contraintes dictées par les domaines d'applications et le choix de l'utilisateur pour répondre à leurs besoins. Cette richesse corrobore la vision de [Bylander (1988)] qui avaient souligné que la représentation des connaissances dans le but de résoudre certains problèmes est fortement affectée par la nature du problème et la stratégie d'inférence à appliquer. Pour [Neches et al. (1991)] une ontologie permet de définir les termes et les relations permettant de les lier à un topique particulier, elle

sert également à identifier les règles permettant de combiner les relations afin d'étendre le vocabulaire utilisé : "*An ontology defines the basic terms and relations comprising the vocabulary of a topic area as well as the rules for combining terms and relations to define extensions to the vocabulary*". Cette définition a été très rapidement abandonnée pour laisser place à celle donnée par [Gruber (1993)] : "*An ontology is an explicit specification of a conceptualization*". Cette dernière définition a été suivie par celle de [Borst et al. (1998)], les auteurs définissent une ontologie comme : "formal specification of a shared conceptualization". Cependant, la définition la plus formelle et la plus utilisée est celle donnée par [Studer et al. (1999)] :"*An ontology is a formal, explicit specification of a shared conceptualization*", où :

1. "Conceptualisation" fait référence à une abstraction du monde d'un point de vue pratique. Le concept peut être vu comme une notion discrète plutôt qu'une vision individuelle devant être utilisée pour décrire les composants d'un phénomène du monde ;
2. "Formal" : signifie compréhensible par la machine. Permet également de s'assurer que ces symboles sont interprétés selon une conceptualisation donnée ;
3. "Shared" : signifie qu'une ontologie qui capture les connaissances soit destinée à supporter une interopérabilité à grande échelle ;

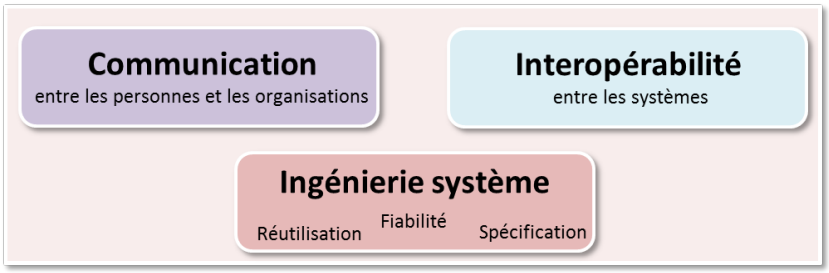


FIGURE 3.1 – Domaine d'utilisation des ontologies. [Uschold et al. (1996)]

Nous retenons aussi la définition de [Guarino (1998)] guidée par le rôle de l'ontologie :"*It enables the developer to practice a 'higher'level of reuse than is usually the case in software engineering (i.e. knowledge reuse instead of software reuse). Moreover, it enables the developer to reuse and share application domain knowledge using a common vocabulary across heterogeneous*

software platforms. It also enables the developer to concentrate on the structure on the domain and the task at hand and protects him from being bothered too much by implementation details". L' auteur souligne l'importance de l'ontologie, qu'est reconnue aujourd'hui dans différents domaines industriels et académiques : Intelligence Artificielle, gestion des connaissances, systèmes d'information, recherche et extraction d'informations, les politiques de sécurité dans les entreprises, etc. Les auteurs ont dénombré divers domaines d'applications tels que, 'entreprise integration' [Gruninger et al. (1995), Uschold et al. (1998)], le domaine médical [Gangemi et al. (1998)] et l'ingénierie mécanique [Borst et al. (1998)] où l'importance des ontologies commençait à prendre place. Les auteurs [Uschold et al. (1996)] avaient présenté trois principales catégories tirant profit des ontologies : communication, interopérabilité et l'ingénierie des systèmes, figure 3.1.

Dans le domaine de la Communication, l'ontologie permet de créer un réseau de relations, explorer et naviguer à travers ce réseau. Particulièrement, l'ontologie permet de fournir un moyen de lever toute ambiguïté sur les termes utilisés par le système logiciel. L' ingénierie des systèmes constitue une autre motivation importante permettant le bon développement des systèmes logiciels : spécification, fiabilité et réutilisation. Les ontologies vont faciliter le processus d'identification des exigences et la compréhension des relations entre composant du système. En conséquence, une compréhension commune du problème et la tâche à accomplir peuvent aider à la spécification des systèmes logiciels. Les ontologies peuvent également être utilisées pour rendre explicite les différentes hypothèses faites par les différents composants d'un système logiciel et faciliter leur intégration. Par cela, l'ontologie peut améliorer la fiabilité des systèmes logiciels en servant de base à la vérification manuelle de la conception par rapport aux spécifications et de la fiabilité des systèmes. Enfin, l'utilisation des outils logiciels aborde sans aucun doute la question de l'interopérabilité, dans laquelle différents utilisateurs ont besoin d'échanger des données ou qui utilisent des outils logiciels différents. Un thème majeur pour l'utilisation d'ontologies dans des domaines tels que la modélisation d'entreprise et les architectures multi-agents est la création d'un environnement intégrant des outils logiciels différents [Uschold et al. (1996)].

Cette première classification des domaines d'utilisation d'une ontologie, a été suivie par une nouvelle étude menée par [Uschold et al. (1999)]. Les auteurs avaient identifié quatre principales catégories d'application d'ontologie : la création, l'ontologie comme spécification, l'accès commun à l'information et la recherche basée sur l'ontologie. Chaque catégorie représente une classe de scénario décrivant un cadre conceptuel dont l'objectif est d'évaluer la maturité des technologies mises en jeu pour mettre en évidence les similitudes et les différences existantes. Le papier de [Van et al. (2000)] est considéré comme une extension de ces scénarios spécifiques à un certain nombre de recherches importantes et aux applications industrielles au sein de diverses communautés telles que : l'ingénierie des connaissances, l'intégration de systèmes d'information hétérogènes, la modélisation d'entreprise, des applications Web et des systèmes distribués orientés objet. Les auteurs ont regroupé les buts et les avantages visés par les ontologies selon trois domaines : communication entre agent systèmes, fiabilité, spécification et acquisition des connaissances et interopérabilité entre les systèmes informatiques où l'otologie est utilisée comme format d'échange. En général, la communauté scientifique considère qu'une ontologie est une conceptualisation formelle du réel, partagée par une communauté à des fins d'échange, elle doit être exploitable par un programme. Elle est composée d'une hiérarchie (Is-A) de concept et d'autres liens sémantiques (e.g., est localisé, est liée à, etc.). Une ontologie permet d'associer de la sémantique aux données de sources externes. On peut diviser les ontologies en deux catégories : i) ontologie légère comprennent les concepts, les taxonomies de concept, les relations entre concepts et les propriétés décrivant les concepts. Ce type d'ontologie permet de modéliser le domaine d'étude de manière approfondie, et ii) une ontologie robuste fournie plus de restrictions sémantiques sur le domaine en ajoutant des axiomes et des contraintes. Les axiomes et les contraintes ont pour objectif de clarifier le sens des termes [Gomez et al. (2004)]. Ces deux types d'ontologies peuvent être modélisés avec différentes techniques de modélisation des connaissances et elles peuvent être mises en œuvre dans différents types de langues.

3.3 Web Sémantique et langages de représentation de connaissances

Le web fut créé par le physicien et l'informaticien Tim Berners-Lee [1] et le défini comme suit : "*... a goal of the Web was that, if the interaction between person and hypertext could be so intuitive that the machine-readable information space gave an accurate representation of the state of people's thoughts, interactions, and work patterns, then machine analysis could become a very powerful management tool, seeing patterns in our work and facilitating our working together through the typical problems which beset the management of large organizations.*". La mise en œuvre de cette vision est rendue possible grâce au langage HTML [2]. Cependant, ce langage permet de donner uniquement un aperçu visuel (grâce aux navigateurs web) des informations véhiculées sous format textuel. Bien que ces informations soient lisibles par un humain, cette conception du web s'est heurtée très rapidement à des problèmes de partage réel et efficace des connaissances. La création d'eXtensible Markup Language 'XML [3]' a permis de mieux structurer les informations, mais n'a pas résolu ces problèmes. En effet, le langage XML est un modèle semblable aux modèles relationnels adapté à stocker les connaissances et à mieux les interroger. L' information véhiculée par un document XML, bien qu'elle soit compréhensible par un être humain, elle n'est pas comprise par une machine. Par conséquent, les machines ne peuvent pas comprendre dans quel but l'utilisateur à utiliser chaque balise et le sens des imbrications d'éléments présentés à travers les balises personnalisées. Doter ces machines des moyens de manipuler et de comprendre les données du web pour un réel partage des connaissances de façon compréhensible fut le rôle du Web sémantique. D'autre part, les machines doivent être capables de traiter les informations et de parvenir à un raisonnement automatisé en utilisant un ensemble de règles d'inférence. Pour atteindre ces objectifs, un modèle de représentation de donnée plus descriptif des informations du web et offrant un support sémantique formel pour la description des connais-

1. https://www.w3.org/People/Berners-Lee/
2. http://www.w3.org/TR/html4/
3. http://www.w3.org/TR/REC-xml

sances compréhensibles à la fois par un humain et par une machine s'est vite ressenti. Ainsi, pour le web sémantique, l'enjeu est de trouver un formalisme capable à la fois de décrire précisément les informations du web avec une sémantique formelle pour ainsi fournir aux machines un support pour traiter, comprendre et permettre un réel partage de ces connaissances. Le langage Resource Description Framework [4] (RDF) permettant de décrire les métas donnés et facilitant leur traitement fut la première réponse pour mettre en œuvre le web sémantique.

3.3.1 Modélisation des ontologies avec les langages traditionnels

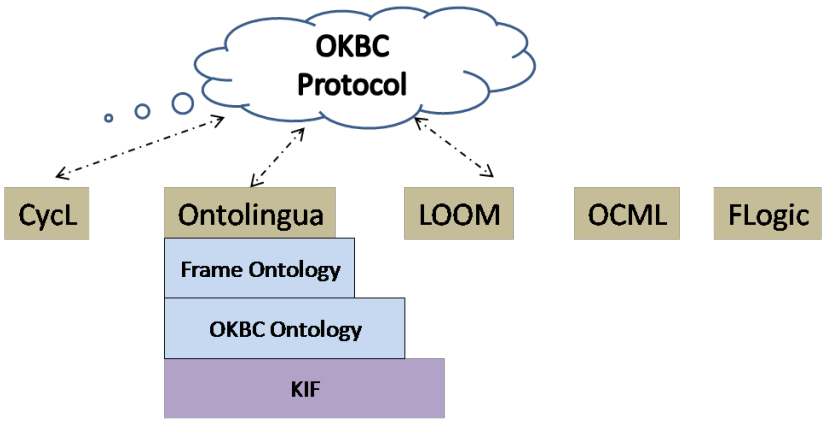


FIGURE 3.2 – Les langages d'ontologie traditionnels. Open Knowledge Base Connectivity (OKBC) [Chaudhri et al. (1998)] fut le premier protocole permettat d'accéder aux ontologies.

Les langages d'ontologies basés sur l'Intelligence Artificielle en vue le jour au début des années 1990. Ces langages sont basés sur :

1. La logique du premier ordre permettant d'exprimer les relations entre concepts, par exemple Knowledge Interchange Format (KIF [5]) ;
2. Les frames [Fikes et al. (1985)] ces derniers sont utilisées pour décrire de manière intentionnelle les classes et les objets. Le concept super

4. https://www.w3.org/TR/2004/REC-rdf-primer-20040210/
5. http://logic.stanford.edu/kif/dpans.html

class et slots relient les frames. Les valeurs des slots doivent appartenir à une classe objet d'un autre Frame combiné avec la logique du premier ordre comme Cycl [Lenat et al. (1990)], Ontolingua, Operational Conceptual Modelling Language (OCML) [Motta (1999)] et FLogic [Kifer et al. (1995)] ;

3. La logique de Description comme par exemple LOOM [MacGregor (1991)] ;

Les composants présentés en Figure 3.2 peuvent être décrits brièvement comme suit :

1. Le Langage Cycl étant le premier langage d'ontologie crée pour décrire l'énorme ontologie Cyc. Cette dernière est composée de plus d'un million d'assertions (faits, axiomes et règles) concernant tous les aspects du monde. Elle décrit 3000 termes groupé en 43 topic (fundamentals, time and dates, spatial relations, etc.). Elle divise l'ensemble de l'univers en deux catégories matérielles et immatérielles, dynamiques et statiques, etc ;

2. LOOM est un langage de représentation des connaissances. Il a été crée pour offrir un moyen de classifier les concepts. LOOM ofre un mécanisme de classification qui intègre un langage de définition de concepts avec un raisonnement basé sur des règles ;

3. Initialement le langage OCML a été défini dans le projet VITAL pour permettre de spécifier des modèles de résolution de problèmes au niveau connaissances exactement comme celles visées par Ontolingua. Sa particularité consiste à supporter différents styles de spécifications : informelle, formelle et opérationnelle. Il a une syntaxe proche de Lisp fournissant des primitives et définit des règles supportant le chaînage avant et arrière ;

4. Le Langage FLogic, acronyme de Frame Logic a été développé initialement comme une approche orienté objet pour la logique du premier ordre. Il a été utilisé dans les bases de données orienté objet, par la suite il a été adapté pour implémenter les ontologies. Il a pour objectif de résoudre des problèmes rencontrés lors du traitement de grande base de connaissances ;

KIF a été développé pour faciliter les échanges de connaissances entre les systèmes informatiques hétérogènes. Il fournit une notation comme celle de Lisp pour définir les objets, les fonctions et les relations.

L' implémentation des ontologies avec KIF est considérée une tâche difficile, mais rendu facile grâce au Frame Ontology (FO). Cette dernière a pour rôle d'unifier la sémantique de toutes les primitives et permet aux développeurs de construire leurs ontologies avec l'approche basée sur les Frames. Le FO a été créé par [Gruber (1993)] est développé par-dessus KIF. La première version du FO contient l'axiomatisation des classes et les instances, les slots et les contraintes sur les slots qui peuvent être vues comme des relations binaires, les classes et les relation (composition, inverse). Le FO a été modifié en 1997 et quelques primitives FO ont été réutilisées dans le protocole OKBC. Une ontologie FO peut être complètement translatée en KIF. Cette opération permet aux utilisateurs de construire et d'importer des ontologies pour les traduire en KIF. Gruber a proposé cinq composants principaux : classes, relations, fonctions, axiomes formels et les instances. Les classes sont les concepts ayant un sens large dans le domaine cible. Par exemple, Bath room, Living room, Table, Robot, etc. Les classes sont organisées en taxonomie de concepts selon un ordre hiérarchique. Selon Gruber, les concepts peuvent entre autres représenter l'intention, les croyances, les sentiments, etc. Une relation représente une association binaire entre différents concepts et en conséquence entre les instances de ces concepts. Les axiomes sont utilisés pour vérifier formellement la consistance d'une ontologie ou la consistance des connaissances stockées dans la base de connaissances et permettent d'inférer de nouvelles connaissances. Les instances servent à représenter les éléments communément nommés individus d'une ontologie.

3.3.2 L' apport du RDF(S) pour la modélisation des connaissances

Le consortium W3C a défini le langage RDF comme un simple modèle de données, permettant de décrire les ressources web et surtout faciliter le traitement des informations par des machines. Il est basé sur des primitives de modélisation : classes, propriétés et instance permettant de fournir un

mécanisme pour décrire les métas donnés du web sous forme de triplets. Un triplet RDF est une association de trois composants : Sujet (ressource), Prédicat (propriété) et Objet (valeur). Ces trois composants constituent une instruction (statement) dans un document RDF. Le prédicat RDF (pouvant être une autre ressource) permet de représenter des prédicats binaires. Il a pour rôle de décrire la relation entre le sujet et l'objet représentant respectivement le domaine et le range. Chaque instruction est représentée par un graphe orienté : les nœuds représentent le sujet et l'objet, tandis que le prédicat est représenté par un arc. Chaque ressource est représentée par un identifiant unique 'Universal Ressource Identifier' (URI) [Berners et al. (1998)].

L' inconvénient majeur de RDF est l'absence de mécanismes pour donner un sens à l'information modélisée. Ainsi, un modèle RDF est associé à un vocabulaire [6] prédéfini pour décrire sémantiquement ces informations échangées. Cette solution est fournie avec RDF Vocabulary Description Language communément connue par RDF Schema [7] (RDFS). Le langage RDFS est considéré comme un modèle permettant de représenter les connaissances du monde réel. Il définit un ensemble de classes et de propriétés permettant de définir une sorte de généralisation/spécialisation sur les classes et sur les propriétés et permet une description précise des ressources. La relation parent-enfant entre les classes et les propriétés n'est autre qu'une taxonomie des termes du vocabulaire organisés de manière hiérarchique. De nombreuses taxonomies exigent qu'un élément ne puisse avoir qu'un seul parent. Dans ce cas, la taxonomie est un arbre ou une collection d'arbres (forêt). Le langage RDFS permet également de définir des restrictions sur les valeurs de propriétés, offrant un moyen de faire de simples inférences comme l'appartenance à une classe, sous classes, les valeurs de propriétés et les relations de sous propriétés grâce à la notion généralisation/spécialisation.

Le vocabulaire RDFS a pour vocation être un langage permettant de partager des connaissances en décrivant les classes de chaque ressource et les propriétés utilisées dans chaque modèle RDF. Toutefois, RDFS ne permet pas entre autres de : i) spécifier des contraintes de cardinalité (i.e. le nombre

6. Un vocabulaire consiste en un ensemble de termes non redondants, sans ambiguïté, ayant un sens cohérent dans tous les contextes de la communication [Hebeler et al. (2009)].

7. http://www.w3.org/TR/PR-rdf-schema

de valeurs que peut prendre une propriété) par exemple dans le domaine industriel, on ne peut pas exprimer que dans un espace aménager, il ne peut y avoir plus de 5 machines, ii) exprimer la négation ou la disjonction entre deux classes (e.g. on ne peut pas exprimer qu'une personne n'a pas pris son médicament ou exprimer que le Robot et l'humain sont disjoints), et iii) d'attribuer une valeur par défaut à un attribut, par exemple attribuer une valeur par défaut à une température, etc. Particulièrement, le système d'inférence est réduit à un système de requête basé sur la relation définie dans le schéma de donnée en termes d'héritage et de spécialisation entre les classes et les propriétés. Pour cela, plusieurs langages d'interrogation de documents RDF existent tel que Query Language for RDF (RDQL [8]) et SPARQL. Ce dernier permet, par exemple, d'interroger un ensemble de descriptions RDF via des requêtes semblables à SQL. Une requête SPARQL correspond à un triplet pouvant contenir des variables dont certaines ne peuvent être libres. La particularité de SPARQL consiste à extraire des données d'un document RDF saturé. L' opération de saturation consiste à générer tous les tuples basés sur les relations entre classes et propriétés utilisant un raisonneur comme Jena [9].

Pour une expressivité plus fine des propriétés des classes, des instances, des relations entre des classes, fournir un moyen d'associer la sémantique aux termes du vocabulaire décrit dans des instructions (statement) RDF, lever l'ambiguïté sémantique sur le sens des termes employé dans un domaine (entreprise, communauté, etc.), décrire des relations entre objets et des changements d'état de ces relations, c'est pourquoi Web Ontology Language [10] (OWL) est né.

3.3.3 Langages de modélisation de connaissances

La figure 3.3 représente l'évolution des langages d'ontologies : le premier langage d'ontologie fut Simple HTML Ontology Extensions [11] (SHOE) combinant le langage de Frame avec les règles. Il est considéré comme une exten-

8. https://www.w3.org/Submission/RDQL/
9. https://jena.apache.org/
10. https://www.w3.org/TR/2012/REC-owl2-primer-20121211/
11. http://www.cs.umd.edu/projects/plus/SHOE/index.html

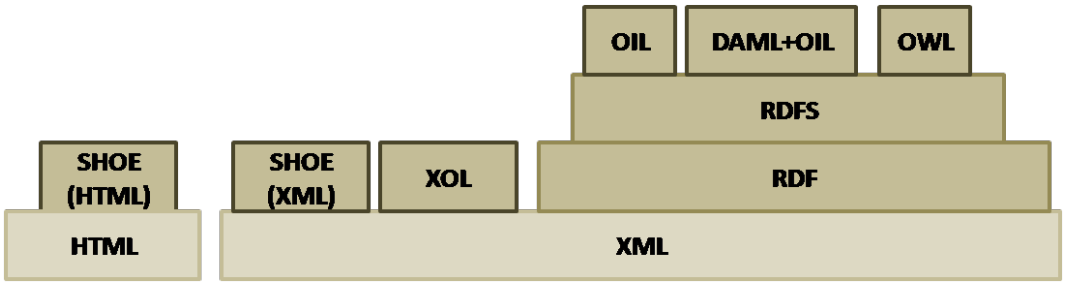


FIGURE 3.3 – Évolution des langages d'ontologies, [Horrocks et al. (2000)].

sion de HTML, cependant, il utilise différents tags pour permettre d'insérer les ontologies dans un document HTML. L' objectif principal de SHOE est d'offrir un moyen de collecter des informations à propos des pages web afin d'améliorer les mécanismes de recherches sur le web. XML-based Ontology exchange Language (XOL) [Karp et al. (1999)] a été désigné pour fournir un format d'échange des données définies dans des ontologies dédiées pour les systèmes software hétérogènes. Il n'a pas été conçu dans le sens à développer des ontologies. Le manque de support de raisonnement pour Ontolingua est l'une des principales motivations qui ont conduit à la création de Ontology Inference Layer (OIL), figure 3.4 [Horrocks et al. (2000)]. Ce langage est une extension de RDF(S) augmenté avec des primitives à base de Fame. Ce langage utilise la logique de description dans l'objectif d'apporter une sémantique plus claire sur les primitives. Les auteurs avaient su tirer profit des remontés d'utilisation du langage OIL [Fensel et al. (2001)] pour arriver à produire une expressivité similaire à Ontolingua.

L' étude comparative figure 3.2 visant à étudier la capacité d'expressivité et d'inférence des langages traditionnels et des langages du web, figure 3.3 a fait objet d'une étude mené par [Corcho et al. (2000)]. La figure 3.5 illustre les résultats de cette étude. Pour la représentation des connaissances, les auteurs ont préféré étudier cet aspect selon un critère d'expressivité basé sur la notion de concepts, de taxonomie, de relations et d'axiomes. Les critères utilisés pour le mécanisme de raisonnement étaient de savoir entre autres si le langage supporte les mises à jour effectuées sur la base des connaissances et de vérifier s'il admet les conjonctions/disjonction de prémisses, etc. Dans leur étude, les auteurs avaient conclu que les langages web sont recommandés pour les échanges d'ontologies sur le web. Les langages d'ontologie

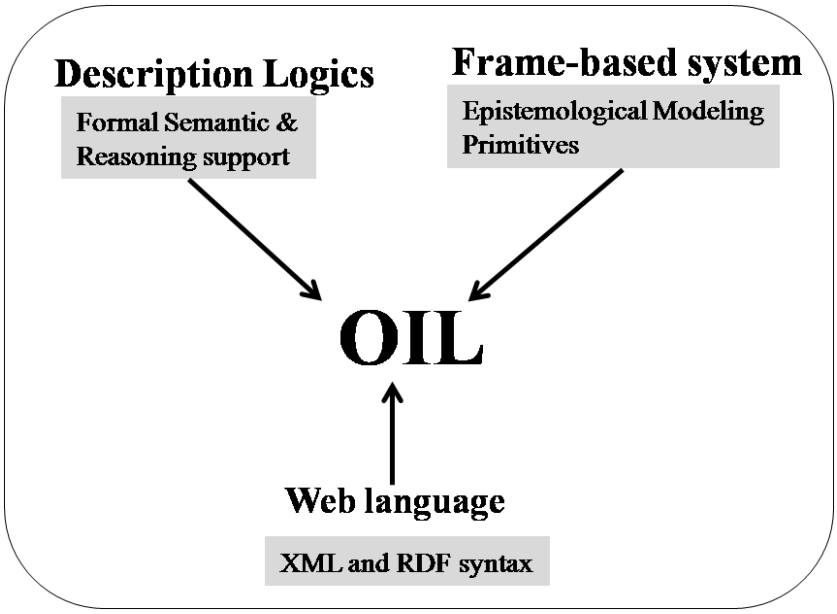


FIGURE 3.4 – Les composants de base OIL, [Fensel et al. (2001)].

traditionnels sont plus adaptés pour la modélisation d'ontologie nécessitant une grande expressivité, tandis que si l'ontologie est juste dédiée pour une taxonomie, l'utilisation des langages à base XML suffit largement.

Darpa Agent Markup Language [12] "DAML"+ OIL a connu deux types de versions lors de son processus de développement. La première version nommée DAML + ONT a été une extension de RDFS. Elle fournit des primitives à base de frame. La seconde version DAML + OIL a abandonné le langage de frame pour la logique de description. Conçu pour fournir plus de faciliter, d'expressivité et de raisonnement sur les classes, les relations entre classes, les types, etc. DAML + OIL fournit 53 primitives de modélisation (i.e. un grand nombre de constructeurs permettant d'exprimer de façon très fine les propriétés des classes). Toutes ces primitives permettent d'exprimer la conjonction, la disjonction et la négation, collection d'individus, propriétés de restrictions définies sur les propriétés, restriction de valeur, restrictions existentielles, restrictions de nombre qualifié (en Anglais qualified number restriction).

La révision de DAML+OIL a donné naissance à OWL. Ce dernier couvre les primitives définies dans DAML+OIL à l'exception de la suppression de

12. https://www.w3.org/TR/daml+oil-reference/

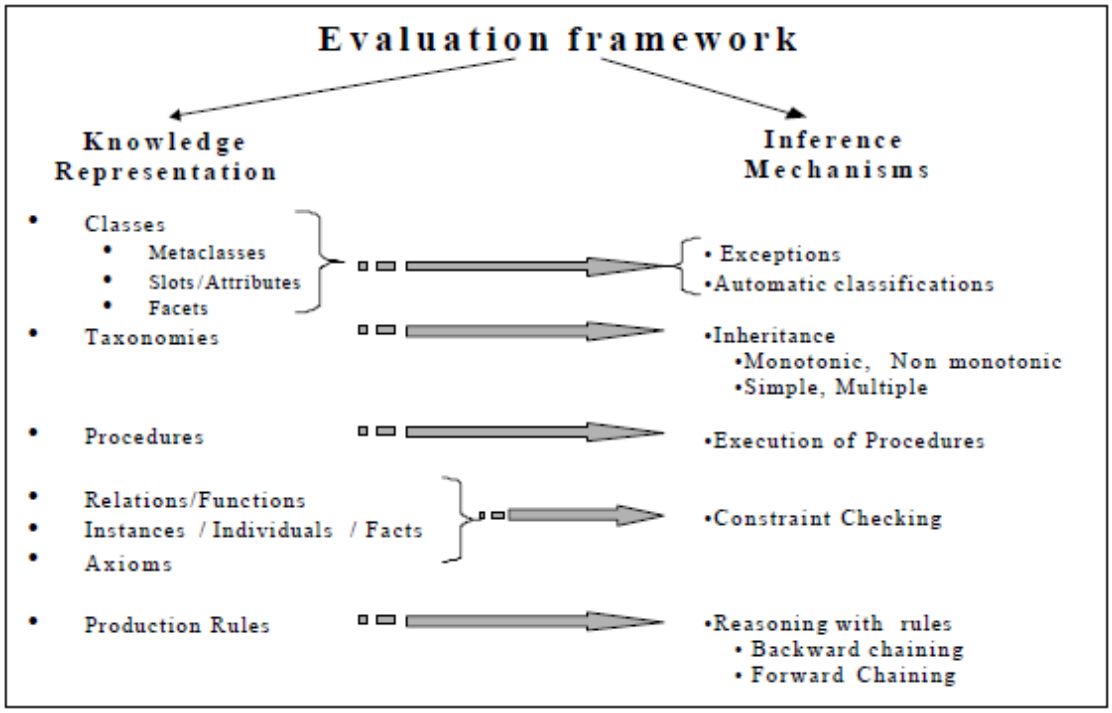


FIGURE 3.5 – Framework d'évaluation des différents langages de modélisation de connaissances, [Corcho et al. (2000)].

la propriété qualified number restrictions et l'inclusion de la propriété SymmetricProperty comme une nouvelle caractéristique de propriété. Toutes les appellations des primitives de DAML+OIL ont été jugées compréhensible que par un expert (pour plus de détails, le lecteur est invité à visiter le site https://www.w3.org/TR/owl-ref/.

Ce langage devrait d'un côté tenir compte de l'aspect distribué des sources de connaissance. D'un autre côté la nécessité de définir un langage suffisamment expressif pour répondre aux besoins de variétés d'applications : "*The next element required for the Semantic Web is a Web ontology language which can formally describe the semantics of classes and properties used in web documents. In order for machines to perform useful reasoning tasks on these documents, the language must go beyond the basic semantics of RDF Schema W3C* [13].". Pour ce faire, il fallait ajouter plus de vocabulaire pour décrire les propriétés et les classe : les relations entre classes (par exemple la disjonction), les cardinalités (par exemple exactement un), l'égalité, etc.

13. https://www.w3.org/TR/webont-req/

3.4 Représentation des connaissances avec OWL

La motivation d'aller au-delà de RDFS schéma est présentée par le consortium W3C à travers six études de cas dont certains cas d'utilisation sont basés sur les efforts recensés en industrie et dans les milieux académiques. Par conséquent, l'interopérabilité entre les différents dispositifs informatiques est l'un des fils conducteurs et représente un des défis à résoudre. Le W3C a dérivé DAML+OIL pour bâtir OWL avec des axiomes plus expressifs et permettant d'utiliser des constructions complexes (exprimer l'équivalence, disjonction entre classes, etc.).

OWL étend RDFS. Il est une mixture de ABox et de TBox et il fournit un vocabulaire de propriétés et de classes utilisées pour construire des ontologies plus expressives. Le niveau du vocabulaire de la TBox est comme suit :

1. Introduit la terminologie $\mathcal{T}$ (i.e., le vocabulaire/axiomes), constitué de concepts qui désignent des ensembles d'individus, et de rôles. Elle contient la représentation des connaissances intentionnelles.
2. La forme de base de la déclaration dans un TBox est une définition de concept (un axiome) à partir de concept déjà définis.
3. La terminologie $\mathcal{T}$ doit contenir
   (a) Une seule définition pour un nom de concept
   (b) Les définitions sont acycliques (i.e. les concepts ne sont ni définis en termes de eux-mêmes ni en termes d'autres concepts qui y renvoient indirectement.)

Quant au niveau de ABox (niveau factuel/assertionnel) est comme suit :

1. Contient les assertions (i.e. connaissances assertionnelles) représentent les instances du domaine.
2. Un ensemble de constructeurs pour combiner des concepts et des rôles : $\wedge, \vee, \sqcup, \sqcap, \equiv, \sqsubseteq, \sqsupseteq$, etc.
   (a) Agent(agent1), Robot(Kompai), Human(David)
   (b) $\neg$Human$\sqcap$ Agent(agent1), exprime implicitement que l'individu *agent1* est un Robot.

(c) estAssister(David, Kompai), spécifie que David a Kompai comme robot assistant

3. Combine les approches logiques et non logiques (i.e. les instructions dans TBox et ABox peuvent être identifiées à l'aide de formules dans la logique du premier ordre.

La sémantique d'OWL peut être définie via une translation de la logique de description. Les concepts sont connus sous le nom de classe, et créés avec la primitive owl :class. Les deux premières primitives (subclaass-Of et disjointWith) définies les conditions nécessaires d'appartenance à la classe (utilisées pour les concepts primitifs) et les concepts "définis" correspondent à la définition d'une classe donnée par des conditions nécessaires et suffisantes. La taxonomie avec OWL est construitée avec la primitive subclassOf pour les concepts primitifs et intersectionOf, unionOf et equivalentClass pour les concepts définis. Similaire à DAML+OIL, les classes sont construites avec des primitives qui sont des propriétés, elles sont divisées en deux groupes, un groupe qui peut être utilisé avec les trois déclinaisons d'OWL et un autre groupe utilisable uniquement avec LD + Full : par exemple, conjonction, value restriction, existentielle restriction, etc. OWL-Lite est la version la plus simple d'OWL, OWL-DL (DL : Description Logic) offre un support pour une expressivité maximale. Une ontologie LD ou Lite peuvent être vue comme une LD TBox où les classes correspondent aux concepts et les propriétés correspondent aux rôles. OWL Full est la version la plus complexe d'OWL mais vraisemblablement indécidable. OWL-DL s'adresse aux utilisateurs qui souhaitent une expressivité maximale sans perdre la complétude et la décidabilité du calcul de subsomption. Pour rendre les calculs décidables, le sous-langage OWL-DL impose des restrictions vis-à-vis de l'utilisation des constructeurs d'OWL et de RDF.

Au départ, OWL est décliné sous forme de trois couches d'une expressivité croissante, OWL-Lite, OWL-DL, et OWL-Full, désormais OWL 2 spécifie trois profils : OWL 2 EL, OWL 2 QL et OWL 2 RL. Afin de garantir un raisonnement évolutif, les profils existants partagent certaines limitations quant à leur expressivité. En général, ils interdisent la négation et la disjonction, car ces constructions compliquent le raisonnement et se sont avérées rarement nécessaires pour la modélisation. Par exemple, dans aucun des pro-

fils, il n'est possible de spécifier que chaque personne est un homme ou une femme. OWL 2 EL est assez similaire au travail avec OWL 2 DL. L' acronyme EL reflète la base du profil dans la famille dite EL des logiques de description [EL++] ; ce sont des langages fournissant principalement une quantification existentielle de variables. Outre la négation et la disjonction, OWL 2 EL interdit également la quantification universelle sur les propriétés. Par conséquent, des propositions telles que "tous les enfants d'une personne riche sont riches" ne peuvent pas être énoncées. De plus, comme toutes sortes d'inverses de rôle ne sont pas disponibles, il n'y a aucun moyen de spécifier que, par exemple, parentOf et childOf sont les inverses l'un de l'autre. OWL 2 EL est conçu en tenant compte des grandes ontologies biosanté, telles que SNOMED-CT [14], le thésaurus NCI [15] et Galen. Les caractéristiques communes de ces ontologies comprennent des descriptions structurelles complexes (par exemple, définir certaines parties du corps en fonction des parties qu'elles contiennent et dans lesquelles elles sont contenues ou propager des maladies selon des relations partie-sous-partie), un grand nombre de classes, l'utilisation intensive de la classification pour gérer les terminologie et l'application de la terminologie résultante à de grandes quantités de données. Ainsi, OWL 2 EL a un langage d'expression de classe relativement expressif et il n'a aucune restriction sur la façon dont ils peuvent être utilisés dans les axiomes. Il a également des expressions de propriété assez expressives, y compris des chaînes de propriétés mais excluant l'inverse.

OWL 2 QL peut être réalisé en utilisant la technologie de base de données relationnelle standard (par exemple, SQL) simplement en élargissant les requêtes à la lumière des axiomes de classe. Cela signifie qu'il peut être étroitement intégré à un système de gestion de base de données relationnelles et bénéficier de leurs implémentations robustes et de leurs fonctionnalités multi-utilisateurs. L' acronyme QL reflète le fait que la réponse aux requêtes dans ce profil peut être implémentée en réécrivant les requêtes dans un langage de requête relationnel standard (DL-Lite). Entre autres constructions, OWL 2 QL interdit la quantification existentielle des rôles dans une expression de classe, par exemple, on peut affirmer que chaque personne a un pa-

14. https://www.snomed.org/
15. https://thesaurus.cancer.gov/ncitbrowser/ConceptReport.jsp?dictionary=NCI_Thesaurus&version=21.07d&code=C98642&ns=ncit

rent mais pas que chaque personne a une mère. De plus, les axiomes de la chaîne de propriétés et l'égalité ne sont pas pris en charge. OWL 2 QL capture également de nombreuses fonctionnalités couramment utilisées dans RDFS et de petites extensions de celles-ci, telles que les propriétés inverses et les hiérarchies de sous-propriétés. OWL 2 QL restreint les axiomes de classe de manière asymétrique, c'est-à-dire que vous pouvez utiliser des constructions comme sous-classe que vous ne pouvez pas utiliser comme superclasse.

Le profil OWL 2 RL est destiné aux applications qui nécessitent un raisonnement évolutif sans sacrifier trop de puissance expressive. Il est conçu pour accueillir à la fois les applications OWL 2 qui peuvent échanger toute l'expressivité du langage contre l'efficacité, et les applications RDF(S) qui ont besoin d'une expressivité supplémentaire de la part d'OWL 2. L' acronyme RL reflète le fait que le raisonnement dans ce profil peut être mis en œuvre à l'aide d'un langage de règles standard. Entre autres constructions, OWL 2 RL interdit les déclarations où l'existence d'un individu impose l'existence d'un autre individu : par exemple, la déclaration « chaque personne a un parent » n'est pas exprimable dans OWL RL. Des implémentations appropriées basées sur des règles d'OWL 2 RL sous une sémantique basée sur RDF peuvent être utilisées avec des graphes RDF arbitraires. Par conséquent, OWL 2 RL est idéal pour enrichir des données RDF.

3.4.1 Modélisation des ontologies avec La Logique de Description

Par opposition au langage de Frame, la Logique de Description (LD) proposée par [Baader et al. (2003)] représente une autre famille de langages de modélisation des connaissances de manière structurée et formellement compréhensible. La LD se base sur quatre composants fondamentaux :

1. La représentation des connaissances intentionnelles sous forme de terminologie contenue au niveau TBox (i.e. contient la définition des concepts et des rôles) ;
2. Les assertions représentant les individus (instances) du domaine, ces derniers sont définis au niveau ABox communément nommé niveau factuel ;

3. Un ensemble de constructeur (conjunction, disjunction, negation, value restriction, existential quantification, existential restriction, etc.) pour construire des concepts et des rôles composés à partir de concept ou de rôle atomique, tels que les 'concepts' dans la LD ont le même sens que dans les frames paradigme (i.e. représente la classe d'objets). Tandis que les 'rôles' décrivant une relation binaire entre concept ;
4. Les mécanismes d'inférence pour faire des raisonnements sur TBox et Abox basé sur le principe de la subsomption ;

Dans les langages à base de LD, les moteurs d'inférence sont communément appelés 'classifier'. La relation 'subclass-of' entre concepts peut être inférée à l'exécution si elles ne sont pas explicitement définies à la conception. Contrairement au langage de Frame où la notion de 'subclass-of' doit être explicitement représentée à la conception.

Afin d'assurer un comportement prévisible d'un système basé sur LD, les inférences devraient être décidables [16] et de faible complexité. Pour atteindre un niveau d'expressivité plus élevé, une grande variété d'extension des langages de description ont été créés, à titre d'exemple, $\mathcal{ALC}$ (Attributes Language with Complemnts) est obtenue à partir la logique minimale $\mathcal{AL}$ en ajoutant un opérateur complémentaire de négation ($\neg$). Quant à l'extension $\mathcal{ALE}$ (pour epsilon) est obtenue à partir du langage $\mathcal{AL}$ en ajoutant le quantificateur existentiel ($\exists$r. $\mathcal{C}$) tel que r représente un rôle, et $\mathcal{C}$ un concept.

Les ontologies et en particulier la logique de description (LD) continuent à jouer un rôle majeur dans le Web sémantique et sont largement utilisées dans de nombreuses applications, par exemple, dans les systèmes de gestion des connaissances, l'e-Science, la bio-informatique et les terminologies médicales, pour les systèmes hybrides - apprentissage automatique et réponse aux questions de bon sens [Tammet et al. (2022)], dans des habitats intelligents pour la description de tâche logique indépendante du simulateur pour l'analyse comparative des agents d'IA incarnés [Ziang et al. (2022)]. Elle trouve sa place dans le domaine d'internet des objets et d'internet des services, la préservation de la vie privée, dans le domaine de la robotique et la combinaison du raisonnement ouvert et fermé, les approches pour la des-

16. Un problème est décidable, si une machine de Turing peut le résoudre en un nombre fini d'étapes.

cription et le déploiement de la logique distribuée qui vise à combler le fossé entre les capacités logiques offertes par l'orchestration des services et l'efficacité de proximité de la chorégraphie des services [Sylvain et al. (2013), Nicola et al. (2019), Sudeepta et al. (2020), Yoji et al. (2018), Gianluca et al. (2021), Claudia et al. (2021)]. Récemment, la LD a été utilisée pour la détection de nouvelles mensongères (fake news en anglais) [Kartik et al. (2021)].

La logique de description a une influence énorme sur la conception du langage OWL. Plus particulièrement sur la formalisation de la sémantique (e.g. le choix des constructeurs, l'intégration des datatype et des datavalues). En effet, la logique de description est considérée comme une plateforme de base pour les langages du web sémantique. Étant donné qu'elle fournit un modèle adapté à la description des ressources (modèle à base de classe et de propriétés), les moteurs d'inférence de la logique de description pour effectuer des classifications automatiques des concepts peuvent être notamment utilisés pour la vérification de contrainte 'constraint cheking' et elle bénéficie d'une communauté de recherche très active.

3.5 Limites du langage OWL

Le fondement d'OWL sur l'hypothèse du monde ouvert et la non supposition du nom unique étaient des choix mûrement réfléchi par le consortium W3C [17]. Dans ce qui suit, nous résumons les principale spécifications du nouveau standard OWL 2 :

1. OWL 2 est conçu pour le Web et la représentation des connaissances est basée directement sur la logique de description SROIQ(D) ;
2. OWL, comme OWL 2, consiste en un ensemble d'axiomes et de faits pour décrire un domaine ;
3. OWL, comme OWL 2, a pour vocation de traiter des connaissances incomplètes, car il est monotone. En effet, l'absence d'une information est considérée par OWL qu'elle n'est pas disponible pour le moment. Contrairement à des nombreuses applications devant avoir une

17. http://www.w3.org/TR/2002/WD-webont-req-20020307/#section-requirements

réponse concrète oui/non. Ainsi on ne peut traiter des raisonnements par défaut ni appliquer des raisonnements sous l'hypothèse CWA.

3.6 Règles : Alternative pour la modélisation des connaissances

Bien que les langages du web sémantiques disposent de nombreux supports pour construire des règles. Cependant, il n'existe pas un langage de règle standard pour le web sémantique. Parmi les langages les plus connus est Semantic Web Rule Language (SWRL [18]). Il est principalement basé en général sur les extensions des propriétés d'inférences de clauses de Horn et DATALOG afin de supporter les structures de données. Rule Interchange Format (RIF) Working Group, quant à lui, est conçu pour assurer l'interopérabilité entre les systèmes de règles et le web sémantique. Différents langages de règles tels que Jena, Jess [19], F-logic [Kifer et al. (1995)] ont été utilisés en fonction des besoins de la communauté. FLogic a étendu les clauses d'Horn pour supporter la négation lors de la déclaration des règles.

SWRL est fondé sur les clauses d'Horn. Il est considéré comme une extension d'OWL-DL permettant d'augmenter l'expressivité d'OWL. SWRL permet de déclarer n'importe quelle description de classe d'OWL, de propriété et d'individus dans le corps comme dans la tête d'une règle. Contrairement à OWL, SWRL permet de traiter les variables et les instances. Une fois la règle écrite, elle peut être exécutée par le moteur d'inférence sur les individus de l'ABox. L' indécidabilité de SWRL est expliquée par le fait de tolérer un raisonnement sur des individus anonymes trouvés dans la base de connaissances ABox. L' approche pour résoudre ce problème consiste en l'introduction du principe DL-safe rules. Cette dernière approche a pour objectif d'assurer que les variables déclarées dans le corps de la règle sont liées uniquement aux individus existant dans la base de connaissances. Ainsi, le risque de traiter les individus anonymes est écarté, par exemple, la règle :
hasAunt(x, y) $\leftarrow$ hasParent(x, z), hasSibling(z, y), Female(y) ..... (R1)

18. https://www.w3.org/Submission/SWRL/
19. http://alvarestech.com/temp/fuzzyjess/Jess60/Jess70b7/docs/index.html

La règle R1 n'est pas DL-safe rule car les atomes des règles sont une sorte de clauses de Horn, ainsi, l'idée est d'ajouter un prédicat externe O pour les contraintes dans le corps de la règle. En conséquence, Pour exprimer la relation "Uncle", on utilise la règle suivante :
$\text{hasParent}(?x, ?y) \wedge \text{hasBrother}(?y, ?z) \wedge O(x) \wedge O(y) \wedge O(z) \leftarrow \text{hasUncle}(?x, ?z)$

Grâce au principe de DL-safe rule, les prédicats O(x), O(y) et O(z) sont ajoutés dans le corps, ainsi toute variable qui apparait dans le corps est encapsulée par un autre prédicat dont le rôle est de s'assurer avoir un raisonnement décidable. SWRL est utilisé dans des applications de contrôle d'accès, domaine clinique, etc. [Qiang et al. (2014), Ronghan et al. (2018), Runumi et al. (2020)]. Actuellement, l'indécidabilité de SWRL est reconnue comme un obstacle pour intégrer OWL avec SWRL. Une autre possibilité consiste à faire appel à des stratégies de moteurs de règles comme Jess, Drools. Une étude a été ménée par [Armando et al. (2016)] pour comparer deux des technologies possibles Drools et Ontology pour la surveillance automatisée des processus de télécommunication. Les résultats montrent que l'implémentation OWL offre des avantages dans l'expressivité des règles, mais Drools est une bonne solution dans les grands environnements en raison de son évolutivité et de ses performances.

3.7 Moteurs d'inférences pour la Logique de Description

De nombreux moteurs d'inférence ont été créés pour raisonner sur les composants ABox et TBox, tels que Renamed ABoxes and Concept Expression Reasoner (Racer) connu également comme Racerpro [Volker et al. (2007)], Fast Classification of Terminologies (FaCT) et Pellet [Sirin et al. (2007)]. Ce dernier offre un moyen pour interpréter les règles SWRL utilisant la notion de DL–Safe rules. Afin de supporter le paradigme du closed world assumption, Pellet étend les axiomes OWL avec le concept des contraintes d'intégrité. Racer est basé sur le langage $\mathcal{SHIQ}$, considéré par la communauté comme un langage très expressif. En effet, $\mathcal{SHIQ}$ permet d'exprimer une restriction sur le nombre d'une propriété grâce à la notion de "Qualified number rets-

riction", par exemple, on peut décrire qu'une personne peut prendre au plus deux comprimés par jour sans mentionner la propriété des médicaments : $\leqslant$2.takeMedecine, on peut également exprimer que la personne est suivie par au plus un ophtalmologue et un cardiologue :
($\leqslant$ 1hasDoctor.Ophthalmologist)$\sqcap$ ($\leqslant$1 hasDoctor. Cardiologist).

L' extension $\mathcal{SHIQ}$ permet de formuler des terminologies complexes telles que les humains ont des parents humains. Humain $\sqsubseteq \exists$hasParent. Humain. Elle permet également de définir le rôle inverse, transitivité, les sous-rôles, etc.

Racer quant à lui, est souvent présenté comme le premier système à supporter le raisonnement à la fois sur TBox et ABox. Il offre également un support pour traiter les formats Lisp, XML, RDF, RDFS, DAML+OIL et OWL. RacerPro utilise l'open world assumption dans le processus de raisonnement. Racer offre en option un moyen pour employer UNA. Bien que de nombreuses requêtes des utilisateurs à vouloir utiliser Racer pour interroger une base "close" (e.g., supporter le CWA). Racer continue à utiliser l'OWA, cependant il propose aux utilisateurs d'assumer le principe du closed world assumption et gérer les réponses des requêtes.

3.8 Concilier OWL avec CWA & UNA

Parmi les premiers travaux dans ce domaine est celui de [Bertino et al. (2003)]. Les auteurs avaient exposé le problème de multi-héritage toléré dans le web sémantique et tous les problèmes d'inconsistance qui en découlent à l'emploi du closed-world assupmtion. Comme solution à ce problème, ils avaient proposé une nouvelle version de la méthode Local Closed-World Assumption (LCWA). Dans leur solution, ils se sont basés sur la technique Answer Set Programming (ASP) utilisée dans les systèmes de bases de données déductibles (ces systèmes déduisent des faits implicites, basés sur les règles et les faits stockés dans la base de données). La technique ASP est utilisée pour contrôler et maintenir la consistance des données dans la base de connaissances décrites en DAML+OIL. Ces données sont traduites en une suite de déclarations dans un programme ASP dont l'objectif est d'offrir un moyen aux langages Web Sémantique (WS) d'adopter les techniques de la

logique non monotone, rappelons qu'elle ne peut être utilisée que sous l'hypothèse de CWA. En effet, les auteurs veulent réconcilier le Web Sémantique avec la possibilité d'effectuer un raisonnement par défaut subordonné à l'utilisation de CWA.

Utiliser donc ASP était une des solutions pour tenter de résoudre ce problème. En effet, ASP à une syntaxe DATALOG, basée sur la définition formelle [Gelfond et al. (1988)], qui applique les idées de la logique auto-épistémique [Moore (1985)] et la logique par défaut [Reiter (1980)] à l'analyse de la "negation as failure" (NAF). La technique ASP est appliquée comme un système de jeu questions-réponses sur les bases de connaissances volumineuses en utilisant des requêtes. L' ensemble de réponses correspond aux différents modèles possibles de l'environnement décrit dans la base de connaissances basé sur le raisonnement non monotone.

[Grimm et al. (2005)] proposaient d'étendre OWL-LD par les opérateurs épistémiques de la logique de description afin d'acquérir les caractéristiques non monotones. L' auto-épistémologie est considérée, rappelons-le, comme un formalisme qui concerne la notion de connaissance et l'assomption pour permettre l'introspection de la base de connaissances. À travers cette approche, les auteurs ont voulu offrir aux systèmes un support d'utiliser les règles par défaut et d'assurer la notion de la contrainte d'intégrité, tout en s'appuyant sur le langage OWL pour la représentation des données. En conséquence, le WS peut tirer profit de toutes ces fonctionnalités et répondre aux nombreuses critiques à propos des difficultés à utiliser le web sémantique à cause d'OWA [Hustadt (1994), Heflin et al. (2002), Kolovski et al. (2005) Damasio et al. (2006)].

Rendre les langages plus d'expressifs a été ressenti dans différentes applications. Cette motivation a entraîné le besoin d'intégrer les règles de Horn et le raisonnement non monotone avec la logique de description. Ces propositions ont relancé les débats sur l'utilité d'implémenter un système de règles capable de fournir les mécanismes semblables aux principes du closed-world assumption. Sans doute, c'est ce qui a poussé le consortium W3C à organiser le workshop [20] dédié pour l'interopérabilité des règles en 2005. Le premier objectif était de trouver des solutions possibles aux problèmes dis-

20. http://www.w3.org/2004/12/rules-ws/report/

cutés ci-dessus (i.e. NAF, default et CWA) : "*We discuss language architecture for the Semantic Web, and in particular different proposals for extending this architecture with a rules component. We argue that an architecture that maximises compatibility with existing languages, in particular RDF and OWL, will benefit the development of the Semantic Web, and still allow for forms of closed world assumption and negation as failure*". Il n'était pas étrange de comprendre pourquoi à l'unanimité, les groupes de travail dans ce workshop ont soulevé la nécessité d'avoir un langage de règles standard capable d'offrir un support aux applications nécessitant un raisonnement rigoureux telles que l'industrie, entreprise, ou relative à la santé et la sécurité des personnes. Toutefois, les participants avaient souligné l'aspect important de l'intégration de la sémantique avec les règles. Ils considèrent qu'un formalisme proposé ne pourrait pas être standardisé si entre autres n'est pas compatible avec RDF et d'un autre côté facilement apparié vers OWL.

Récemment d'autres approches ont été proposées en vue de combiner le raisonnement CWA et OWA, toutefois, ces tentatives sont avérées très complexes et même impossibles à réaliser [Claudia et al. (2021), Henrik et al. (2020), Joachim et al. (2017), Marcelo et al. (2016), Vinicius et al. (2014)].

3.9 Discussion

L' extension d'OWL consiste en quelques légères modifications pour supporter quelques fonctions telles que les contraintes sur les propriétés, les contraintes d'intégrité et l'introduction de trois profils. Cependant, leurs utilisations sont contrariées à des restrictions. À titre d'exemple, bien qu'OWL 2 RL inspiré par les bases de données relationnelles permette des raisonnements en temps polynomial, le degré de son expressivité consiste à appliquer les constructeurs de la logique de description sur les individus explicitement définis dans la base. Ce langage ne pourra jamais être utilisé dans des applications réelles où la santé et la sécurité des personnes sont des objectifs pour lesquels un système de supervision est conçu. Dans ce domaine, on a vu qu'OWL présente des limites, une conséquence de l'héritage de la logique de description qui hérite le principe d'OWA.

L' autre possibilité consiste à utiliser la logique non monotone, parfois

appelée closed world assumption. Quelques approches pour concilier OWL avec CWA et UNA sont occasionnellement des propositions théoriques, étendre les langages de description, celles proposant d'étendre ASP pour trouver un support à la logique de description pour raisonner dans un environnement dynamique. D'autres approches consistent à utiliser LCWA. Les nombreuses approches pour combiner OWA et CWA sont actuellement reconnues comme très difficile, parfois impossible à réaliser. D'autres propositions ont revendiqué de modifier l'architecture d'OWL pour supporter la logique non monotone. Il est évident que la décision est prise et les fondements d'OWL sur le mode OWA sont définitivement adoptés.

L' émergence des moteurs d'inférence dont la plupart basé sur la logique de description pour raisonner sur le web sémantique est une conséquence du manque d'expressivité et de modélisation des connaissances. Ces moteurs sont encapsulés dans des systèmes de requêtes. Leur rôle entre autres concerne le contrôle de consistance de concepts basé sur la subsomption, restrictions sur les cardinalités des classes ou des propriétés définies au niveau terminologique. Les moteurs de raisonnements sont utilisés pour faire des inférences à partir des faits (e.g., les assertions existantes dans la ABox) et les axiomes à insérer dans la base de connaissances TBox. La complémentarité des règles avec les ontologies pour la représentation de connaissances et le raisonnement consiste en un partage de rôle respectif comme suit : Les ontologies encapsulent la définition des concepts et des propriétés et la construction des concepts complexes, les règles sont principalement conçues pour faire des inférences afin de déduire de nouveaux faits à partir des informations stockés dans la base de connaissances. Cependant, l'intégration des règles avec les ontologies n'est pas une tâche facile qu'elle apparaît.

3.10 Conclusion

Les nombreuses approches pour combiner OWA et CWA sont actuellement reconnues comme très complexes. D'autres travaux ont eu comme objectif de créer un nouveau standard. Toutes ces propositions sont une conséquence du fondement d'OWL sur l'hypothèse OWA sans supposition

du nom unique. Ces hypothèses sont définitivement établies avec le nouveau standard OWL 2. D'autres approches ont été proposées pour combiner les capacités d'inférence des systèmes à base de règles avec les raisonneurs créés dans le cadre du W3C (Pellet, Jena, etc.). Toutes ces approches sont utilisées soit avec des restrictions, soit au détriment de la décidabilité. En conséquence, les limites d'OWL restent posées même dans sa nouvelle version OWL2.

Chapitre 4

Vers une nouvelle approche sémantique pour la protection de l'environnement et le bien-être humain

4.1 Introduction

La mobilité et la protection de l'environnement sont des aspects importants des applications de l'Internet des Objets, par conséquent, la modélisation du contexte et le raisonnement sur les connaissances contextuelles constituent une problématique clé pour la mise en œuvre des environnements à intelligence ambiante. En effet, de nombreux défis doivent être résolus tels que l'acquisition des informations brutes à partir des composants physiques de l'environnement et le traitement de ces informations. Pour cela, ces applications requièrent un langage de modélisation expressif, un moteur de raisonnement capable de détecter les incohérences des informations, de maintenir le système cohérent et de raisonner sur ces connaissances contextuelles associées aux informations de bas niveau. Par le raisonnement, le système doit réagir et s'adapter aux changements observés dans les environnements ambiants, par exemple, réagir quand la localisation de la personne change, la température augmente, la personne oublie de prendre son médicament, détecte une tentative d'accès non autorisés, etc.

Malgré que le standard OWL, en particulier sa nouvelle spécification OWL-2 soit un langage expressif et permet de modéliser divers aspects liés à

la reconnaissance de contextes. Incluant la représentation des concepts, leurs relations et des restrictions sur ces relations. Cependant, compte tenu de la logique d'inférence monotone avec non-supposition du nom unique sur lesquelles sont fondés OWL et son successeur OWL 2, ne permettent pas d'acquérir un résultat déterministe (vraie/fausse) dû principalement à la non-présupposition du nom unique, et plus particulièrement, l'hypothèse du monde ouvert autorise la coexistence des connaissances contradictoires dans la base de connaissances et parfois génère des inconsistances comme illsutré par les exemples exposés par Ian horrocks lors de la présentation aux Journées Sémantiques [1]. Nous tenons à rappeler que Ian Horrocks est membre du W3C WebOnt.

Pour répondre à ces problématiques liées aux fondements d'OWL, nous avions adopté une nouvelle approche qui consiste en un langage de représentation de connaissances basé sur le monde fermé avec supposition du nom unique et la reconnaissance de contexte à base de règles basées sur la logique non monotone. Dans ce chapitre, nous présentons le formalisme du modèle cω-Model pour la gestion sémantique et le langage de Règles Sémantique (LRS, en Anglais Semantic Rule Language (SRL)). Enfin, nous présentons le formalisme de la modélisation des informations narratives NKRL basés sur les dimensions spatio-temporelles.

4.2 Modèle sémantique pour la gestion d'accès

Définition 1 : cω-Model (closed ωorld-Model) est un modèle conçu pour décrire sémantiquement des composants élémentaires des systèmes complexes hétérogènes. Il offre un moyen simple pour la supervision et le contrôle des environnements via la combinaison des concepts et de leurs propriétés dans un ensemble de règles métiers. Les règles sont définies dans un langage de règles sémantique garantissant un lien sémantique entre les concepts et les propriétés exprimées dans une ontologie. Par conséquent, via le cω-Model différents corps métiers peuvent raisonner sur les mêmes concepts, indépendamment de contraintes techniques (langages, interfaces,

1. https://www.academia.edu/2686675/Ontologies_and_databases

etc.). La définition des actions pouvant être supportées par les objets peut être facilement définie.

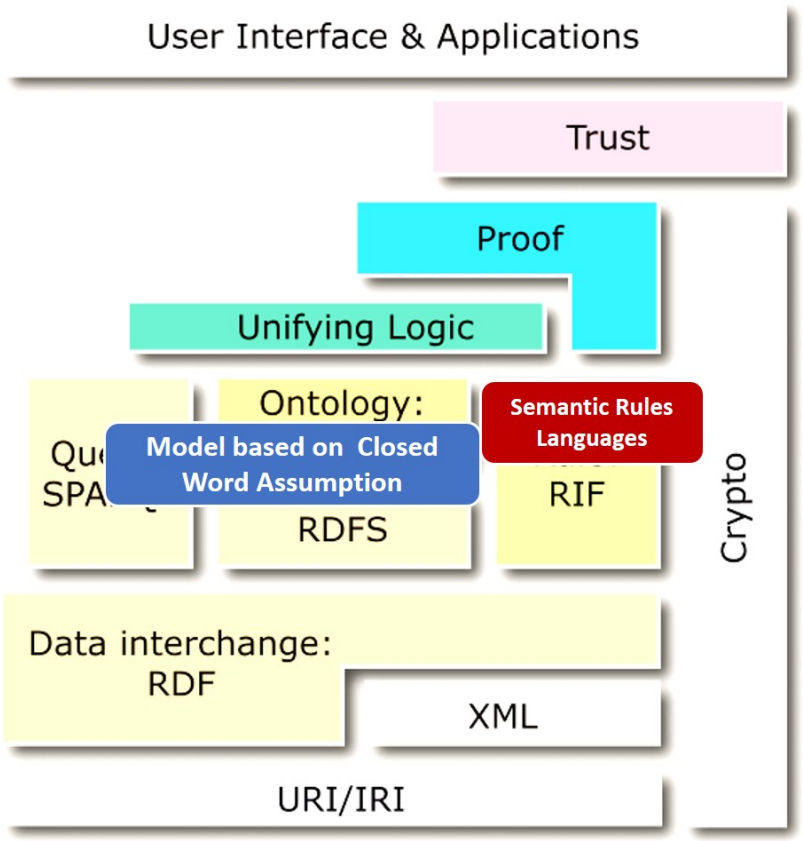


FIGURE 4.1 – cω-Model Vs OWL/RDF standard.

La représentation des connaissances dans le formalisme cω-Model s'exprime à l'aide d'un concept ou d'un ensemble de concepts et des propriétés. S'appuyant sur RDF et RDF-Schema, le modèle cω-Model permet de réutiliser des concepts décrits dans OWL, figure 4.1. La seule exception étant que les instances et les classes sont disjointes (un élément ne doit pas être simultanément une instance et un concept). Outre ce point, un document RDFS doit directement être utilisé comme modèle d'un cω-Model. Il peut être étendu en utilisant des attributs spécifiques au modèle de cω-Model. En plus de la description du langage, une représentation du standard en RDFS a été définie, permettant de manipuler cω-Model par les outils RDF/RDFS.

De plus, le modèle cω-Model définit des groupes d'objets partageant des

caractéristiques communes. Les "propriétés d'objets" expriment des relations entre des concepts définis indépendamment du modèle cω-Model, et peuvent symboliser une relation entre n'importe quel cω-Model.

Les propriétés de type données (c'est-à-dire une valeur littérale telle qu'un entier ou une chaîne) sont utilisées pour décrire des objets et définir leurs caractéristiques, leur état et leur structure. Une sémantique formelle du modèle cω-Model peut être décrite comme suit : une interprétation $.^I$, une abstraction du domaine d'interprétation $\Delta^\mathcal{I}$, $\Delta^\mathcal{I}_\mathcal{D}$ représentant le domaine de don-nées, $\Delta^\mathcal{I}_\mathcal{A}$ et $\Delta^\mathcal{I}_\mathcal{C}$ sont respectivement une abstraction des domaines d'interpr-étation des actions et des Concepts. $\Delta^\mathcal{I}_\mathcal{C} \cap \Delta^\mathcal{I}_\mathcal{A} = \emptyset$, signifie ainsi qu'il existe une distinction concrète entre le domaine d'interprétation des concepts et les instances d'actions. En outre, nous avons $\Delta^\mathcal{I} = \Delta^\mathcal{I}_\mathcal{C} \cup \Delta^\mathcal{I}_\mathcal{A}$.

Une base de connaissances exprimée en cω-Model peut être représentée comme un tuple :

$$\mathcal{O} = \langle \mathcal{C}, \mathcal{I}s, \mathcal{A}, \mathcal{R} \rangle$$

où :

- $\mathcal{C}$ est l'ensemble des concepts ;
- $\mathcal{I}s$ représente l'ensemble des instances qui englobe toutes les instances de concepts, d'actions et de relations, i.e., $\mathcal{I}s = \mathcal{I}_c \cup \mathcal{I}_r$, où $\mathcal{I}_c$ et $\mathcal{I}_r$ représentent respectivement les instances de concepts et de relations ;
- $\mathcal{A}$ modélise d'ensemble des actions qu'un objet peut exécuter, i.e., une instance d'un concept c puisse exécuter un ensemble d'actions $\mathcal{A}(c)$;
- $\mathcal{R}$ représente l'ensemble des relations liant les instances d'un concept à d'autres instances (*relation concept à concept* [2] *ou* relation d'héritage*) ; ou à une valeur (*relation de concept/instances-littérale*) ; ou à des actions (*relation concept-action *)*. Par exemple, la relation concept-concept c_1 R$_c$ c_2 associe les instances des concepts c_1 et c_2, tandis que la relation d'héritage c_1 R$_i$ c_2 modélise que le concept c_2 est une spécialisation du concept c_1. Dans les deux cas, $c_1 \neq c_2$ et $c_1, c_2 \in \mathcal{C}$. quant à la relation concept/instances-littéralle, permet de lier une valeur littéralle

2. la relation concept-concept est similaire à la relation définie dans la propriété Object d'OWL

v à une instance i du concept c, i.e., i R_l v, ou bien lier directement le concept c à une variable v, i.e., c R_l v. Ce dernier est utilisé pour définir des contraintes, via des modificateurs, pour les instances d'un concept donné. Les relations concept-action permettent de relier les actions plausibles que les instances d'un concept peuvent effectuer, i.e., c_1 R_a a_1, où $c_1 \in \mathcal{C}$ et $a_1 \in \mathcal{A}$.

Le formalisme cω-Model permet à différents modificateurs de donner plus d'expressivité dans les définitions des relations. Ces modificateurs peuvent être utilisés ensemble pour fournir une liste de contraintes imposées à une relation spécifique. Ils dépendent de la relation, c'est-à-dire que chaque relation R a une liste particulière de modificateurs possibles $\mathcal{M}(\mathsf{R})$ qui peuvent être utilisés. Par exemple, on peut imposer une contrainte pour limiter le nombre d'instances associées à un même concept pouvant être stockées dans la base de connaissances. Formellement,

$x\ \mathsf{R}_p^M\ y \equiv (x\ \mathsf{R}_p^{m_1}\ y) \sqcap (x\ \mathsf{R}_p^{m_2}\ y) \sqcap \ldots \sqcap (x\ ;\mathsf{R}_p^{m_n}\ y)$ pour $\mathsf{R} \in \mathcal{R}$,
avec $m_i \in\ M$, $M \subseteq \mathcal{M}(\mathsf{R})$, $|M| = n$ et p un type générique de relation.

La liste des modificateurs possibles est :

1. **cardinalité** limite le nombre d'instances pouvant être liées simultanément au concept ;
2. **ordre** associe un numéro de séquence à l'instanciation d'une relation ;
3. **valeur par défaut** affecte une valeur spécifique au concept de relation lorsqu'il n'est pas explicitement spécifié lors de son instanciation ;
4. **valeur statique** indique que tout changement dans la spécification d'une relation doit être propagé dans toutes les instances précédentes et en cours ;
5. **valeur maximale** indique la valeur maximale pouvant être attribuée à une instance d'un concept lors de son instanciation ;
6. **valeur minimale** indique la valeur minimale pouvant être attribuée à une instance d'un concept lors de son instanciation.

R_c et R_a peuvent utiliser les modificateurs 1 et 2, tandis que R_l, qui implique des concepts et des littéraux, peut utiliser tous les modificateurs. Les concepts doivent être associés a au moins une relation concept-littéralle ou une instance de relation concept-concept, c'est-à-dire :

$$\forall c \in \mathcal{C}\ \exists v\ ((c\ \mathsf{R}_l\ v\ \ \in \mathcal{I}_r) \vee (c\ \mathsf{R}_c\ v \in \mathcal{I}_r))$$

Définition 2 : Tous les concepts sont disjoints deux à deux et tous les ordres partiels sont notés $\sqsubseteq$. Soit A, B des concepts, on dit que A subsume B (A est plus général que B, et B est subsumé par A, ou B est plus spécifique que A), les axiomes terminologiques ont la forme A $\sqsubseteq$ B. Si $\cdot^{\mathcal{I}}$ satisfait un axiome (resp un ensemble d'axiomes), alors on dit que c'est un modèle de cet axiome (resp un ensemble d'axiomes).

Définition 3 : La subsomption et l'héritage sont des relations non réflexives, antisymétriques, transitives. En particulier, cela signifie qu'il ne peut pas y avoir de cycle dans la définition d'héritage (A $\sqsubseteq$ B $\sqsubseteq$ C $\sqsubseteq$ A). Si deux concepts parents définissent des restrictions sur les propriétés, alors les restrictions sont fusionnées dans le sous-concept.

Définition 4 : $(a : E)$ décrit une instance de concept (fait) $(E \in \mathcal{C})$, ainsi, une interprétation $.^I$ consiste en un modèle assertionnel de a; $a : E$ si $a^I \in E^I$.

Définition 5 : Le modèle proposé permet que les restrictions de cardinalité : min ($\leq$ nR) ou max ($\geq$ nR) puissent être qualifiées par un concept/sous-concept, et il définit une propriété fonctionnelle entre les concepts R($\top \sqsubseteq$ ($\geq$ 1 R)), ou (R $\in$ TR) où $\top$ est le concept universel :

{ a | $\exists$ b.(a,b) $\in \mathsf{R}^I$} $\geq$ n et { a | $\exists$ b.(a,b)$\in \mathsf{R}^I$} $\leq$ m.

Le modèle XACML permet de spécifier les mécanismes de contrôle d'accès à la gestion des politiques. Cela signifie que la politique d'autorisation autorise l'agent initiateur à agir sur les objets cibles dans un certain contexte. La séparation de la politique de gestion des gestionnaires de systèmes dis-

tribués pour faciliter le comportement dynamique et l'ajout de la sémantique au contrôle d'accès basé sur XML ont été étudiées depuis longtemps.

Le langage de contrôle d'accès nommé XML Access Control Language (XACL [3]) est un exemple célèbre influençant le modèle XACML utilisé pour spécifier un objet-sujet-condition-action orienté politique d'accès dans le contexte d'un document XML particulier.

Les politiques d'autorisation définissent ce qu'un gestionnaire est autorisé ou non à faire [Marcelo (1994)]. Cependant, la complexité des systèmes distribués a entraîné une tendance à rencontrer des goulots d'étranglement lors du chargement d'un ensemble de règles à grande échelle. Le point de décision politique (PDP) peut charger un grand nombre de politiques qui contiennent de nombreuses règles, et le temps d'évaluation du PDP augmente fortement [Scheffler et al. (2013), Mourad et al. (2015)]. En effet, le temps d'évaluation d'un PDP augmente significativement lors-que le PDP charge un ensemble de politiques à grande échelle codé en XACML [Fan et al. (2021)].

Selon les spécifications XACML, il n'existe pas de définitions standard d'actions telles que celles effectuées par les appareils ou les applications IdO reposant sur la version 3.0 de XACML. Au lieu de cela, pour appliquer la sécurité comme décrit par [Marcelo (1994), Kudo et al. (2000)], XACML fournit une spécification de politiques d'accès entre un point d'administration de politique (PAP) et un point d'application de politique (PEP). Le PEP doit autoriser l'accès uniquement s'il comprend et peut s'acquitter de tous les éléments d'obligation associés à la politique applicable. Le modèle de langage politique XACML est principalement composé des composants suivants :

1. Rule : elle est composée principalement d'éléments cibles et de conditions. L' élément cible définit les demandes, identifiées par ressource, sujet et action, que chaque règle est destinée à évaluer. Les éléments de condition couvrent une expression booléenne qui vérifie et confirme l'objectif de l'élément cible.
2. Policy : selon OASIS, une politique se compose d'un élément cible, d'un ensemble de règles et d'un algorithme de combinaison de règles. Ce

3. http://xml.coverpages.org/xacl.html

dernier précise comment l'évaluation des règles du composant est combinée lors de l'examen de la politique. Quant à l'élément cible, il permet d'identifier l'ensemble des demandes de décision destinées à être évaluées.

4.3 Mise en correspondance entre LRS avec des politiques XACML

Un domaine contient des informations qui permettent d'identifier et de décrire les caractéristiques et les politiques d'organisation, etc. Une politique de sécurité est un ensemble de règles d'autorisation, de contrôle d'accès et de confiance dans un domaine spécifique. Tous les services/utilisateurs du domaine doivent appliquer une politique et imposer une politique d'accès locale. Ainsi, nous surmontons les limites d'OWL et ses variantes en termes d'expressivité, d'évolutivité, et améliorons les performances XACML.

Notre approche construit des concepts et des règles sémantiques au-dessus du modèle XACML, décrivant comment utiliser les ressources partagées dans le consortium et leurs restrictions et contextes. Par exemple, si une organisation veut être membre d'un consortium, elle doit être compatible avec l'ensemble des règles de sécurité données par le consortium. Cela implique la « composition » de la politique locale de l'entreprise et des politiques globales du consortium pour faciliter le travail avec le consortium. Par conséquent, des règles peuvent être définies sans connaître à l'avance les sujets ou les objets et même s'appliquer à des sujets d'un domaine externe. L' ontologie du consortium nommée Dynamic Security Network Ontology (DSNO), développée en cours de cette thèse, est construite selon les principaux concepts XACML et fournit des concepts supportant toute instanciation aux domaines locaux. La figure 4.2 montre quelques classes que nous avons définies dans l'ontologie DSNO.

Le langage de règles LRS est fondé sur le principe des règles de production et utilise des concepts/propriétés définis dans l'ontlogie DSNO. Cette ontologie réconcilie les différences sémantiques d'autorisation d'accès dans les environnements multi-domaines. Il définit certaines propriétés fondam-

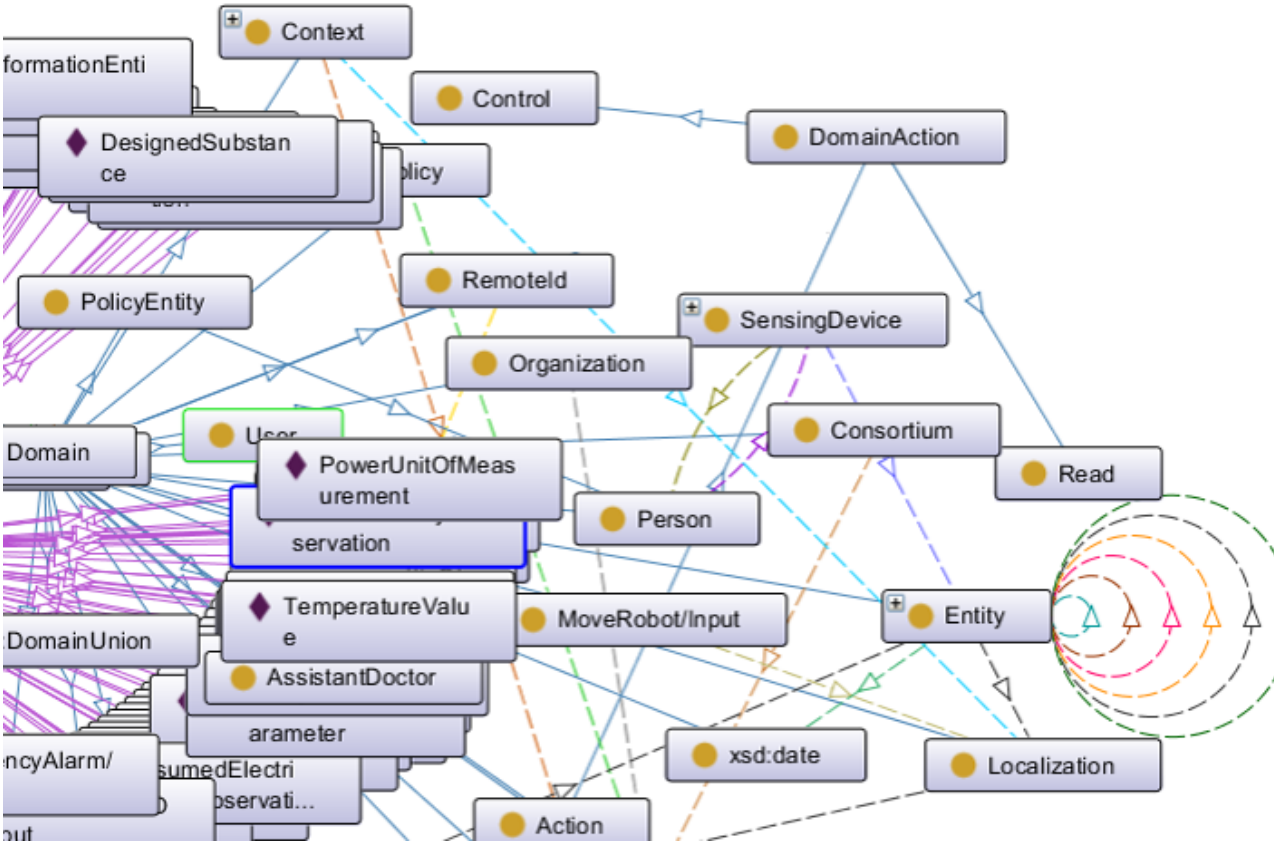


FIGURE 4.2 – Un extrait d'ontologie de politique multi-domaines de consortium.

entales que peut avoir un objet (selon les détails de la représentation).

Le concept *dul :Object* décrit toutes les entités qui peuvent être virtuelles/artefact/humaines. DUL/Object se spécialise dans trois sous-concepts : *smc :ActiveObject*, *smc :StaticObject* et *smc :MovableObject*. *smc :ActiveObjects* sont des objets physiques tels que des capteurs (ssn :Sensor), des actionneurs (smc :Actuator) ou des dispositifs informatiques (smc :Device). *smc :StaticObject* et *smc :MovableObject* décrivent les entités nécessaires à l'interprétation du contexte.

smc :Action décrit toutes les actions d'adaptation au contexte. Les concepts d'instances de smc :Action font référence aux commandes qu'une entité (par exemple, médecin, Internet des services (en Anglais, Internet of Services(IoS)), robot) doit invoquer, telles que la lecture des dossiers des patients, la demande d'autorisation d'accès à un appareil donné (par exemple,

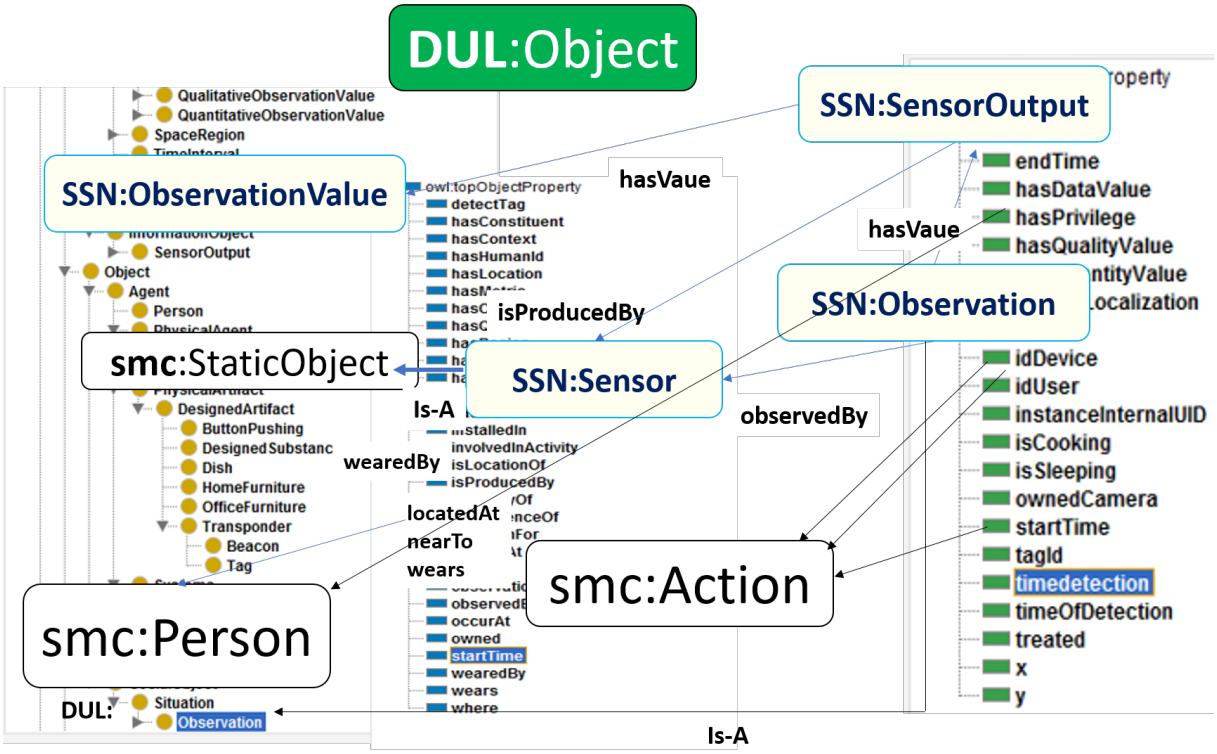


FIGURE 4.3 – Vue d'ensemble de la taxonomie DSNO-Ontology. De plus, l'éditeur cω-Model fournit des fonctionnalités intéressantes qui importent l'ontologie OWL et se traduisent en cω-Model. La description des capteurs et des actionneurs est basée sur les concepts et les propriétés du Semantic Sensor Network (SSN) [Compton et al. (2012)].

une caméra), etc. Par exemple, le concept de capteur, qui hérite du concept ActiveObject, a deux propriétés de base : observes et produces. La propriété observes permet de décrire les propriétés qualitatives d'un capteur, telles que sa précision, sa résolution, son temps de réponse, etc. La propriété produces représente les données fournies par les appareils IdO. De plus, smc :-Action, est une notion fondamentale du modèle proposé. Elle possède trois propriétés importantes : idUser, IdDevice et startTime. La propriété idUser identifie qui doit accéder au contrôle ou exécuter une action. La propriété IdDevice fait référence aux objets cibles de cette action. La propriété startTime enregistre le début du contrôle d'accès accordé. Le concept Observation, Figure 4.3, résume les sorties du capteur. La DSNO définit une taxonomie d'observations : MoveStatusObservation, AspirinAllergyObservation, etc.

Selon les privilèges de leur domaine d'origine, les systèmes/humains peuvent accéder à distance aux services d'autres domaines via une politique multi-domaines abstraite partagée. Par exemple, le personnel hospitalier, les forces de l'ordre et les systèmes distribués collaboreront pour le bien-être de l'être humain en général. Bien que le LRS permette de correspondre une autorisation ou une interdiction, le cadre proposé fournit une abstraction de haut niveau des politiques multi-domaines.

Dans ce qui suit, nous présenterons d'abord les règles de gestion spécifiées avec LRS.

4.4 Modélisation des actions via LRS

Une caractéristique fondamentale sur laquelle s'appuie cω-Model est la définition des actions. Chaque Action a au moins un concept de domaine, et chaque cω-Model peut définir des actions que chaque instance (ou objet concret) appartenant à ce cω-Model pourra effectuer. La classe d'action décrit les propriétés d'action autorisées pour une ressource contrôlée par les règles de politique du consortium. La classe DomainAction permet de faire une catégorisation des types d'action. Le type DomainAction est une sous-classe de smc :Action qui peut faire référence à un nom d'application, une organisation ou un domaine demandant une action. La structure syntaxique d'une LRS suit le paradigme conditions-actions. Chaque règle basée sur LRS est définie à l'aide de la formule suivante :

$$\bigwedge_{i=0}^{m} CP \longrightarrow \bigwedge_{j=0}^{n} AP \tag{4.1}$$

où CP et AP appartiennent à l'ontologie de domaine, et CP représente une conjonction de conditions : ($cp_0 \wedge cp_1 \wedge ... \, cp_{m-1} \wedge cp_m$),

et AP représente une conjonction d'actions :

($ap_0 \wedge ap_1 \wedge ... \, ap_{n-1} \wedge ap_n$).

Une Action peut être représentée comme un tuple : $\langle D, act, In, On \rangle$, où $D \in C$ représente les instances du domaine. Chaque instance de ces concepts ou leur sous-concept peut effectuer une action.

$act \in A$ représente une action à effectuer, In et On représentent des paramètres qui seront utilisés comme valeurs d'entrée et/ou de sortie. Le paramètre d'entrée est obligatoire, tandis que le paramètre de sortie est facultatif $act_{i,o}(\mathrm{D}^{I_n}) \mid (i \in In \wedge o \in On)$. De plus, les propriétés définies dans une action peuvent être des restrictions de cardinalité et des valeurs par défaut. Soit $a(i, o) \in A$, les restrictions sur les valeurs des propriétés sont appliquées avant et après l'exécution d'une action, $\{ \forall(i \in In$ et $o \in On) \mid i^{I_n} \sqsubseteq \triangle^{I_n}$ et $o^{I_n} \sqsubseteq \triangle^{I_n} \}$ et $\{$ a $\mid \exists$ b.(a,b) $\in R^{I_n} \} \geq n$, et $\{$ a $\mid \exists$ b.(a,b) $\in R^{I_n} \} \leq n$.

Définition 6 : La description de l'état d'une instance (d'un fait) dans la base de connaissances est décrite par les valeurs de ses propriétés. Par exemple, les affirmations : House (isEmpty == true), User (isOutSide == true) ; User(hasTag := RFIDTag) indiquent respectivement que la maison est vide, que la personne n'est pas à l'intérieur et que la personne est équipée d'un tag RFID.

Définition 7 : La notion de variables dans le langage de règles LRS est similaire à celle utilisée dans les autres systèmes basés sur des règles, y compris les règles de production, telles que Drools [4], etc. Contrairement aux autres langages de règles du Web sémantique, le langage LRS déduit automatiquement le type de l'élément référencé par une variable. Il permet d'exprimer des règles de production telles que "si-alors" en utilisant des variables correspondant aux concepts et aux propriétés définis dans l'ontologie. Le système d'inférence basé sur des règles traite les évènements sémantiques des entités et vérifie les instances DSNO. Ce processus repose sur un principe d'appariement qui consiste à unifier chaque instance correspondante avec le concept/sous-concept d'une ontologie de domaine encapsulé dans la partie condition (antécédent) de la règle. Celles-ci se déclenchent lorsqu'une situation de demande sensorielle/d'autorisation d'accès est détectée, par conséquent le système ajoute une nouvelle connaissance au modèle sémantique, produit une action à effectuer, supprime/met à jour ou crée une instance, met à jour la valeur de propriété des instances. De plus, chaque action pourrait définir des valeurs d'entrées/sorties. Par exemple, supposons qu'une ontologie pour la gestion des applications basées sur le paradigme

4. https://drools.org/

Internet des Objets a été définie, le système déclenche des règles pour permettre au personnel hospitalier de vérifier la santé de la personne en observant l'interaction entre un robot et un personnel hospitalier. Nous pouvons ainsi définir des règles pour envoyer une notification au personnel hospitalier. Une autre règle pour déplacer un robot où l'évènement de chute est détecté. Enfin, une règle autorisant le personnel d'accéder à la caméra embarquée sur un robot. Ainsi, un système embarqué dans un robot accorde le contrôle d'accès au médecin, lui permettant de modifier à distance l'angle de la caméra pour surveiller la scène et obtenir des représentations directes du monde. Nous soulignons ici que MoveRobot est une instance de smc :Action.

4.4.1 Fondement du raisonnement

La logique d'inférence en OWL peut dans certains cas générer une base de connaissances incohérente (i.e., encapsule des connaissances contradictoires). Par conséquent, les conclusions dérivant des inférences peuvent être incohérentes et parfois rien ne peut être inféré. Ceci n'est pas toléré dans les applications mettant la vie et le confort des humains en jeu.

Une des caractéristiques principales du modèle cω-Model, qui implémente le paradigme du "monde fermé", est de vérifier que toutes les contraintes définies dans le modèle sémantique sont satisfaites avant d'effectuer la mise à jour de la base de connaissances. Ainsi, si un fait est indéterminé, il est considéré comme faux. Manipuler des connaissances complètes sur l'environnement (e.g., une description des actions pouvant être exécutées) permet un contrôle plus sûr du système. Le contrôle est assuré via la combinaison des concepts et des propriétés en sein d'un ensemble de règles. Ces dernières manipulent uniquement les faits insérés dans la base de connaissances. Ces règles permettent d'exprimer un raisonnement de haut niveau (i.e. le système raisonne sur la représentation sémantique des entités de l'environnement). Cette approche à base de règles, permet de garantir que le modèle sémantique représente le dernier état d'une entité physique ou logique de l'environnement. Elle permet aussi de simplifier l'écriture des règles de raisonnement et d'augmenter le niveau d'abstraction dans la gestion et le

contrôle de l'environnement. En effet, contrairement à OWL, quand une nouvelle valeur est assignée à la propriété d'une entité, elle écrase l'ancienne valeur. Dans ce cadre, les règles sont étroitement liées à l'ontologie, du fait qu'elles n'utilisent que des termes (prédicats) liés aux concepts et aux propriétés (relations) de l'application, tout en utilisant des symboles propres aux langages de règles LRS.

La méthode la plus courante permettant d'obtenir une meilleure interprétation de données hétérogènes consiste à créer un lien sémantique entre des données numériques de bas niveau issues de systèmes de perception tels que la localisation avec des représentations sémantiques de haut niveau d'ontologie [Sejdiu et al. (2020)]. Par conséquent, l'ontologie entrelacée avec des systèmes de sécurité tels que les technologies Blockchain ou le modèle ABAC offre un niveau d'autonomie efficace et plus élevé en partageant les données IdO associées, résout les problèmes d'interopérabilité sémantique. Ainsi, la meilleure approche pour améliorer la gestion sécurisée et sémantique des connaissances distribuées consiste à créer un lien sémantique entre les données numériques de bas niveau issues des systèmes de perception avec des représentations sémantiques de haut niveau de l'ontologie.

La seconde approche que nous adoptons dans cette thèse est l'approche narrative. Elle permet des descriptions sémantiques d'entités, d'évènements et de relations entre évènements. Cette approche consiste à analyser des évènements et des comportements complexes en utilisant Narrative Knowledge Representation Language (NKRL) [Zarri (1997)]. NKRL définit Une ontologie de concepts appelée HClass, et une ontologie n-aire appelée HTemp. Cette dernière utilise des structures hiérarchiques n-aires de prédicats sémantiques et des rôles sémantiques n-aires pour représenter des évènements dynamiques et des connaissances contextuelles telles que : qui est l'initiateur (c'est-à-dire l'agent) d'un évènement/action ? Le contexte dans lequel un évènement est observé ou une action est réalisée ? Quelle entité (bénéficiaire) tire profit de la réalisation de l'évènement/action ? etc. La principale différence avec les paradigmes ontologiques actuels tels qu'OWL est que le langage de représentation des connaissances narratives proposé ajoute aux ontologies habituelles du concept, l'ontologie des évènements appelée

HTemp (Hierarchy of Templates). Une template est une structure hiérarchique où les nœuds correspondent à des structures n-aires.

Chaque modèle permet de représenter une connaissance dynamique, structurée et complexe, par exemple, un médecin souhaite accéder au dossier électronique d'un malade. NKRL définit également une ontologie de concepts appelée HClass (Hierarchy of Classes). Il comprend plus de 3000 concepts. HClass n'est pas différent de frame-based ou Protégé (https://protege.stanford.edu/).

4.5 Fondement de NKRL

NKRL a été conçu à l'origine pour formaliser, gérer et traiter les connaissances décrites dans des rapports, mémos, dossiers médicaux, etc, [Zarri (1997)]. NKRL consiste à mettre en place des procédures de représentation et d'inférence efficaces pour établir des relations intéressantes entre les éléments narratifs. La représentation conceptuelle des connaissances narratives s'effectue à travers l'ontologie des concepts HClass. Ce dernier est similaire aux langages d'ontologie traditionnels tels qu'OWL, DAML + OIL. La partition entre concept_sortal et concept non_sortal constitue le principe architectural principal de HClass. Il correspond à la différenciation entre "les notions (en Anglais sortal) qui peuvent être instanciées directement en spécimens dénom-brables", comme "la caméra" (un objet physique), et "les notions (non-sor-tales), qui ne peuvent pas être instanciées directement en spécimens," co-mme "incorporé".

Les spécialisations de sortal_concept, comme camera_, table_ peuvent avoir des instances directes (CAMERA_1, TABLE_2), tandis que les spécialisations du non_sortal_concept telles que embedded_, ou color_, peuvent admettre d'autres spécialisations : embedded_sensor, blue_chair, mais ne possèdent pas d'instances directes.

4.6 Ontologie HTemp

L' ontologie HTemp exprime le sens de connaissances (actions, événements, etc.) come un arbre, où les nœuds correspondent à des structures n-aires. Dans ce qui suit, nous soulignerons les propriétés de NKRL qui pourraient s'avérer particulièrement utiles dans le cadre d'applications distribuées et fournirons la modélisation de NKRL qui, grâce à la richesse du système de représentation, peut automatiquement établir des relations sémantiques intéressantes entre les connaissances dynamiques.

La représentation narrative conceptuelle des connaissances est structurée en quatre composants connexes (c'est-à-dire le composant définitionnel, le composant énumératif, le composant descriptif et le composant factuel) :

1. **Composant définitionnel** : Permet la représentation des concepts. Un concept est une représentation binaire de notions générales (être humain, artefacts) ou de notions spécifiques (médecin, capteur, chaise). La représentation formelle de ces notions est appelée concepts. Les concepts sont insérés dans l'ontologie HClass en tant que structure de généralisation/spécialisation. Un concept est nommé à l'aide d'étiquettes symboliques en minuscules et incluant un « trait de soulignement », comme humain_being, artifact_, doctor_, sensor_, robot_.
2. **Composant énumératif** : Concerne la représentation formelle des instances (individus) définies dans le composant définitionnel. Les instances sont créées en instanciant les propriétés des concepts. Ils se caractérisent par le fait qu'ils sont dénombrables (énumérables) et toujours associés, souvent de manière implicite, à une dimension spatio-temporelle. Les instances sont représentées en majuscules, y compris un symbole de soulignement. MOTION_SENSOR et CAMERA_1 sont des instances du concept sensor_, et KITCHEN est une instance de concept location_. Pour répondre à la complexité des évènements dynamiques/modélisation du contexte, NKRL fournit les deux composants suivants.
3. **Composant descriptif** : est une représentation structurelle des classes générales d'évènements. Les représentations n-aires formelles de ces

TABLE 4.1 – Structure générale d'une template NKRL.

PREDICATE
SUBJ {<argument > : [location] }
OBJ {<argument> : [location] }
SOURCE { <argument> : [location] }
BENF {<argument> : [location] }
MODAL {<argument> }
TOPIC { <argument> }
CONTEXT { <argument> }
[modulators]
[temporal attributes]

classes générales en termes NKRL sont appelées modèles. « évènement élémentaire » correspond simplement à une connaissance spatio-temporelle (c'est-à-dire une occurrence de prédicat), d'une des structures n-aires appelées modèles. Il est indiqué par son étiquette symbolique (voir ci-dessous pour plus de détails). Une occurrence de prédicat s'exprime par un prédicat, un ou plusieurs rôles, et chaque rôle peut être associé à des arguments. Le tableau 4.1 montre la structure générale d'un modèle, dans laquelle : PREDICATE : relatif à l'ensemble des prédicats (MOVE, OWN, EXIST, PRODUCE, RECEIVE, EXPERIENCE, BEHAVE). L' argument représente les attributs qui peuvent être associés à chaque rôle générique (subject(SUBJ), object(OBJ), SOURCE, MODAL, TOPIC, CONTEXT, Beneficiary (BENF)).

4. **Composant factuel** : Permet la représentation de tous les évènements élémentaires extraits dans un récit (c'est-à-dire en tant qu'instances des modèles du composant descriptif). Comme déjà indiqué, ces représentations formelles du modèle sont appelées occurrences de prédicats. Les évènements élémentaires (les occurrences de prédicats) concernent finalement la description d'un ensemble particulier d'interactions entre les individus (par exemple, le cas échéant, les concepts) telle que l'interaction entre JOHN_ et le ROBOT_KOMPAI.

4.7 Représentation des évènements en NKRL

Un évènement élémentaire dans NKRL est exprimé par un prédicat, un ou plusieurs rôles, et chaque rôle peut être associé à des arguments. Table 4.2 et Table 4.3 affiche respectivement les modèles Produce et Own, où : locations : désigne l'espace où les évènements/actions se sont produits. Les modulateurs temporels et les attributs temporels sont des étiquettes symboliques associées à l'occurrence de prédicat. Ils sont utilisés pour représenter le début ou la fin d'évènements élémentaires ou la durée de l'observation selon laquelle, à un instant donné, un évènement spécifique est en cours ou une transaction a été exécutée. De plus, les deux modulateurs : begin/end, sont l'horodatage marquant respectivement le début et la fin de l'évènement, et le modulateur obs est un horodatage spécifique de l'évènement qui se produit. Une autre possibilité est que seul un horodatage intermédiaire t3, entre t1 et t2, soit connu. Dans tous ces cas, NKRL exige que l'on utilise uniquement le premier attribut temporel, date-1, c'est-à-dire que l'unique horodatage disponible est systématiquement associé comme valeur à date-1, les variables définies entre crochets ([ ]) sont des éléments facultatifs. Dans la Produce template, table 4.2, cela signifie que les rôles SUBJ et SOURCE et (var1, var3) sont obligatoires, alors que les rôles et les variables BENF et SOURCE (var7, var2) par exemple sont facultatifs . Les variables var1, ..., var10 représentent des contraintes, permettant de vérifier que les valeurs affectées à chaque variable lors de l'instanciation de chaque template (concept, sous-concepts) sont définies dans l'ontologie HClass. Pour mieux caractériser chaque rôle, un opérateur SPECIF est utilisé. Il permet d'associer une liste de propriétés sous forme de concepts ou d'instances à ces rôles. De plus, les «attributs de localisation» ne peuvent être associés qu'à des arguments de prédicat à l'aide de l'opérateur deux-points (:).

Dans le modèle OWN, table 4.3, le rapport (i.e., charge, filler en Anglais) OBJ doit nécessairement être le concept non-sortal (par exemple, propriété_) ; par souci de généralité, les termes spécifiques de propriété_ (propriété quantifiante, propriété relationnelle, etc. sont également admises). L' alternative concernant les rapports du rôle TOPIC nous permet de différencier le modèle Own :CompoundProperty de Own :SimpleProperty. Dans le premier

TABLE 4.2 – Structure de la template Produce.

name : Produce :Entity
PREDICATE : PRODUCE
SUBJ var1 : [(var2)]
OBJ var3
[SOURCE var4 : [(var5)]]
[BENF var6 : [(var7)]]
[MODAL var8]
[TOPIC var9]
[CONTEXT var10]
{[modulators]!=abs}
var1 = $< artefact\_ > \mid < human\_being\_or\_social\_body >$
var2 =$< location\_ > \mid < pseudo\_sortal\_geographical >$
var3 = $< artefact\_ > \mid < information\_content > \mid < internet\_location >$
var4 = $< human\_being\_or\_social\_body >$
var5 = $< location\_ > \mid < pseudo\_sortal\_geographical >$
var6 = $< human\_being\_or\_social\_body >$
var7 = $< location\_ > \mid < pseudo\_sortal\_geographical >$
var8 = $< artefact\_ > \mid < activity\_ > \mid < process\_ >$ $\mid < temporal\_development >$
var9 = $< physical\_appearance > \mid < situation\_ >$
var10 = $< situation\_ > \mid < symbolic\_label >$

TABLE 4.3 – Structure de la template Own.

name : Own :SimpleProperty PREDICATE : OWN SUBJ var1 : [(var2)] OBJ var3 [SOURCE var4 : [(var5)]] [(BENF) var4] [MODAL var6] TOPIC var7 [CONTEXT var8] {[modulators]!=abs} var1!= $< human\_being\_or\_social\_body > \mid < property\_ >$ var2 = $< location\_ >$ var3 = $< property\_ >$ var4 = $< human\_being\_or\_social\_body >$ var5 = $< location\_ >$ var6 =$< activity\_ > \mid < artefact\_ > \mid < process\_ > \mid < reified\_event > \mid$ $< symbolic\_label > \mid < temporal\_sequence >$ var7!= $< animate\_entity\_property > \mid < human\_being\_or\_social\_body > \mid$ $< part/whole\_relationship > \mid < spatio/temporal\_relationship >$ var8 = $< situation\_ > \mid < symbolic\_label >$

cas, la ”propriété” est nécessairement représentée par une liste SPECIF où le premier argument (var7) doit être un terme spécifique des concepts (non sortal) : ensemble_relation, relationnel_propriété, et spatio-temporel _relationship, et la seconde (var8) peut être n'importe quelle spécialisation ou instance de sortal_concept. Dans la seconde, la ”propriété” est directement représentée par le(s) rapport(s) principal(aux) du slot TOPIC – qui peut aussi être, par exemple, le premier argument d'un opérateur SPECIF dans une liste ”expansion” en dehors des en-têtes et du spécifiques termes des trois sous-arbres ”relationnels” de HClass.

4.8 Représentation des connaissances n-aires

Les modèles de NKRL sont instanciés selon une structure n-aire décrite comme suit :

(Li (Pj (R1 a1) (R2 a2) . . . (Rn an)) Eq 1.

Où :

- Li une étiquette symbolique générique identifiant un modèle donné ;
- Pj un prédicat conceptuel relatif à l'ensemble (MOVE, PRODUCE, RECEIVE, EXPERIENCE, BEHAVE, OWN, EXIST) ;
- Rk (k=1,..,n) un rôle générique appartenant à l'ensemble BEN(e)F(iciary), MODAL(ity), TOPIC, CONTEXT, SUBJECT, OBJECT et SOURCE , et avec ak l'argument correspondant (concepts, individus ou associations de concepts ou d'individus) ;

L' occurrence de prédicat aal1.c18 (table 4.4) exprime que le symbole FRONT_DOOR_BUTTON qui est utilisé comme rapport du rôle SUBJ(ect), représente le bouton_, la propriété déverrouillée comme rapport du rôle TOPIC, enfin date-1 est l'attribut temporel qui ne représente qu'un point précis dans l'intervalle temporel associé à l'évènement : la porte d'entrée a été déverrouillée. À son tour, l'occurrence de prédicat aal2.c3 (tableau 4.4) exprime que la caméra notée CAMERA_1 a enregistré une activité dans LOCATION_1.

L' occurrence de prédicat aal3.c6 (tableau 4.4) exprime que le bouton lumineux localisé dans le hall désigné par HALL_1 change d'état, de switch_off

TABLE 4.4 – Quelques exemples d'occurrences de prédicats instanciées selon le principe décrit par l'équation Eq1.

aal1.c18) PREDICATE : OWN
SUBJ : FRONT_DOOR_BUTTON
OBJ : property_
TOPIC : unlocked_
{ obs }
date-1 : 04/06/2021 :9 :56 :15 :362
date-2 :
Own :SimpleProperty
aal2.c3) PREDICATE : PRODUCE
SUBJ : CAMERA_1 : (LOCATION_1)
OBJ : detection_
TOPIC : activity_
{ obs }
date-1 : 04/06/2021 :10 :31 :20 :102
date-2 :
Produce :Assessment/Trial
aal3.c6) PREDICATE : OWN
SUBJ : LIGHT_BUTTON_1 : HALL_1
OBJ : property_
MODAL : lighting_ : (switch_off, switch_on)
{ obs }
date-1 : 04/06/2021 :10 :31 :22 :523
date-2 :
Own :SimpleProperty
aal1.c14) PREDICATE : EXPERIENCE
SUBJ : PERSON_1
OBJ : respiratory_distress
MODAL :SENSOR_DISTRESS_1
{ obs }
date-1 : 04/06/2021 :17 :57 :35 :105
date-2 :
Own :SimpleProperty

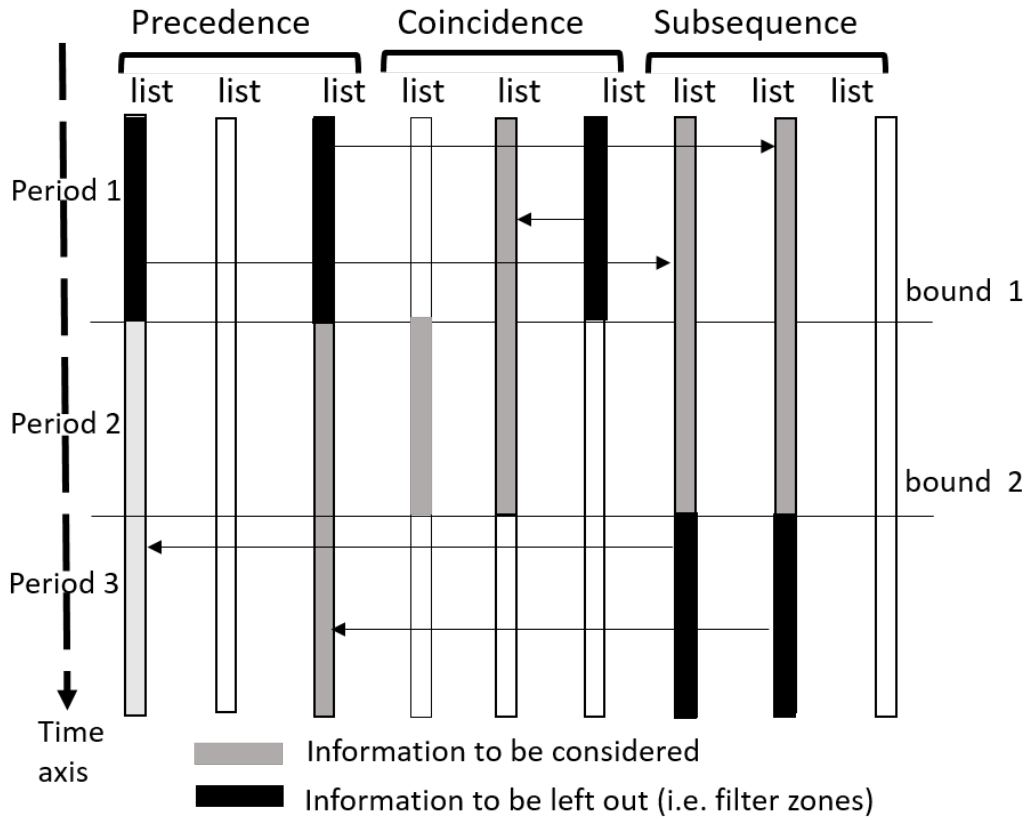


FIGURE 4.4 – Algorithme Temporel NKRL, [Zarri (1997)].

TABLE 4.5 – Autres exemples d'occurrences de prédicats.

aal8.c29) PREDICATE : BEHAVE
SUBJ : ENTITY_1 : LIVING_ROOM_1
MODAL : sitting_position
{ obs }
date-1 :24/06/2021 :19 :20 :45 :785
is instance of Behave :HumanProperty (1.1)
aal8.c28) PREDICATE : PRODUCE
SUBJ : ROBOT_KOMPAI
OBJ : detection_ : LIVING_ROOM_1
TOPIC : (SPECIF ENTITY_2(SPECIF different_from JOHN_))
date-1 :24/06/2021 :19 :42 :12 :556
is instance of Produce : Assessment/Trial

à switch_on. Alors que le capteur_embarqué (c'est-à-dire la sous-classe d'artefact_) observe qu'un patient désigné par PERSONNE_1 (aal1.c14, tableau 4.4) présente une insuffisance respiratoire aiguë sans donner aucune information sur le début, la durée, ou la fin de cet évènement particulier. Ces connaissances sont exprimées en NKRL à l'aide du modèle EXPERIENCE. Ce dernier est principalement utilisé pour représenter des évènements où une entité donnée, humain ou non, est exposé à une certaine expérience (maladie, croissance, succès, etc.). L' occurrence de prédicat aal1.c14 (table 4.4) exprime que le symbole PERSON_1 qui est utilisé comme rapport du rôle SUBJ, représente un humain, la propriété de respiratory_distress comme rapport du rôle OBJ, enfin, date -1 est l'attribut temporel qui représente uniquement un point spécifique dans l'intervalle de temps associé à l'évènement.

4.9 Représentation spatio-temporelle et corrélation sémantique entre évènements

Basé sur l'instant de temps, NKRL utilise deux attributs temporels : date-1 et date-2, permettant d'annoter un évènement/contexte pour reconstruire la logique de l'intervalle d'Allen. L' attribut temporel, date-1, représente l'évènement qui commence à être vrai à l'horodatage t1, la deuxième date-2, qui indique la fin du même évènement à l'horodatage t2.

L' intervalle de temps est organisé en neuf listes correspondant à trois catégories : priorité, coïncidence, sous-séquence, voir figure 4.4. La catégorie précédente représente les événements qui sont apparus avant la date indiquée dans l'attribut date-1. La catégorie de sous-séquence représente les évènements qui se sont produits après la date-2. La catégorie de coïncidence permet de représenter des évènements à l'aide du modulateur obs(erve) utilisé pour désigner le début d'un évènement. Ces trois catégories se composent chacune de trois listes. Chaque liste est divisée en trois sections correspondant à la période 1, à la période 2 et à la période 3. Enfin, la borne 1 et la borne 2 délimitent ces périodes.

Une autre possibilité est que seul un horodatage intermédiaire t3, entre t1 et t2, soit connu. Chaque évènement nécessite de distinguer son début et

sa fin ; cependant, il est difficile d'établir ou de déduire la fin d'un évènement dans de nombreux scénarios. Néanmoins, conserver au moins le début d'un évènement est obligatoire pour poursuivre le raisonnement. La représentation des connaissances dans NKRL permet de spécifier uniquement l'attribut date-1 (c'est-à-dire que l'unique horodatage disponible est systématiquement associé à date-1, le deuxième attribut, date-2, étant vide). Par exemple, le *home control system* observe que ENTITY_1 est assis mais ne donne aucune information sur la fin de cet évènement ni sur sa durée. Ces informations sont exprimées en NKRL avec l'occurrence prédicative aal8.c29 (table 4.5). Le prédicat BEHAVE est utilisé pour exprimer un évènement où une entité exécute une tâche (c'est-à-dire, manifeste un comportement donné directement). L' instance ENTITY_1 comme rapport du rôle SUBJ(ect), la propriété sitting_position comme filler du rôle MODAL, enfin date-1 est l'attribut temporel qui marque le début de l'évènement.

4.10 Conclusion

Dans ce chapitre, nous avons présenté deux modèles de représentation de connaissances et de raisonnements : cω-Model et NKRL (Narrative Knowledge Representation Language) permettant de reconnaître des contextes/-situations complexes. Nous nous sommes focalisés sur les fondements de base de la modélisation de chacun des modèles. Les avantages d'un système de raisonnements à base de règles aident à séparer le raisonnement à haut niveau sur la représentation contextuelle de connaissances liées aux informations brutes générées par l'ensemble des entités dans l'environnement. Par conséquent, cela permet de se concentrer à la définition des règles de contrôle de l'environnement et la gestion du bien-être humain.

Bien que, les règles d'inférences soient découplées de la modélisation de l'environnement, cependant ces règles sont indissociables de l'ontologie de l'application pour la reconnaissance de contexte (i.e., ces règles utilisent les concepts et leurs relations définis dans l'ontologie). De plus, La difficulté à représenter les connaissances de l'environnement telles que le système alerte l'hôpital pour un problème de santé d'une personne, etc. s'accroît en prenant en compte les dimensions spatiales et temporelles. La représent-

ation de la cause ou le but pour lequel le système a déplacé le robot constitue une difficulté supplémentaire nécessitant d'établir une relation sémantique entre évènements élémentaires (e.g., le système constate qu'une personne oublie de fermer la porte principale ou une tentative d'accès à un dossier médical, le système alerte la personne concernée). La réponse apportée par NKRL à cette problématique est basée sur la représentation conceptuelle des informations narratives, en offrant : i) un moyen de combiner les prédicats et les rôles conceptuels pour encoder de manière adéquate les informations narratives, et ii) un support pour construire les liens sémantiques (causalité, but, etc.) entre évènements élémentaires.

Chapitre 5

Mise en œuvre

5.1 Introduction

Dans un premier temps de ce chapitre, nous validons notre approche de politique d'accès sécurisée fondée sur le modèle XACML et le Langage de Règles Sémantique (LRS, en Anglais Semantic Rule language (SRL)). Nous nous concentrons sur les principaux problèmes suivants :

1. Aborder l'hétérogénéité sémantique des données des capteurs lors du partage des connaissances ;

2. Faire une abstraction de l'implémentation de la sécurité à l'aide d'une approche sémantique pour concilier les divergences sémantiques à travers plusieurs domaines et maintenir la politique de sécurité locale ;

Dans la suite du chapitre, nous montrons, l'apport du raisonnement narratif entrelacer avec la technologie émergente, Blockchain. Cette dernière est livrée avec des outils pour protéger les données personnelles sensibles. De plus, la technologie Blockchain surmonte les problèmes de fiabilité en fournissant une architecture de communication sécurisée dans la conception d'applications distribuées.

5.2 Plateforme sémantique pour le contrôle d'accès dans des applications Internet des Objets

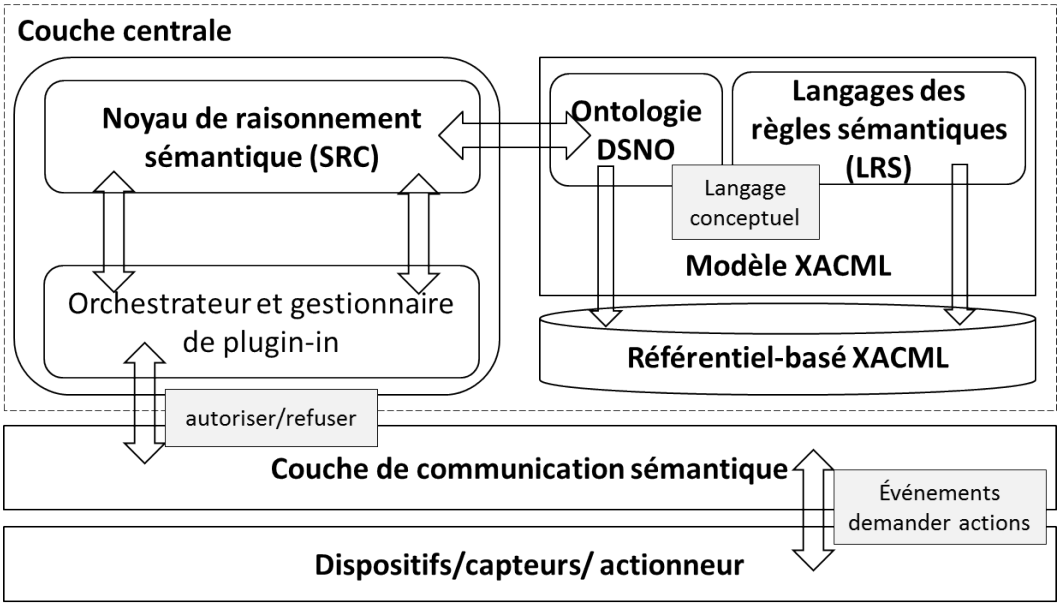


FIGURE 5.1 – La plateforme basée sur une ontologie pour le partage des politiques de contrôle d'accès dans des environnements collaboratifs de l'Internet des objets.

Un schéma simplifié de l'architecture du système est représenté par la figure 5.1. Cette architecture est conçue comme un mécanisme de plug-in, permettant l'insertion de modules supplémentaires. La principale caractéristique architecturale concerne le découplage de la couche inférieure représentant le monde réel (l'architecture du système ignore quelle interface de communication est utilisée). Les deux composants (la couche de communication sémantique et la couche centrale) sont interconnectés à l'aide du protocole JMS [1] pour échanger des informations sémantiques.

La plateforme comprend quatre composants principaux : le référentiel basé sur XACML (XACML-R), l'ontologie DSNO basée sur cω-Model, la couche Semantic Communication Layer (SCL) et le Noyau de raisonnement sémantique (SRC). Cette couche est considérée comme le Noyau qui permet le raisonnement sémantique.

1. https://www.oracle.com/java/technologies/java-message-service.html

Les trois composants (DSNO, XACML-R et SRC) sont construits autour du moteur de règles (LSR) qui représente le cœur de la logique métier utilisée dans l'ensemble de la plateforme. La logique d'authentification et de contrôle d'accès sont ensuite réalisées en combinant les concepts DSNO et leurs propriétés dans un ensemble de règles de production et de requêtes à l'aide du langage de règles sémantiques. Les règles de production nous permettent d'exprimer un raisonnement de haut niveau sur les évènements envoyés depuis le SCL et un raisonnement basé sur l'ontologie, ce qui permet d'autoriser/refuser une demande d'autorisation d'accès à distance lors de l'exécution. Le SCL coordonne l'accès aux appareils IdO. Son objectif principal est de traiter l'énorme quantité de données générées à la fois par les appareils et les services, et de masquer l'hétérogénéité des sources IdO (par exemple, les capteurs et les actionneurs). La plateforme traite les connaissances de SCL et décode les actions en commandes.

Un environnement distribué est généralement composé de plusieurs domaines de politiques de sécurité. Chaque domaine fournit des services d'accès aux ressources locales physiques ou logiques. Pour illustrer ce problème, nous prenons le scénario de trois domaines (hôpital, Smart Home, ambulance). Des appareils IdO sont déployés dans la Smart Home pour surveiller des personnes âgées vivants seules et en maintien à domicile, prévenir les cambriolages et augmenter la sécurité de leur domicile en intégrant des caméras de sécurité. Chaque domaine a sa propre politique de sécurité, mais le personnel hospitalier (c'est-à-dire les sujets dans le jargon XACML) doit accéder aux appareils de l'IdO et aux services IoS. Ces domaines sont régis par des politiques de sécurité indépendantes et coopèrent pour assurer le bien-être et le confort des personnes âgées. Dans ce scénario, nous supposons que le convalescent Samuel porte des capteurs physiologiques (par exemple, le bracelet). Lorsque ce capteur enregistre une chute, l'intervention d'une équipe médicale est nécessaire pour juger de la gravité de la situation et prodiguer les premiers soins. Le médecin de l'hôpital vérifiera l'état de santé de la personne en observant l'interaction entre le robot et Samuel. Le robot doit se déplacer jusqu'à l'emplacement exact de la chute. Ainsi, le médecin doit accéder à distance à la caméra embarquée du robot et mettre en évidence la chute en conséquence. Nous supposons maintenant que le

personnel hospitalier s'est engagé à évacuer Samuel d'urgence vers l'hôpital le plus proche.

Comme deuxième scénario, supposons que pour fournir des soins intensifs pendant le transport médical. Le médecin qui a accompagné Samuel dans l'ambulance a jugé qu'il devait accéder au dossier médical du patient. Par conséquent, la composition de chaque politique locale des trois environnements (hôpital, Smart Home, ambulance) améliorera les applications IdO collaboratives dans chaque environnement. Par conséquent, il est nécessaire d'utiliser une communication sécurisée qui préserve les mécanismes d'authentification. Cependant, ces domaines sont régis par des politiques de sécurité indépendantes et coopèrent pour assurer le bien-être de Samuel. Ainsi, sans contrôle d'accès collaboratif inter-domaines, l'équipe médicale de l'hôpital se verra refuser l'accès aux dossiers médicaux de Samuel. Dès lors, le pronostic vital de Samuel est engagé.

L' objectif des deux scénarios consiste à modéliser une gestion décentralisée des autorisations de contrôle d'accès entre plusieurs domaines. Ainsi, l'hétérogénéité sémantique entre les politiques locales de la politique de sécurité des différents domaines est cruciale pour la mise en œuvre de ce processus. L' architecture sémantique que nous proposons facilite ce mécanisme d'interopérabilité qui garantit la préservation de la politique locale de chaque domaine et l'accès à un utilisateur externe selon les privilèges dont il dispose dans son domaine de sécurité d'origine. En effet, cela permet aux utilisateurs spécifiques au domaine d'accéder à d'autres services à distance et permet au médecin de partager tous les dossiers médicaux du patient avec le pompier sur place pour fournir les premiers soins. Quant au personnel médical de l'hôpital évalue la santé physique de l'utilisateur en accédant à distance à la caméra du robot, par exemple. Par conséquent, selon le contexte, la plateforme donne au personnel hospitalier des privilèges d'accès pour avoir un contrôle total.

En s'appuyant sur LRS décrit dans la section 4.4, des règles permettent de détecter que l'utilisateur est tombé au sol et envoyer une alarme pour alerter le personnel hospitalier. Dans ce cas, les règles extraient les informations des données de capteur et le système déduit les informations d'emplacement à partir de la propriété d'observation occurAt. Tout d'abord, le per-

sonnel hospitalier doit prouver qu'il appartient à un domaine de confiance (c'est-à-dire l'identifiant AssistantDoctor ID). Notez que le Subject : Docteur et Object : Robot vivent dans des environnements différents. Selon la règle XACML (voir Listing 5.1), le système de contrôle du robot donne les informations d'identification qui permettent au médecin de modifier à distance l'angle de la caméra pour surveiller la scène et obtenir des représentations directes du monde.

Listing 5.1 – Un extrait de la politique XACML gérant l'accès à la caméra et l'accès au dossier du patient.

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
    xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:lissi="http://lissi.com/security/authorization/policy/schemas/record.xsd"
    xmlns:home=http://home.com/security/authorization/policy/schemas/record.xsd
    ....
    PolicyId="http://lissi.com/security/authorization/policy/robot-camera"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides"
        Version="1.0">
    <VariableDefinition VariableId="00124B000123D129">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <Apply

           FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:3.0:example:attribute:physician-id"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Apply>
           <Apply
            FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                <AttributeSelector MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                Path="home:cameras/home:robot-camera/"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Apply>
        </Apply>
    </VariableDefinition>
    <Rule
        Effect="Permit"
        RuleId="http://home.com/security/authorization/policy/permit-access-to-physicains" >
        <Description>
         Access to the /robot-camera/ is only allowed to physicians and law enforcement agencies.
        </Description>
        <Target>
            <AnyOf>
```

```
            <AllOf>
              <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue
                 DataType="http://www.w3.org/2001/XMLSchema#string"
                 >accesscamera</AttributeValue>
                 <AttributeDesignator  MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
              </Match>
            </AllOf>
          </AnyOf>
        </Target>
        <Condition>
           <VariableReference  VariableId="00124B000123D129"/>
        </Condition>
    .....
            <AttributeValue
            DataType="urn:oasis:names:tc:xacml:3.0:data-type:xpathExpression"
            XPathCategory="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            > lissi:record</AttributeValue>
    .....
        </Rule>
</Policy>
```

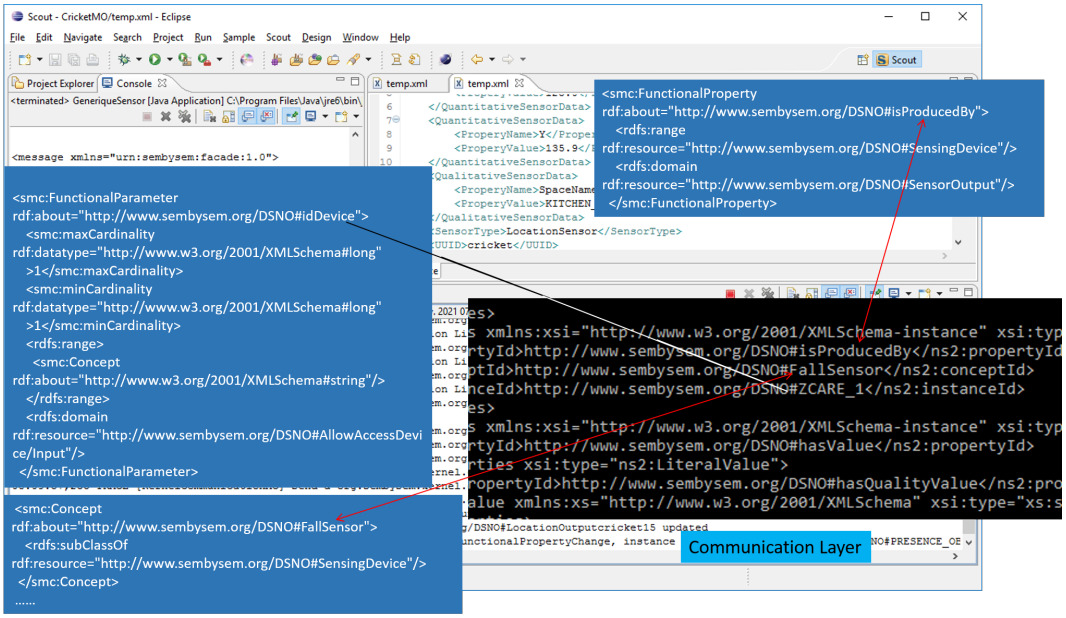


FIGURE 5.2 – Vue d'ensemble de la connexion de SCL en s'appuyant sur des concepts définis dans l'ontologie DSNO dédiée aux environnements collaboratifs de l'Internet des Objets.

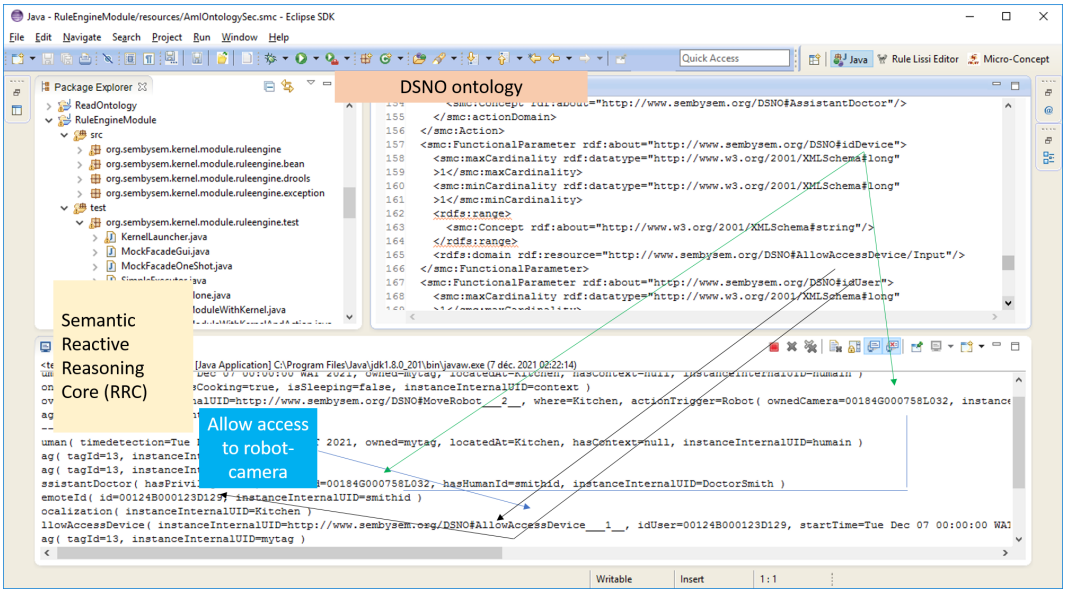


FIGURE 5.3 – Journal d'exécution du noyau de raisonnement et de la couche de communication.

Tous les capteurs/actionneurs sont connectés au SRC, en s'appuyant sur les concepts cω-Model correspondant définis dans l'ontologie DSNO. Par exemple, ZCare_1 est un ID qui représente une instance du FallSensor Concept, Figure 5.2. Le *hasValue* représente les valeurs des capteurs dans FallObservation. Le robot se déplace pour vérifier l'état de santé de Samuel. Si Samuel n'interagit pas avec le robot, il est considéré comme inconscient. Par conséquent, le contexte actuel correspond à une urgence. Les actions sont lancées et une alarme est envoyée pour avertir le personnel hospitalier. La règle correspondante est déclenchée, puis une demande d'autorisation du personnel hospitalier pour accéder à la caméra du robot est exécutée. Un message indiquant clairement l'URI (idDevice) et smc :Action correspondant au AllowAccessDevice sont transmis à la couche de communication sémantique. Cette dernière décode l'action en une commande que les entités impliquées (robot-caméra) peuvent exécuter. Le robot vérifie l'identité de l'hôpital à l'aide de LRS, qui résume toutes les politiques multi-domaines et l'authentification de l'utilisateur (c'est-à-dire l'ID du médecin), figure 5.3. Après avoir terminé ce processus, le robot permet au personnel hospitalier d'accéder à sa caméra embarquée, voir Listing 5.2.

Listing 5.2 – Les règles sémantiques pour le contrôle d'accès à la caméra du robot.

```
rule   "FallPerception"
  conditions
    ?entity := ObjectFall();
    ?entity isInstanceOf(Person);
  actions
    FallEvent ?event :=createInstance(FallEvent);
    Action ?alarm :=createInstance(EmergencyAlarm);
    insert(?event);
    insert(?alarm);
end
rule  "MoveRobot"
  conditions
    RFIDReader (?tag := detectTag,  ?location := locatedAt);
    ?human := Human(?tag == owned);
    ?robot := Robot();
  actions
    MoveRobot ?action :=createAction(?robot,MoveRobot);
    ?action->where := ?location;
    ?human -> locatedAt := ?location;
    execute(?action);
end
rule  "AccessCamera"
  conditions
    ?assistant :=AssistantDoctor(?tg := hasHumanId,
                                 ?askdeviceId := idDevice);
    ?tg(id == "00124B000123D129");
    ?assistant (hasPrivilege==true);
    ?robot :=Robot(?askdeviceId == ownedCamera);
  actions
    AllowAccessDevice ?accessAction :=createAction(?assistant,
                                AllowAccessDevice);
    ?accessAction->idDevice := ?askdeviceId;
    ?accessAction->idUser := ?tg->id;
    ?accessAction->startTime := createTime(timestamp([now]));
    execute(?accessAction);
end
```

Comme décrit ci-dessus, pour la cible (Target en Anglais) d'une stratégie (voir Listing 5.1). L' élément VariableDefinition permet la vérification de l'iden-

tité du médecin en faisant correspondre l'attribut de sujet de l'identifiant du médecin avec l'identifiant du médecin dans la ressource. Comme pour l'élément cible, l'élément VariableDefinition définit toutes les demandes de décision (par exemple, les actions) que la règle est censée évaluer. L' élément Match compare la valeur de l'attribut d'action *action-id* dans le contexte de la requête avec la valeur littérale "access". Le VariableId dans l'élément Condition contient une référence à l'agent (c'est-à-dire le médecin) ayant accès à la caméra-robot. La figure 5.3 montre le processus d'exécution pour accéder à une caméra. Un éditeur spécifique a été conçu comme un plug-in eclipse modulaire. Il assure la vérification syntaxique et sémantique lors de l'édition des règles (c'est-à-dire que toutes les références à l'ontologie de domaine sont valides), figure 5.4.

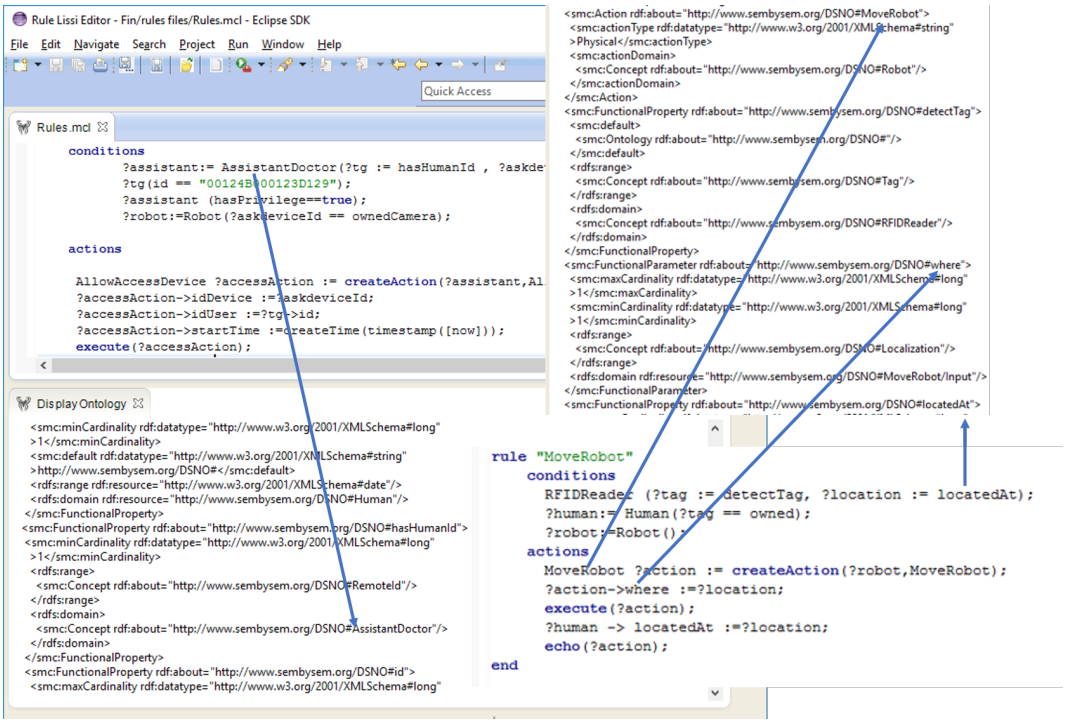
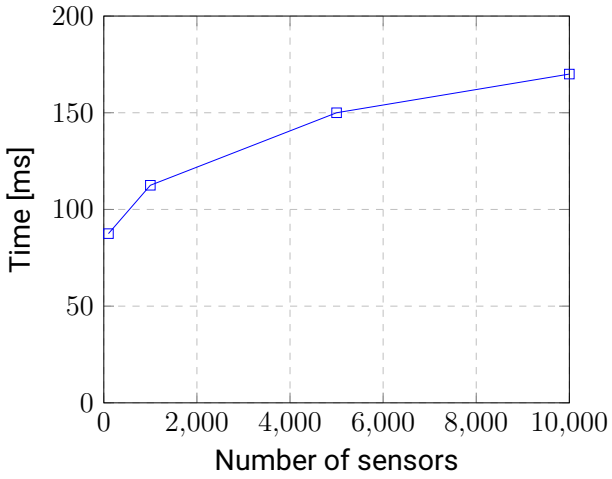
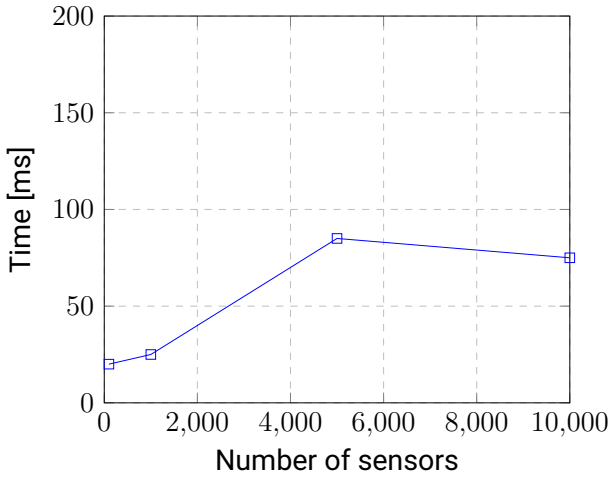


FIGURE 5.4 – Conception globale de l'éditeur de règles sémantiques. l'idUser, idDevice, startTime sont des paramètres d'entrées et de sorties pour les actions MoveRobot et AssistantDoctor.

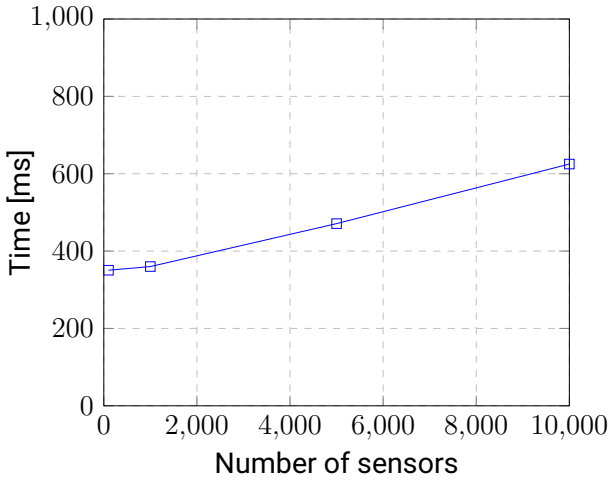
Nous avons évalué le temps de réponse du système, y compris (l'encodage des données, le déclenchement des règles, la réception de la demande d'autorisation d'accès et l'exécution de l'autorisation d'accès). Le délai mo-



(a) Temps d'encodage des données du capteur



(b) Délai de traitement du SRC.



(c) Temps de traitement de l'action.

FIGURE 5.5 – Résultats des tests d'évolutivité.

yen entre les évènements et les actions est de 3 s.

Nous avons également effectué de nombreux tests pour la scalabilité de la plateforme. Nous avons simulé des scénarios en utilisant jusqu'à 10 000, et avons observé les temps d'exécution des différentes parties de l'application. La figure 5.5 illustre les résultats. La figure 5.5a montre les temps d'encodage des informations données par les différents capteurs en observations cω-Model. La figure 5.5b donne le temps que le SRC prend pour traiter les observations et déclenche le LRS pour générer des actions. Quant à la figure 5.5c montre le temps nécessaire pour décoder les actions dans la

couche de communication. Pour chaque scénario, nous exécutons la plateforme plusieurs fois. Les tests ont été effectués sur deux machines distinctes. Le moteur de règles sémantiques et la couche de communication sémantique sont configurés respectivement dans la configuration matérielle suivante : quatre machines virtuelles exécutant Ubuntu 20.04 dans un processeur Intel Xeon E5-2620 à 2,00 GHz (12 cœurs), une RAM de 128 Go, un processeur graphique NVIDIA Quadro K5000 et un Pentium (R) double cœur 2,60 GHz.

5.3 SWRL vs LRS : Différences sémantiques

De facto, OWL est considéré comme un standard pour décrire des objets, des relations et des raisonnements. Cependant, voir les sections précédentes, nous pensons que cette norme n'est pas très bien adaptée aux systèmes distribués, en particulier pour les applications IdO. En effet, le caractère dynamique des entités impliquées dans de telles applications nécessite des formalismes pour manipuler des entités qui changent fréquemment dans le temps. Le processus de raisonnement doit être adapté à cette contrainte. OWL et cω-Model ont des constructions de modélisation similaires : les deux sont basés sur des notions de classes (concept), de propriété, d'instance et d'énumération. Cependant, il existe des différences significatives entre le raisonnement SWRL et le LRS, comme le montre la figure 5.6.

5.4 Discussion

Pour le bien-être humain, plusieurs solutions basées sur OWL ont été proposées. Pour ce faire, il fallait répondre à des exigences telles que l'agrégation des informations provenant de sources hétérogènes et la prise de décisions adéquates en conséquence. On peut noter que, malgré l'apport important des langages du W3C pour par exemple, faciliter la gestion et l'interprétation des informations hétérogènes, certains problèmes conceptuels et pratiques importants gênent encore l'utilisation de ces langages dans des applications IdO. La logique de description fournit un raisonnement com-

?AssistantDoctor(?doctor) /\ hasDomain(?doctor, ?domain) /\ ?Domain(?domain) /\ domainId(?domain, ?id) /\ swrlb:**notEqual**(?id, ?domain) ⟶ **not possible to trigger an action in SWRL**	**rule "CheckDomainOfSubject "** **conditions** ?domain:=Domain(?domainId:=id); ?assistant:= AssistantDoctor (?hasid:=hasHumainId, ?works:=hasdomainId); ?assistant (**not** (hasdomainId == ?domainId) **actions** AlertDifferentDomainMessage ?send_message := createInstance(AlertDifferentDomainMessage); ?send_message -> toDomain := ?domainId; **execute**(?send_message); **end**
?Person(?samuel) /\ hasPosition(?samuel, ?position) **not possible to get a new localization to update Samuel's position** ⟶ hasPosition(?samuel, **???????**) **Retracting of old values is not possible in the SWRL.** *SRL* allows real-time Samuel localization tracking. The problem with SWRL is that the ontology keeps all the localization positions. Thus, SWRL cannot update system beliefs regarding the environment and Samuel position. The first line in the condition part of the **SpaceLocation** rule captures outputs of the localization sensor. The *hasValue* property links the observation to quality values in the SSN ontology, which describe the actual values produced Space Name Value, which has a list of location names produced by the location sensor. The property *isProducedBy* associated with the LocationOutput Concept describes the position. The variable ?**sensor** associated with the localization sensor creates a relationship between ?human and the ?*spacename*. The ontology is then updated with action operations.	**rule** "SpaceLocation" **conditions** ?detect := LocationOutput(?spacename := one (hasValue), ?sensor := isProducedBy); ?sensor(?human := wearedBy); **actions** ?human>locatedAt := ? spacename; **update**(?human); **end**
SWRL is monotonic, thus does not support negation: ?person(?p) /\ ~~**not**~~ hasAspirinAllergy(?p,?aspirinallergy) SRL allows checking if a human does not have an aspirin allergy. Not possible to model such a piece of knowledge in SWRL. SRL relies on non-monotonic reasoning that supports negation as failure or assertions retraction or update.	**rule** "AspirinAllergyChecking" **conditions** Person(not (AspirinAllergyOutput()) , ?wears:= hasTag)); **actions** **execute any action** **end**

FIGURE 5.6 – Différences sémantiques concernant SWRL/LRS. Notez que l'intelligence ambiante repose sur l'identification et la localisation de personnes et d'objets à l'intérieur de divers espaces (maisons, bâtiments). Ces informations de localisation sont utiles, par exemple, pour reconnaître un contexte, analyser le comportement d'une personne, protéger un accès à une ressource ou choisir le service le plus approprié (proximité du service avec la position actuelle de l'utilisateur, préférences de l'utilisateur, etc.). swrlb est un Built-in [2], un langage extensible et modulaire pour le langage SWRL

plet et est prise en charge par des outils tels que Pellet, c'est pourquoi la LD est apparue comme un formalisme dans la représentation symbolique des connaissances. De plus, du point de vue des règles, la version OWL 2 introduit trois sous-langages (sous-ensembles syntaxiques) appelés profils. Les trois profils OWL 2 peuvent offrir des avantages dans des scénarios d'application particuliers, mais sont plus restrictifs. Cependant, plusieurs chercheurs ont tenté d'étendre la syntaxe d'OWL. Néanmoins, utiliser ces extensions pour enrichir la version standard du langage OWL nécessite de changer la majorité des outils existants. En fait, OWL et ses variantes sont i) caractérisés par une « expressivité limitée » (bien connue) d'un point de vue de la représentation/inférence des connaissances qui les rend inadaptés pour la protection de l'environnement au bien-être humain et ii) aborder en conséquence la représentation des connaissances et de raisonnement. Ainsi, suivre le paradigme d'hypothèse de monde ouvert" - donne certainement lieu à des incohérences logiques dans le contexte des systèmes distribués tels que les applications IdO. Comme déjà indiqué tout au long de ce mémoire, OWL n'adhère pas au paradigme UNA, alors que les applications IdO typiques doivent suivre l'hypothèse du monde fermé (CWA) et l'utilisation de l'UNA (c'est-à-dire, permettent d'identifier l'appareil de manière unique). Même si SWRL peut aller bien au-delà d'OWL, il soulève plusieurs limitations, comme l'absence de négation par l'échec. SWRL correspond aux règles Horn, ne peut pas déclencher d'action (autrement dit, il ne prend pas en charge le principe des règles réactives), ne peut pas rétracter les anciennes valeurs/instances, figure 5.6.

5.5 NKRL & Blockchain : Améliorer la protection de l'environnement et la gestion sémantique des connaissances distribuées

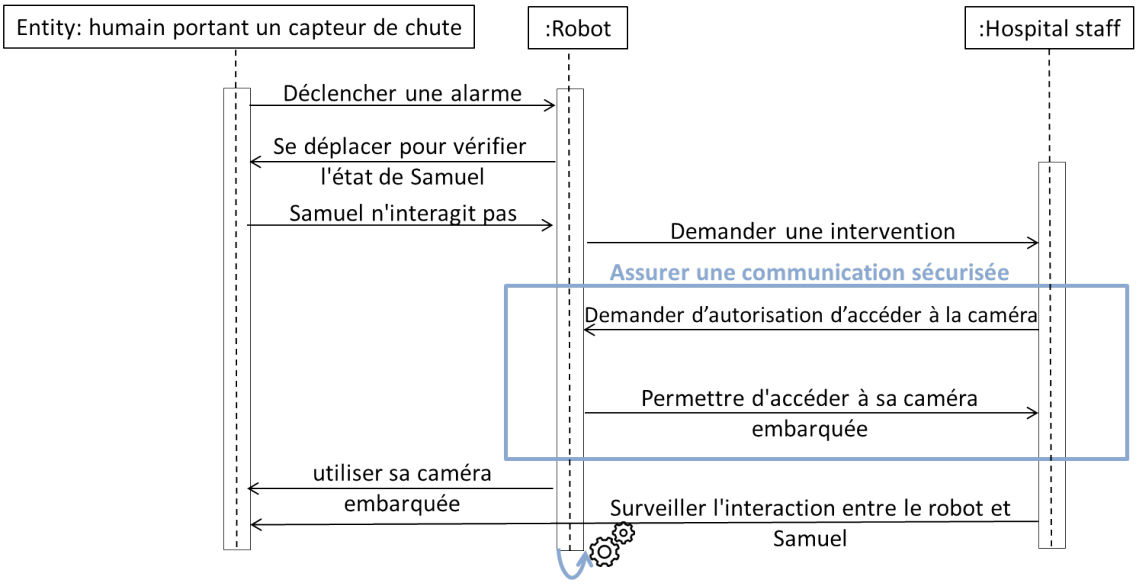


FIGURE 5.7 – Le diagramme de séquences du scénario.

Considérons une application dédiée au suivi de personnes âgées à domicile. Nous supposons que John porte un capteur de chute. Ainsi, les informations contextuelles pertinentes considérées dans ce cas d'utilisation sont : 1) La localisation précise de John ; 2) Le statut de Jean (inconscient/-conscient). La seconde information contextuelle n'est pas directement mesurable ; par conséquent, il obéit à des processus complexes.

Plusieurs évènements/actions doivent être corrélés et analysés au fur et à mesure qu'ils se produisent dans le temps et dans l'espace pour déterminer le statut de John et évaluer le contexte/la situation actuelle. Le premier objectif consiste à comprendre ce qui se passe après le déclenchement d'une alarme, figure 5.7. Dans ce cas, le système doit pouvoir déduire la situation de John à partir des informations disponibles. Il s'agit de fournir une rétroaction, avertir le personnel hospitalier, et permettre au personnel hospitalier d'évaluer son état de santé à l'aide d'une caméra embarquée sur le robot en attendant l'arrivée du personnel d'urgence. Le deuxième objectif

consiste à assurer une communication sécurisée qui préserve la confidentialité et les mécanismes d'authentification. En effet, le médecin de l'hôpital vérifiera l'état de santé de la personne en observant l'interaction entre le robot et John. Pour ce faire, le médecin doit accéder à distance à la caméra embarquée du robot. Comme déjà étudié par [Mazhar et al. (2021)], ce type de service et de prise de décision sont difficiles à réaliser. En effet, il s'agit de garantir le bon déroulement des actions telles que permettre au personnel hospitalier d'accéder à distance à la caméra de sécurité intérieure de la maison ou à une caméra embarquée dans un robot pour évaluer la santé mentale et physique des personnes, etc.

5.5.1 Hyperledger Fabric et les systèmes complexes distribués

Hyperledger Fabric est une plateforme distribuée open source de la Fondation Linux. Elle établit une confiance décentralisée dans un réseau. Seules les données que nous voulons partager sont échangées entre les participants concernés (i.e., assurer des contrôles de confidentialité avancés). Hyperledger Fabric est une Blockchain dédiée à la création de consortium, ce qui signifie que les participants (autrement dit les organisations) sont identifiés et peuvent ne pas se faire confiance. De plus, elle fournit des protocoles de consensus permettant aux organisations (multi-domaines) de personnaliser leur protocole de consensus. Chaque participant contrôle un ou plusieurs pairs (i.e., un nœud dans la chaîne) et doit traiter un code Blockchain comme non fiable et malveillant puisque n'importe qui peut déployer dynamiquement un contrat intelligent. De plus, les appareils IdO sont limités en énergie, ce qui nécessite une alimentation autonome pour récupérer l'énergie ambiante. Actuellement, les appareils IdO ne fournissent pas la puissance de calcul requise dans un réseau Blockchain. En effet, tous les appareils IdO génèrent une quantité considérable de données, créent des blocs et participent au protocole consensuel basé sur le POW (Proof of Work), qui a une latence élevée (fréquence de bloc de 10 min) [Reyna et al. (2018)], ce qui le rend inadapté pour traiter les évènements/contextes décrits dans l'application ci-dessus. Contrairement à d'autres registres distribués comme Ethereum et Bitcoin, au sein de HF, le principe de traitement des transactions suit

les platesformes d'architecture d'exécution-commande-validation. Le processus se fait en trois étapes. Premièrement, HF exécute une transaction et vérifie son exactitude avant de l'approuver. Deuxièmement, commandez les transactions via un protocole de consensus, et à la fin, il valide la politique d'approbation des transactions avant de les valider dans le grand livre. En s'appuyant sur l'identité des participants, HF peut utiliser à sa convenance un protocole de consensus qui ne nécessite pas de minage coûteux, tel que crash tolérant aux pannes ou Byzantine Fault Tolerance [Li et al. (2021)]. Cette conception répond aux défis de résilience, de flexibilité, d'évolutivité, de confidentialité et de sécurité. Ce qui rend HF plus adapté pour répondre aux exigences de l'IdO et effectuer une transaction, synchroniser les informations partagées en temps réel et réduire la latence du réseau.

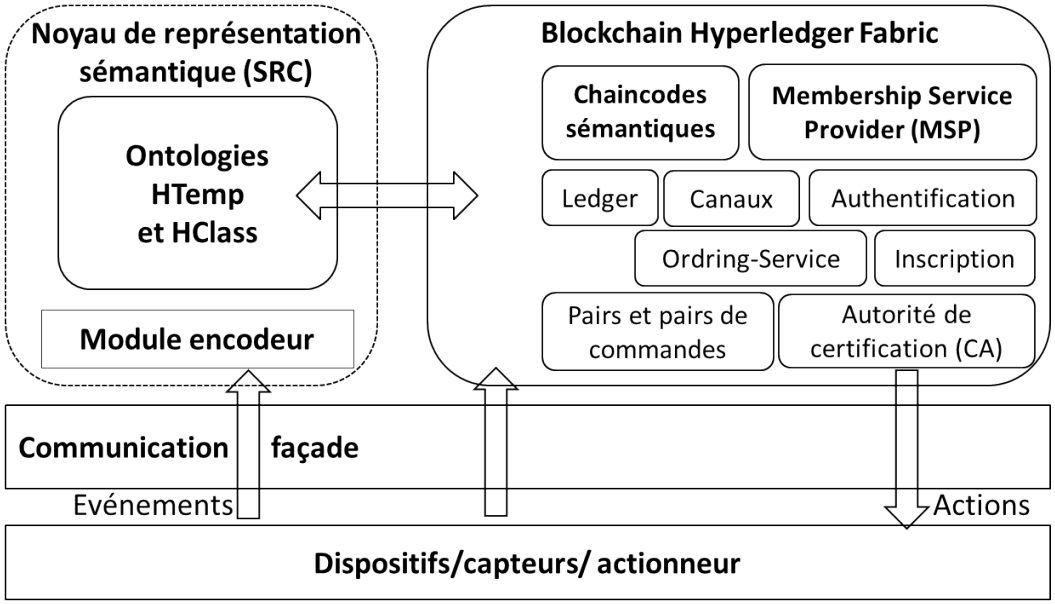


FIGURE 5.8 – Vue d'ensemble des couches d'architecture de la fusion des ontologies Blockchain et NKRL.

La figure 5.8 présente un aperçu des couches d'architecture de la fusion de la Blockchain et de l'ontologie NKRL. Il comprend trois couches logicielles faiblement couplées : le composant de communication Façade, le module Hyperledger Fabric, l'ontologie HTemp et l'ontologie HClass. Le composant de communication de Façade fait abstraction de l'accès aux capteurs et aux actionneurs. Il permet de collecter des données numériques. Le mo-

dule Encodeur transforme les données d'évènements de bas niveau d'entités virtuelles ou physiques générées par des capteurs en une abstraction de niveau supérieur de connaissances complexes et structurées grâce à une représentation conceptuelle. Une fois l'identité d'un appareil authentifiée, les données contextuelles sémantiques sont extraites. Des actions basées sur la connaissance du domaine, représentées dans les ontologies HClass/H-Temp et dont la sémantique est véhiculée par le contrat intelligent (i.e., Smart Contract) sont générées. Un robot compagnon équipé de divers capteurs et actionneurs fournit plusieurs services de haut niveau contrôlés à distance, comme permettre l'interaction vocale avec le personnel clinique.

Créer un lien sémantique entre les données numériques de bas niveau issues des systèmes de perception tels que la localisation avec les représentations sémantiques de haut niveau de l'ontologie. Un concept défini dans une ontologie HClass devient identifiable à partir des informations générées par des entités IdO de différentes modalités multimédias (signaux biométriques, vidéo, position, signaux physiologiques comme la fréquence cardiaque, la pression artérielle), mais aussi d'évènements et de situations complexes et structurés impliquant des interactions mutuelles et des relations entre les entités de niveau inférieur et la nécessité de prendre en compte de vastes informations spatiotemporelles.

5.5.2 Environnement d'exécution

L' architecture s'appuie sur l'ontologie NKRL entrelacée avec Hyperledger Fabric. Ainsi, un niveau d'abstraction plus élevé des objets et des évènements permet aux modules HF et Semantic Representation Core (SRC) de partager les mêmes connaissances, et donc de partager une compréhension commune de la structure du contexte sémantique. Dans ce scénario, nous considérons que le réseau du consortium (participants) est constitué de trois organisations : robot, hôpital et maison. Seul hôpital participe avec un pair (i.e., un nœud) et un nœud de commande (i.e., ordering peers), dans la mesure où le robot et la maison participent avec deux pairs et deux nœuds de commande. Le robot est responsable de la mise en place de la version initiale du réseau. Le robot a également le privilège de créer des canaux et de démarrer

les nœuds de commande.

Seuls les canaux entre le robot et la maison sont privés. Chaque canal a son registre, qui est répliqué sur d'autres pairs. Ces pairs sont intégrés au réseau Fabric à l'aide de l'autorité de certification. Les les nœuds de commande reçoivent des blocs et génèrent des transactions validées avant de s'engager dans la copie du registre du nœud. Cependant, seuls les nœuds de commande au sein des organisations de robots et maison approuvent les pairs puisqu'ils ont installé le code de chaîne. Le module MSP et les nœuds de commande (i.e., ordering peers) sont les principaux composants car ils établissent un consensus sur les transactions, maintiennent la liste des participants et associent les appareils IdO du réseau à des identités cryptographiques. Les contrats intelligents déployés sur des canaux s'exécutant dans un Docker [3] génèrent un programme exécutable.

L' API Fabric SDK est utilisée pour invoquer les contrats intelligents à partir d'une application cliente. Elle permet d'approuver les transactions et d'interagir avec les enregistrements du grand livre Blockchain. Ce dernier est composé de deux composants : l'état du monde et le journal des transactions. Le premier représente une base de données du grand livre et sert à décrire l'état du grand livre à un instant donné. Quant au composant du journal des transactions, il s'agit de l'historique mis à jour de l'état du monde.

Étant donné que HF est une plateforme de grand livre distribué, les membres s'enregistrent et s'authentifient auprès de la Blockchain avant d'effectuer des transactions sur le réseau. Le composant Authentification vise à établir un environnement sécurisé pour la communication entre pairs. Il gère et vérifie les identités des pairs et authentifie les messages échangés entre les pairs impliqués dans l'interaction.

À cet effet, une Infrastructure à Clés Publique (en Anglais Public Key Infrastructure (PKI)) permet de vérifier les identités à travers une chaîne de confiance. Le composant MSP vérifie que la transaction signée par le pair avec sa clé privée est valide en utilisant la clé publique correspondante. Ainsi, le MSP est l'épine dorsale de tous les systèmes puisqu'il permet à chaque appareil IdO d'être reconnu et approuvé par les membres du réseau. En effet, le MSP contient toutes les identités autorisées et intègre la chaîne

3. https://www.docker.com/

de confiance des membres de l'organisation qui ont rejoint le réseau.

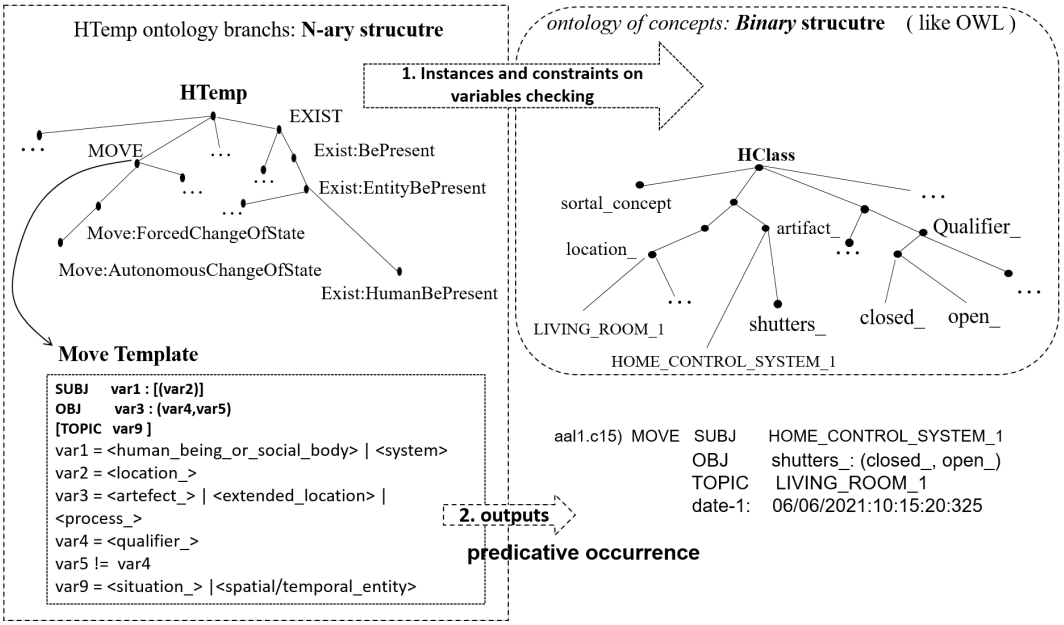


FIGURE 5.9 – Annotation des données numériques extraites du capteur en connaissances sémantiques. Cette figure illustre le processus d'annotation des données d'un capteur dans une occurrence de prédicat. Par exemple, lorsque l'utilisateur ou le système ouvre le volet, un évènement est envoyé au module Encodeur pour effectuer l'appariement avec le modèle NKRL afin de le transmettre au composant SRC.

Les pairs conservent toutes les données stockées dans le grand livre. Cependant, lorsque la confidentialité et la préservation de la vie privée via des canaux sont requises, les participants peuvent développer des sous-réseaux (en évitant de créer un canal séparé) pour réduire la visibilité des membres sur un ensemble de transactions. Ainsi, le nombre de participants autorisés à accéder au code Blockchain et à obtenir des données privées est réduit. Le sous-groupe s'appuie sur une fonctionnalité de données privées pour permettre les collectes entre les sous-réseaux sur un canal. Ils utilisent l'API de code Blockchain PutPrivateData et GetPrivatDataHash pour stocker des données privées et vérifier si elles correspondent aux hachages en chaîne créés à partir de données privées dans les blocs précédents. Dans un tel cas, le sous-groupe conserve le hachage de données pour la validation de la transaction et les données traitées. Les données IdO (c'est-à-dire la proposition de transaction qui contient l'identité du client (selon le MSP)) émises par

les appareils IdO sont envoyées à leurs pairs. Après avoir exécuté le contrat intelligent, le pair répond au client de l'application si la transaction est approuvée (c'est-à-dire validée). Le service de commande crée le bloc, puis le grand livre est mis à jour.

5.6 Mise en œuvre et résultats

Nous implémentons la solution sur trois environnements différents du même réseau. La Fabric 2.3 a été déployée en tant qu'application Blockchain sous-jacente et configurée dans la configuration matérielle suivante : Quatre machines virtuelles exécutant Ubuntu 20.04 dans un processeur Intel Xeon E5-2620 à 2,00 GHz (12 cœurs), une RAM de 128 Go et un GPU NVIDIA Quadro K5000 pour agir en tant que nœuds périphériques IdO. La couche d'abstraction fonctionne sur un processeur double cœur Pentium (R) à 2,60 GHz, avec 8 Go de RAM. Le composant SRC fonctionne sur un processeur Intel Core i7, avec 8 Go de RAM, et nous utilisons node.js pour écrire le code de chaîne et les applications client.

La représentation conceptuelle des évènements par des occurrences de prédicats nécessite la définition d'un modèle générique faisant l'appariement sémantique entre les modèles NKRL et un évènement observé dans l'environnement. Ainsi, les relations entre les entités du monde réel et leurs représentations sémantiques sont définies par le modèle, permettant ainsi une correspondance sémantique. Par exemple, à partir des descriptions des propriétés d'un capteur/actionneur et du prédicat MOVE, il est possible de représenter l'action « ouvrir le volet du salon ». Notez que les rôles SUBJ(ect) et OBJ(ect) sont obligatoires. Ainsi, le modèle d'appariement prend des valeurs d'entrée telles que HOME_CONTROL_SYSTEM_1 comme SUBJ(ect), et des informations temporelles correspondant à l'évènement d'ouverture. Le modèle génère l'occurrence de prédicat correspondante, figure 5.9. Ainsi, l'interface de communication assure une représentation cohérente des situations du monde en traitant les liens entre l'abstraction du monde réel et la base de connaissances. De ce fait, l'architecture proposée assure l'homogénéité de la base de connaissances.

Après la détection de l'évènement de chute, la chaincode correspondante

installée sur le robot est lancée, puis une demande d'autorisation d'accès à la caméra du robot est exécutée. Ainsi, la couche de communication permet de convertir la requête en commandes pour accéder à la caméra du robot. Par conséquent, la plateforme peut traduire cette action de message en commandes. Grâce à Hyperledger Fabric, le robot vérifie l'identité de l'hôpital à l'aide d'un fournisseur de services MSP, en faisant abstraction de tous les mécanismes cryptographiques et en validant les certificats et l'authentification des utilisateurs. Une fois ce processus terminé, l'action Message visuel est approuvée et le robot permet aux membres de l'hôpital d'accéder à sa caméra intégrée.

Hyperledger Fabric, par défaut, s'appuie sur NoSql LevelDB pour stocker les valeurs de clé publique, et chaque entité (c'est-à-dire, membre) a sa propre identité Blockchain qui ne s'enregistre qu'une seule fois. Dans notre scénario, nous utilisons un nœud de commande. Nous nous limiterons à mentionner ici que le nœud de commande peut gérer environ 100 transactions par bloc en utilisant le mode Solo pour la mise en œuvre du nœud de commande. Cela signifie que le nœud de commande coupe les blocs lorsque le nombre de transactions atteint un BatchSize (c'est-à-dire 100 transactions/-bloc). En effet, HF exécute une transaction (chaque transaction contient des signatures et est soumise à des pairs sur un canal), vérifie son exactitude avant de l'approuver et valide la politique d'approbation des transactions avant de les valider dans le grand livre. Ainsi, les avantages d'Hyperledger Fabric consistent principalement à : i) permettre uniquement aux membres identifiables (par exemple, robot, capteurs, personnel hospitalier) d'effectuer des actions dans le consortium, ii) chaque organisation (hôpital, maison et robot) gère ses membres (c'est-à-dire, nœuds) et avec la collaboration du module de commande et d'adhésion (MSP), ils établissent un consensus sur les transactions et associent les appareils IdO du réseau à des identités cryptographiques. Cette conception traite de la résilience, de la flexibilité, de l'évolutivité et de la confidentialité, ce qui rend HF plus adapté pour répondre aux exigences de l'IdO et réduire la latence du réseau. Enfin, le déploiement de Fabric 2.3 en tant que Blockchain sous-jacente de la plateforme n'a pas eu d'impact négatif sur le temps de réponse. Nous avons réalisé des expérimentations pour valider le temps nécessaire à une action

pour se produire et avons évalué le temps de réponse du système après observation du contexte, obtention de l'accès à la requête caméra et exécution de la commande d'accès. Le temps de réponse inclut le temps de traitement dans la couche de communication, ainsi que le temps de génération de l'action et d'envoi de la commande à un dispositif actionneur. Nous avons soumis 100 transactions à partir de capteurs au pair de type ordering. Nous avons mesuré le temps entre la soumission d'une transaction, y compris la date d'écriture dans le code Blockchain et son engagement envers le grand livre. Figure 5.10 indique le temps d'approbation de toutes les transactions. Les résultats obtenus montrent que les transactions sont endossées en moins d'une seconde dans la plupart des cas, et la durée moyenne pour approuver une transaction est de 819,77 ms, figure 5.11 . Nous avons répété la même chose avec cinq capteurs émettant 100 transactions à un débit de cinq transactions par seconde, figure 5.12. L' analyse des performances de HF est étudiée par de nombreux auteurs, tels que ([Canhui et al. (2020), Caixiang et al. (2020)]). Les auteurs ont étudié la performance et le goulot d'étranglement dans l'Hyperledger de chaque phase de commande de services et d'évolutivité des pairs endosseurs qui valident une transaction. Leurs expériences visent à évaluer les plateformes de technologies Blockchain telles que Hyperledger et Ethereum. Tous les auteurs ont souligné que l'analyse comparative est difficile dans les systèmes de Blockchain publics, par contre, les Blockchains autorisées (i.e., privées, en Anglais permissioned) permettent de meilleures performances. De plus, les auteurs dans [Suporn et al. (2017)] ont comparé les plateformes Hyperledger Fabric et Ethereum en fixant le nombre de transactions de 1 à 10000. Les auteurs ont conclu que HF surpasse Ethereum. C'est pourquoi nous avons choisi HF puisque seuls les membres restreints ont accès au réseau. La mise en œuvre de concepts d'ancrage définis dans des ontologies avec les entités présentes dans l'environnement permet d'ajouter de l'intelligence aux appareils IdO. Il représente la principale difficulté à surmonter.

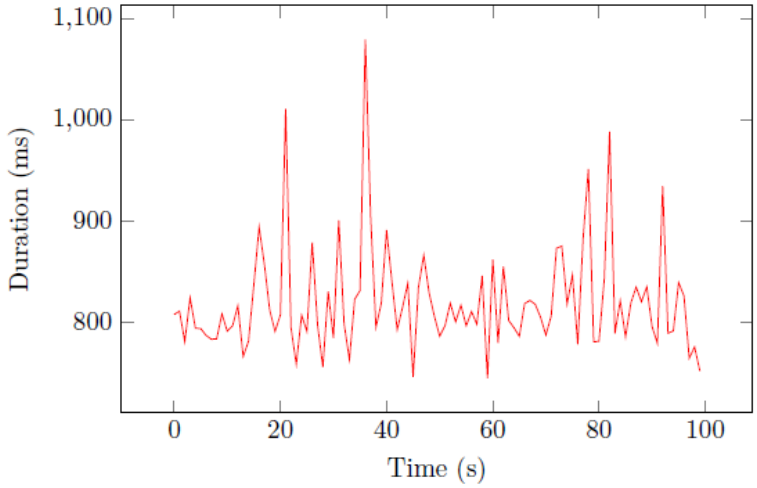


FIGURE 5.10 – Durée d'approbation de 100 transactions à partir d'un capteur.

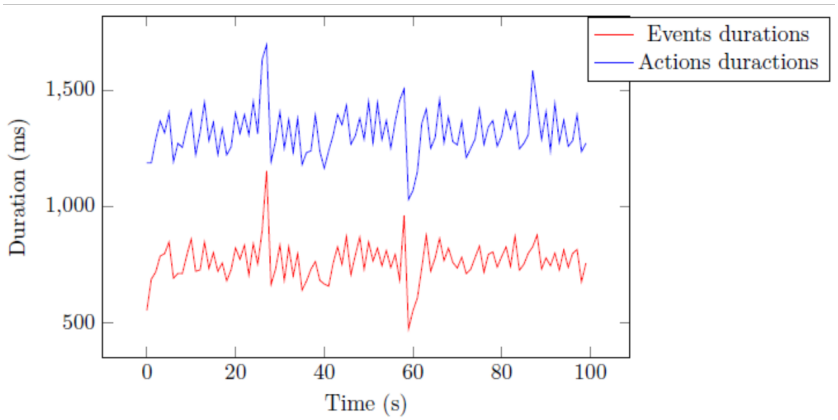


FIGURE 5.11 – Durée d'approbation de la transaction et le déclenchement de l'action correspondante.

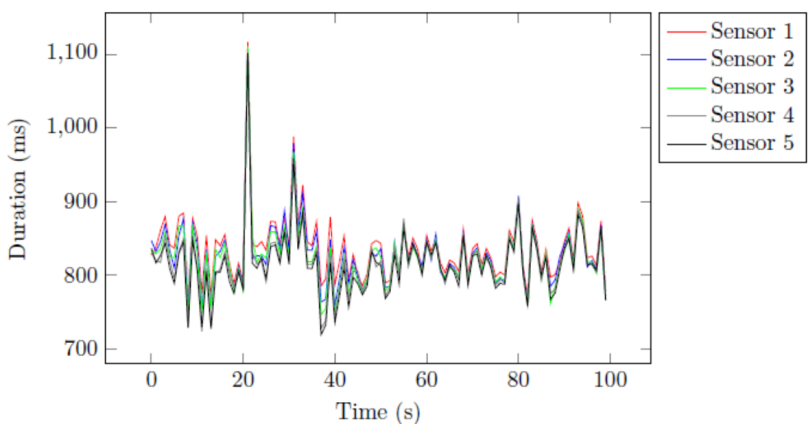


FIGURE 5.12 – Durée d'approbation de 100 transactions à partir de cinq capteurs.

5.7 Conclusion

Il existe des propositions pour supporter la représentation de relations n-aires ; toutefois, elles sont définitivement exclues du langage OWL 2 et ses variantes. En effet, ces propositions ont inutilement augmenté la complexité du raisonnement dans différentes couches ontologiques. Par conséquent, il reste des problèmes importants qui ne sont pas traités par OWL 2 qui le rend inadapté dans des applications Internet des Objets. Les travaux présentés dans cette thèse ont démontré que la mise en œuvre du contrôle d'accès pour les systèmes distribués via les modèles XACML, cω-Model et NKRL assurent l'intégrité, la vérification, l'authentification, la sécurité et la confidentialité des messages, et permet de partager des connaissances contextuelles sémantiques afin d'invoquer un ou plusieurs services. En effet, les formalismes que nous explorons permettent des descriptions sémantiques des caractéristiques dynamiques (i.e., qui changent fréquem-ment) des entités impliquées dans les applications IdO. Par ailleurs, nous avons proposé une architecture sémantique reposant sur XACML et HF pour assurer l'intégrité et l'authentification des connaissances tout en préservant la confidentialité et la protection de l'environnement de l'humain. L' utilisation d'une Blockchain de consortium dans laquelle tous les pairs n'ont pas les mêmes droits pour approuver une transaction proposée est un inconvénient potentiel de l'architecture proposée. Au sein du HF, seuls quelques pairs peuvent vali-

der les transactions. En raison du fait qu'il s'agit d'une technologie émergente, nous devrions explorer l'utilité du principe de la Blockchain publique décentralisée.

5.8 Publications

Les travaux de cette thèse nous ont permis de faire deux publications (revues), la première dans une revue de catégorie A et la seconde dans la catégorie B (scopus). De plus, une conférence IEEE :

Intitulé de la première revue :
International Journal of Ad Hoc and Ubiquitous Computing ISSN : 1743-8233 EISSN : 1743-8225.
Catégorisation de la revue : A
Accès vers revues catégorie A : https://www.univ-usto.dz/wp-content/uploads/2021/02/Liste-desrevues-scientifiques-de-Categorie-A-2021.pdf
Titre de la revue :
XACML-based Semantic Rules Language and ontological model for reconciling semantic differences of access control rules.

Url de la revue :
https://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijahuc

---

Intitulé de la seconde Revue :
Journal of Telecommunications and Information Technology ISSN : 15094553 quarterly with 4 issues EISSN : 18998852
Catégorisation de la revue : B (scopus)
Accès vers revues catégorie B (scopus) :
https://www.univ-usto.dz/wpcontent/uploads/2021/02/Liste-SCOPUS.pdf
Titre de la revue :
Semantic Knowledge Management and Blockchain-based Privacy for Internet of Things Applications.
Url de la revue/article :
https://www.il-pib.pl/czasopisma/JTIT/2022/3/75.pdf

---

intitulé de la conférence :

IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS)

Titre du papier :

Ontological-based ABAC and Blockchain Organizational Cooperation Framework for Security Management in AmI environment

Lien vers la conférence :

http://www.idaacs.net/elfinder/connector?_token=FI8Qv0oZ23BEdRJ3qoLPz5SIGDMvfTfZgAvKu0M2&cmd=file&target=fls2_cHVibGljL2NvbmZlcmVuY2VzLzcvV1RQL1ByZWZpbmFsIFRlY2huaWNhbCBQcm9ncmFtIHYuMDkucGRm

Conclusion Génarale

Le choix entre les hypothèses CWA et OWA est important et dépend de la capacité du système d'inférence utilisé. Dans ce contexte, de nombreux chercheurs ont étudié la différence dans les décisions prises par un système confronté aux mêmes situations à travers des scénarios concrets. Ainsi, ni SWRL ni OWL ne conviennent à un raisonnement réactif sur des connaissances dynamiques dont la valeur de vérité peut évoluer dans le temps. En effet, un tel raisonnement peut conduire dans certains cas à des décisions d'autorisation conflictuelles ou erronées lorsqu'une ressource est accessible dans un environnement ouvert et dynamique (c'est-à-dire multi-domaine). Cependant, certaines de ces limitations peuvent être dépassées avec les éléments intégrés (built-in en Anglais). Toutefois, la méthode intégrée n'exprime pas de règles complexes qui traitent de nombreux attributs, tels que ceux utilisés dans nos scénarios et requis par le langage XACML. L' encodage statique des politiques dans XACML manque d'expressivité sémantique, d'interopérabilité et de capacités de raisonnement. Il ne permet donc pas de traduire une politique sans perdre de sémantique lorsqu'une demande d'accès passe d'un domaine à un autre. Par conséquent, il est nécessaire de s'appuyer sur un modèle sémantique associant une politique XACML à des annotations sémantiques pour faciliter l'appariement entre des entités de politique de différents domaines. Notre approche répond à cette limitation critique en s'appuyant sur un modèle ontologique qui offre une nouvelle ontologie abstraite en plus des représentations politiques proposées : XACML.

La plateforme proposée surmonte les inconvénients des technologies du Web sémantique telles qu'OWL/RDF-S. Elle pourrait répondre aux exigences IdO courantes telles que la protection des appareils IdO contre les applications/utilisateurs et l'exécution de certaines actions non autorisés. Par conséquent, cette approche œuvre pour l'intérêt du bien-être humain,

la protection de son environnement et la bonne prise en charge de sa santé. Nous pouvons conclure qu'une plateforme basée sur une ontologie améliore les capacités des applications IdO à collecter, récupérer, partager, manipuler et analyser les données des capteurs. Notre contribution du domaine de l'ontologie est longuement discutée tout au long de cette thèse. Nous soulignons ici qu'OWL a été explicitement conçu pour les besoins du Web sémantique. Il peut avoir des difficultés à traiter des problèmes complexes en intelligence artificielle (par exemple, les comportements humains et les évènements complexes). Basés sur la notion de prédicat sémantique et de rôles fonctionnels en tant que classes générales d'évènements, les modèles de NKRL traitent les problèmes ci-dessus.

Perspectives

La principale limitation de l'approche proposée survient lorsqu'une règle XACML contient une obligation qui nécessite d'effectuer une autre action ou expression de conseil. Nous devrions explorer l'utilité de ces expressions dans nos travaux futurs. Nous comptons travailler sur ce point à court terme, et en particulier tester les scénarios sur une Blockchain publique. Comme objectif à long terme, nous pensons travailler sur l'apprentissage profond et les ontologies. Dans ce contexte, deux thèses sont en cours à l'université de Bordj Bou Arreridj et encadrées par Mr. Sabri, ce qui ouvre la voie à travailler en étroite collaboration sur l'aspect protection de la vie privée et sécurité d'accès basées l'apprentissage profond. Nous pouvons situer cette nouvelle perspective dans l'étude réalisée par [Maulana et al. (2021)]. Les auteurs utilisent la technologie IdO et l'apprentissage profond pour le suivi en temps réel des patients souffrant d'insomnie. Ce système offre la possibilité d'obtenir des informations que les patients recueillent depuis longtemps à leur domicile grâce à des capteurs intégrés. Les informations de santé collectées peuvent être envoyées à un médecin distant pour une analyse de données supplémentaire basée sur le système d'apprentissage profond pour évaluer et diagnostiquer la qualité du sommeil.

Bibliographie

Bylander, T. "A critique of qualitative simulation from a consolidation viewpoint". IEEE Trans. Syst. Man Cybern. 18(2) : 252-263, 1988.

Neches, R., Fikes, R.E., Finin, T., Gruber, T.R., Senator T., and Swartout W.R. "Enabling technology for knowledge sharing". AI Magazine 12(3) :36–56, 1991.

Gruber, T.R. "A translation approach to portable ontology specification". Knowledge Acquisition 5(2) :199–220, 1993.

Borst, W. N., Akkermans, J. M., and Top, J. L. "Engineering Ontologies". International Journal of Human-Computer Studies, 46 : 365-406, 1997.

Uschold M. and Grüninger M., "Ontologies : Principles, Methods and Applications". Knowledge Engineering Review 11(2) :93–155, 1996.

Studer, R., Benjamins, V.R., and Fensel, D. "Knowledge Engineering : Principles and Methods. IEEE Transactions on Data and Knowledge Engineering". 25(1-2) :161–197, 1998.

Guarino, N. "Formal Ontology in Information Systems". In : Guarino N (ed) 1stInternational Conference on Formal Ontology in Information Systems (FOIS'98). Trento, Italy. IOS Press, Amsterdam, pp3–15, 1998.

Gruninger, M. and Fox, M. S. "The Logic of Enterprise Modelling". In J. Brown and D. O' Sullivan (eds.), Reengineering the Enterprise. Chapman and Hall, 1995.

Gangemi, A., Pisanelli, D., and Steve, G. "Ontology Alignment : Experiences With Medical Terminologies". In N. Guarino (ed.) Formal Ontology in Information Systems. IOS Press (this volume), 1998.

Borst, W. N., Akkermans, J. M., and Top, J. L."Engineering Ontologies". International Journal of Human-Computer Studies, 46 : 365-406, 1997.

Uschold, M., King, M., Moralee, S., and Zorgios, Y. " The Enterprise Ontology". The Knowledge Engineering Review (to appear), 1998.

Uschold, M. Jasper, R."A Framework for Understanding and Classifying Ontology Applications". Proceedings of the IJCAI-99 Workshop on Ontologies ans Problem-Solving Methods, Stockholm, 1999.

Van Zyl, J. Corbett, D. "Population of a Framework for Understanding and Classifying Ontology Applications". Proceedings of the ECAI-00 Workshop on Applications of Ontologies and Problem-Solving Methods, Berlin, 2000.

Gómez-Pérez A., Fernández-López M.,and Oscar C. “Ontological Engineering, with examples from the areas of Knowledge“, Management, e-Commerce and the Semantic Web, ISBN 1-85233-551-3 Springer, 2004.

Chaudhri VK, Farquhar A, Fikes R, Karp PD, Rice JP. "Open Knowledge Base Connectivity 2.0.3". Technical Report, 1998.

Fikes, R., and Kehler, T. "The role of frame-based representations in reasoning". Communications of the ACM 28 : 904–920, 1985.

Lenat DB, Guha RV. "Building Large Knowledge-based Systems : Representation and Inference in the Cyc Project". Addison-Wesley, Boston, Massachusetts, 1990.

Motta E. "Reusable Components for Knowledge Modelling : Principles and Case Studies in Parametric Design". IOS Press, Amsterdam, The Netherlands, 1999.

Kifer M, Lausen G, Wu J. "Logical Foundations of Object-Oriented and Frame-Based Languages". Journal of the ACM 42(4) : 741–843, 1995.

MacGregor R. "Inside the LOOM clasifier". SIGART bulletin 2(3) :70–76. 1991.

T. Berners-Lee, R. Fielding, L. Masinter. "Uniform Resource Identifiers (URI) : Generic Syntax". Request for Comments 2396, IETF, 1998.

Hebeler J., Fisher M., Blace R., Perez-Lopez A., Mike Dean. “Semantic Web Programming“, Published by Wiley Publishing, Inc. ISBN : 978-0-470-41801-7, 2009.

Weiser, M. "The computer for the 21st century". Scientific American 265(3), 94–104, 1991, https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf

Karp, P. D., Chaudhri, V. K., Thomere, J. "XOL : An XML-based ontology exchange language". 1999. https://www.sri.com/wp-content/uploads/2021/12/676.pdf.

Horrocks I, Fensel D, Harmelen F, Decker S, Erdmann M, Klein M. "OIL in a Nutshell". In : Dieng R, Corby O (eds) 12th International Conference in Knowledge Engineering and Knowledge Management (EKAW’00). Juan-Les-Pins, France. (Lecture Notes in Artificial Intelligence LNAI 1937) Springer-Verlag, Berlin, Germany, pp 1–16, 2000.

Fensel D, van Harmelen F, Horrocks I, McGuinness LD, Patel-Schneider PF. "OIL : An ontology infrastructure for the Semantic Web". IEEE Intelligent Systems their applications 16(2) :38–44, 2001.

Corcho, O. Gomez-Perez, A. "Evaluating Knowledge Representation and Reasoning Capabilities of Ontology Specification Languages". Proceedings of the ECAI-00 Workshop on Applications of Ontologies and Problem-Solving Methods, Berlin, pp. 3/1-3/9, 2000.

Baader, F., Calvanese, D., McGuinness, D., Nardi, D., and Patel-Schneider, P.F., eds. "The Description Logic Handbook :Theory, Implementation, and Applications". Cambridge : Cambridge University Press, ISBN 0-521-78176-0, 2003.

Tammet, T., Draheim, D., Järv, P. "GK : Implementing Full First Order Default Logic for Commonsense Reasoning (System Description)". In : Blanchette,

J., Kovács, L., Pattinson, D. (eds) Automated Reasoning. IJCAR 2022. Lecture Notes in Computer Science(), vol 13385. Springer, Cham, 2022.

Ziang L., Roberto M.M., Fei X., Jiajun W., Li F.F. "BEHAVIOR in Habitat 2.0 : Simulator-Independent Logical Task Description for Benchmarking Embodied AI Agents". CoRR abs/2206.06489. 2022.

Sylvain C., Yacine G.D., Stéphane L., Gilles R. "SALT : A simple application logic description using transducers for Internet of Things". ICC 3006-3011. 2013.

Nicola V., Giuseppina G. "Reasoning on objects and grasping using description logics". Adv. Robotics 33(13) : 616-635, 20190.

Sudeepta P., Sugyan K.M., Chouhan K.R., Narayan C.D., Anirban S. "Enrichment of Semantic Sensor Network Ontology : Description Logics based approach". ICIT : 995-1000, 2020.

Yoji Y., Naoto H., Hirofumi N., Tatsuya D., Misao K. "A study of coordination logic description and execution for dynamic device coordination services". CoRR abs/1804.00704, 2018.

Gianluca C., Domenico L., Riccardo R., Domenico F.S. "Privacy Preserving Query Answering in Description Logics Through Instance Indistinguishability (Discussion Paper)". SEBD 2021 : 490-497, 2021.

Claudia C., Magdalena O., Nir P. "Closed- and Open-world Reasoning in DL-Lite for Cloud Infrastructure Security (Extended Abstract)". Description Logics 2021.

Kartik G., C.G., Ria R., Prateek A., Vishu M. "FaD-CODS Fake News Detection on COVID-19 Using Description Logics and Semantic Reasoning". Int. J. Inf.Technoll. Web Eng. 16(3) : 1-20. 2021.

Kifer M, Lausen G, Wu J. "Logical Foundations of Object-Oriented and Frame-Based Languages". Journal of the ACM 42(4) : 741–843, 1995.

Ronghan L., Zejun J., Lifang W. "Representing RCPBAC (Role-Involved Conditional Purpose-Based Access Control) in Ontology and SWRL". BICS 697-706, 2018.

Qiang G., Guohua S., Zhiqiu H., Changbo K. "The Application of SWRL Based Ontology Inference for Privacy Protection". J. Softw. 9(5) : 1217-1222, 2014.

Runumi D., Deepti M., Hajer B.Z., Ghada B. "SWRL reasoning on ontology-based clinical dengue knowledge base". Int. J. Metadata Semant. Ontologies 14(1) : 39-53, 2020.

Armando O., Luis E., Hugo O., Luis M. "Comparing Drools and Ontology Reasoning Approaches for Automated Monitoring". In Telecommunication Processes, Procedia Computer Science, Volume 95, Pages 353-360, 2016.

Sirin, E., Parsia, B. , Grau, B. C., Kalyanpur, A., Katz, Y. "Pellet : A Practical OWL-LD Reasoner". Web Semantics : Science, Services and Agents on the World Wide Web 5 (2), 2007.

Volker H., Kay H., Ralf M., and Michael W. "The RacerPro Knowledge Representation and Reasoning Systems", Semantic Web Journal, IOS Press, 2011.

Bertino, E., Provetti, A., Salvetti, F. (2003). Local Closed-World Assumptions for reasoning about Semantic Web data. Proc of the APPIAGULPPRODE Conf on Declarative Programming AGP 03 (pp. 314-323).

Gelfond, M., and Lifschitz, V. "The stable model semantics for logic programming". In Kowalski, R., and Bowen, K., eds., Proceedings of International Logic Programming Conference and Symposium, 1070–1080. MIT Press, 1988.

Moore, R. "Semantical considerations on nonmonotonic logic". Artificial Intelligence 25(1) :75–94, 1985.

Reiter, R. 1980. A logic for default reasoning. Artificial Intelligence 13 :81–132.

Grimm, S., Motik, B. (2005). Closed World Reasoning in the Semantic Web through Epistemic Operators. CEUR Proceedings of the OWL Experiences and Directions Workshop Galway Ireland (Vol. 188).

Hustadt, U. "Do we need the closed-world assumption in knowledge representation ? ". In Reasoning about Structured Objects : Knowledge Representation meets Databases (KRDB'94), 1994.

Heflin H., Avila, H. M."Lcw-based agent planning for the semantic web". In Ontologies and the Semantic Web, WS-02-11, pages 63-70. AAAI Press, 2002.

Kolovski. V., Parsia, B., Katz,y., Hendler J. "Representing Web Service Policies in OWL-LD". In Proc. of the 4th Intern. Semantic Web Conf.(ISWC), 2005.

Damasio, C. V., Analyti, A., Antoniou, G., Wagner, G. "Supporting Open and Closed World Reasoning on the Web. Principles and Practice of Semantic Web Reasoning", 4187(506779), 149. Springer Berlin Heidelberg. 2006.

Claudia C., Magdalena O., Nir P. "Closed- and Open-world Reasoning in DL-Lite for Cloud Infrastructure Security". KR 2021 : 174-183, 2021.

Henrik F., Evgeny K., Evgenij T. "On Equivalence and Cores for Incomplete Databases in Open and Closed Worlds". ICDT 2020 : 10 :1-10 :21, 2020.

Joachim B., Martin B., Michael B. "Inference control of open relational queries under closed-world semantics based on theorem proving". Inf. Syst. 70 : 32-47, 2017.

Marcelo A., Martín U. "Designing a Query Language for RDF : Marrying Open and Closed Worlds". PODS 2016 : 225-236, 2016.

Vinicius M., Iara A., José P. M. de Oliveira. "Are The Integrations Between Ontologies and Databases Really Opening the Closed World in Ubiquitous Computing ?". SEKE, 453-458, 2014.

Sloman, M. "Policy driven management for distributed systems". Journal of Network and Systems Management, Vol. 2, No. Part 4, pp.333–360, 1994.

Scheffler, T., Schindler, S. and Schnor, B. "Using AOP-based enforcement of prioritised XACML policies for location privacy", Int. J. Internet Technol. Secur. Trans., Vol. 5, No. 1, pp.84–104, 2013.

Mourad, A. and Jebbaoui, H. "SBA-XACML : set-based approach providing efficient policy decision process for accessing web services". Expert Syst. Appl., Vol. 42, No. 1, pp.165–178, 2015.

Fan, D., Zhenhua, Y., Wenjing, L., Xiaoqing, L., Yu, F., Ben, Q., Chaoyang, X. and Zhiwu, L. "An efficient policy evaluation engine for XACML policy management", Information Sciences Inf. Sci., Vol. 547, pp.1105–1121, 2021.

Kudo, M. and Hada, S. "XML document security based on provisional authorization". Proceedings of the Seventh ACM Conference on Computer and Communications Security, Athens, Greece, November, pp.87–96, 2000.

Compton, M., Barnaghi, P., Bermudez, L., García-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., Huang, V., Janowicz, K., Kelsey, W.D., Phuoc, D.L., Lefort, L., Leggieri, M., Neuhaus, H., Nikolov, A., Page, K., Passant, A., Sheth, A. and Taylor, K. "The SSN ontology of the W3C semantic sensor network incubator group". Web Semantics : Science, Services and Agents on the World Wide Web, Vol. 17, pp.25–32, ISSN : 1570-8268, websem. 2012.

Sejdiu, B., Ismaili, F. and Ahmedi, L. "A management model of real-time integrated semantic annotations to the sensor stream data for the IoT", WEBIST, pp.59–66. 2020.

G.P. Zarri, “A knowledge representation tool for encoding the ‘meaning’ of complex narrative texts”, Natural Language Engineering, vol. 3, pp. 231–253, 1997.

Mazhar, N., Salleh, R., Zeeshan, M. and Hameed, M.M. "Role of device identification and manufacturer usage description in IoT security : a survey", IEEE Access, Vol. 9, pp.41757–41786, ISSN : 2169-3536, 2021.

Reyna, A., Cristian, M., Chen, F., Soler, E., and Díaz, M. “On blockchain and its integration with IoT. Challenges and opportunities”, J. Future Generation Computer Systems, vol. 388, pp. 173–190, 2018.

Abunadi, I.; Kumar, R.L. BSF-EHR : Blockchain Security Framework for Electronic Health Records of Patients. Sensors 2021, 21, 2865. 2021.

Nguyen, D. C., Pathirana, P. N., Ding, M. and Seneviratne, A. "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems" in IEEE Access, vol. 7, pp. 66792-66806, 2019.

J. Huang, Y. W. Qi, M. R. Asghar, A. Meads and Y. -C. Tu, "MedBloc : A Blockchain-Based Secure EHR System for Sharing and Accessing Medical Data," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 594-601, 2019.

U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for industry 4.0 : a comprehensive review,". IEEE Access, vol. 8, pp. 79 764–79 800, 2020.

Kim, M., Laskowski, M., Nan, N. "A First Step in the Co-Evolution of Blockchain and Ontologies : Towards Engineering an Ontology of Governance at the Blockchain Protocol Level". SSRN Electronic Journal, 2018.

Li, Y., Qiao, L., and Lv, Z. “An Optimized Byzantine Fault Tolerance Algorithm for Consortium Blockchain”, Peer-to-Peer Netw. Appl, vol. 18, pp. 2826–2839, 2021.

Caixiang, F. Sara, G, Hamzeh, K. and Petr, M. "Performance Evaluation of Blockchain Systems : A Systematic Survey", journal IEEE Access, volume 8, pages 126927-126950, 2020.

Canhui, W. and Xiaowen, C. "Performance Characterization and Bottleneck Analysis of Hyperledger Fabric", 40th IEEE International Conference on Distributed Computing Systems, ICDCS 2020, Singapore, 2020.

Suporn, P., Chaiyaphum, S., Suttipong, T. "Performance analysis of private blockchain platforms in varying workloads", 26th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2017.

Maamar, Z., Noura, F., Ejub, K., MuhammadA. and Ayesha, Q."OWL-T for a Semantic Description of IoT". ADBIS (Short Papers) : 108-117, 2020.

Wirawit, C., Masahiro, B., Noboru, K. and Ken, S. "Human Localization Sensor Ontology : Enabling OWL 2 DL-Based Search for User’s Location-Aware Sensors in the IoT". ICSC : 107-111, 2016.

Nakul, G., Yang, B. and Nirupam, R. "Owlet : enabling spatial information in ubiquitous acoustic devices'. MobiSys : 255-268, 2021.

Sharma, N., Mangla, M., Mohanty, S.N., Gupta, D., Tiwari, P., Shorfuzzaman, M. and Majdi, R. "A smart ontology-based IoT framework for remote patient monitoring". Biomed. Signal Process. Control. 68 : 102717.

Denker, G., Kagal, L. and Finin, T. "Security in the Semantic Web using OWL". Information Security Technical Report. 10(1), 51-58, 2005.

Safyan, M., Qayyum, Z.U., Sarwar, S. , Raúl-García, C. and Mehtab, A.R. "Ontology-driven semantic unified modelling for concurrent activity recognition (OSCAR)". Multimed Tools Appl 78, 2073–2104, 2019.

Choudhury, O., Rudolph, N., Sylla, I., Fairoza, N. and Das, A. "Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules". IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 963-970, 2018.

Li, M., Xia, L. and Seneviratne, O. "Leveraging Standards Based Ontological Concepts in Distributed Ledgers : A Healthcare Smart Contract Example". IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 2019.

HÍolbl, M. ; Kompara, M. ; Kamišalić, A. ; Nemec Zlatolas, L. "A Systematic Review of the Use of Blockchain in Healthcare". Symmetry, 2018.y,

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., Burgelman J.-C. "Scenarios for Ambient Intelligence in 2010". IST Advisory Group Final Report, European Commission, February 2001, EC. Brussels, ISBN 9289407352. 2001.

Emile A., Rick H., Martin S., Chapter. "Ambient Intelligence". In The Invisible Future : The Seamless Integration Of Technology Into Everyday Life, McGraw-Hill Companies, 2001.

Atzori, L., Iera, A., and Morabito, G. "The Internet of Things : A survey," Computer Networks, vol. 54, no. 15, p. 2787–2805, October 2010.

Casagras, "Final Report, RFID and the Inclusive Model for the Internet of Things," 2009. Available : https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf

Dong, Z., Yian, Z., Wangbao, L., Jianhua, G., Yunlan, W. "Object service provision in Internet of Things". Proceedings of the International Conference on e-Education, e-Business, eManagement, and e-Learning (IC4E'10), 2010.

Jara, A. J., Zamora, M. A., Skarmeta, A. F. G. "An architecture based on Internet of Things to support mobility and security in medical environments". Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC), 2010.

Bandyopadhyay, S., Sengupta, M., Maiti, S., Dutta, S. (2011). Role of middleware for Internet of Things : a study. International Journal of Computer Science Engineering Survey, 2(3), 94–105 ; 2011.

Broll, G., Paolucci, M., Wagner, M., Rukzio, E., Schmidt, A., Hussmann, H. (2009). Perci : pervasive service interaction with the Internet of Things. IEEE Internet Computing, 13(6), 74–81.

Bondi AB. "Characteristics of scalability and their impact on performance". In : Workshop on Software and Performance ; pp. 195–203. 2000.

Ganz, F., Li, R., Barnaghi, P., and Harai, H. "A Resource Mobility Scheme for Service-Continuity in the Internet of Things," in IEEE International Conference on Green Computing and Communications, 2012.

Fu, H.L., Lin, P., Yue, H., Hua, G.M., and Lee, C.P. "Group mobility management for large-scale machine-to-machine mobile networking". IEEE Vehicular Technology Society, vol. 63, no. 3, p. 1296–1305, 2014.

Elsaleh, T, Gluhak, A., and Moessner, K."Service continuity for subscribers of the mobile real world Internet". In IEEE International Conference on Communications Workshops (ICC), 2011.

Jussi K., Alfredo D.E., Francesco M., Pasi H., Janne T.M., Arto Y., Juha-Pekka S., Tullio C. "Semantic interoperability architecture for pervasive computing and internet of things". Access IEEE. 2 :856–73, 2014.

Elkhodr, M., Shahrestani, and H. Cheung, H."The Internet of Things : New Interoperability, Management and Security Challenges," International Journal of Network Security & Its Applications (IJNSA), vol. 8, no. 2, pp. 85-102, 2016.

Wang, S., Zhang, X., Zhang, Y., Wang, L., Yang, J., and Wang. W. "A survey on mobile edge networks : Convergence of computing, caching and communications". IEEE Access, 5 :6757–6779, 2017.

Siow E., Tiropanis T., Hall W. "Analytics for the internet of things : a survey". ACM Comput Surv. 2018 ;51(4) :74 :1-74 :36.

Haimour Jnd Abu-Sharkh, O. "Energy Efficient Sleep/Wake-up Techniques for IOT : A survey". IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 478-484, 2019.

Elsts A, Mitskas EOG. Distributed ledger technology and the internet of things : a feasibility study. Proc 1st Workshop Blockchain-Enabled Netw Sens Syst. 11 :7–12. 2018.

Klinefelter A, Roberts NE, Shakhsheer Y, Gonzalez P, Shrivastava A, Roy A, Craig K, Faisal M, Boley J, Oh S, Zhang Y, Akella D, Wentzloff DD, Calhoun BH. 21.3 a 6.45 w self-powered IdO soc with integrated energy-harvesting power management and ulp asymmetric radios. In : 2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers, . pp. 1–3, 2015.

Johannes, G., and Eric B.. “A systematic literature review of model-driven security engineering for cyber–physical systems”. In : Journal of Systems and Software 169, p. 110697, 2020.

Nivedita, M., Sharnil, P., Chirag, I.P., Nagaraj, G.C., Kirit, M., Pooja, S., Madhuri, C., Sudha, P., Ketan, K. Memcached : An Experimental Study of DDoS Attacks for the Wellbeing of IoT Applications. Sensors 21(23), 8071, 2021.

Sicari, S., Rizzardi, A., Grieco, L.A., and Coen-Porisini, A.”Security, privacy and trust in internet of things : The road ahead,” Computer Networks, 76 :146–164, 2015.

K. T. Nguyen, K.T., Laurent, M., and Oualha, N. “Survey on secure communication protocols for the internet of things,” Ad Hoc Networks, 32 :17–31, 2015.

Dimitrios, A., Nikolaos, T., George, P., Dennis, H., Rita, K., Hugo, M., João, J., João, Q. "SmartWork : An IoT Enabled Unobtrusive Worker Health, Wellbeing and Functional Ability Monitoring Framework". IJCCI, 398-408. 2021.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P.,and Sikdar, B. "Goyal and B. Sikda “A Survey on IoT Security : Application Areas, Security Threats, and Solution Architectures”. In : IEEE Access 7, pp. 82721–82743, 2019.

Leonardo, B., Kyle, D., Berkay, C., Patrick D., McDaniel, A., Selcuk, U. "A survey on IoT platforms : Communication, security, and privacy perspectives". Comput. Networks 192 : 108040, 2021.

Xu, B., Xu, D.L., Cai, H., Xie, C., Hu, J. and Bu, F. "Ubiquitous data accessing method in IdO-based information system for emergency medical services". IEEE Transactions on Industrial Informatics, vol. 10, no. 2, p. 1578–1586, 2014.

Ullah, S. M. A., Islam, M. M., Mahmud, S., Nooruddin, S., Raju, S. M. T. U., and Haque, M. R. “Scalable Telehealth Services to Combat Novel Coronavirus (COVID-19) Pandemic”. SN Comput. Sci., vol. 2, no. 1, p. 18, Feb. 2021.

Graham, C. M., and Jones, N. “Impact of IoT on geriatric telehealth,” Work. with Older People, vol. 24, no. 3, pp. 231–243, Aug. 2020.

Rokonuzzaman, MD., Hossain, M.I., Islam, T., Sarkar, P.P, Islam, M.R., Amin, N. “Design and Implementation of Telehealth Device : Linking IoT Sensors to Cloud Networks”. IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES), pp. 281–285. 2021.

Ayshwarya B., and Velmurugan, R. “Intelligent and Safe Medication Box In Health IoT Platform for Medication Monitoring System with Timely Remainders”. In 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1828–1831. 2021.

Harsha Vardhini, P. A., Harsha, M. S., Sai, P. N., and Srikanth, P. “IoT-based Smart Medicine Assistive System for Memory Impairment Patient”. In 12th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 182–186. 2020.

Sundaravadivel, P., Kesavan, K., Kesavan, L., Mohanty, S.P., and Kougianos, E. "Smart-Log : A deep-learning based automated nutrition monitoring system in the Iot", In IEEE Transactions on Consumer Electronics, volume 64, number 3, pages 390– 398, 2018.

Norfeldt, L., Botker, J., Edinger, M., Genina, N., Rantanen, J. "Cryptopharmaceuticals : increasing the safety of medication by a blockchain of pharmaceutical products". J. Pharm. Sci-Us. 108(9) :2838–2841, 2019.

Chen, H.S., Jarrell, J.T., Carpenter, K.A., Cohen, DS., Huang, X. "Blockchain in healthcare : a patient-centered model". Biomed J Sci Tech Res. 20(3) :15017–15022.2019.

Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y. "MedBlock : efficient and secure medical data sharing via blockchain". J Med Syst. 42 :136, 2018.

Sharma, A., Tomar, R., Chilamkurti, N., and Kim, B.G. “Blockchain based smart contracts for internet of medical things in e-healthcare”. Electronics, vol. 9, no. 10, p. 1609, 2020.

Zhang, X., and Poslad, S. “Blockchain support for flexible queries with granular access control to electronic medical records (EMR)”. In Proceedings of the IEEE International conference on communications (ICC), pp. 1–6, Kansas City, MO, USA, May 2018.

Adly AS, Adly AS. Adly MS approaches based on artificial intelligence and the internet of intelligent things to prevent the spread of COVID-19 : scoping review. J Med Internet Res. 22(8), e19104, 2020.

Chatterjee P, Tesis A, Cymberknop LJ, Armentano RL. Internet of things and artificial intelligence in healthcare during COVID-19 pandemic-A South American perspective. Front Public Health. 8 :600213, 2020.

Cui M, Baek SS, Crespo RG, Premalatha R. "Internet of things-based cloud computing platform for analyzing the physical health condition". Technol Health Care. 2021.

Y. Zhang, J. Cui, K. Ma, H. Chen, and J. Zhang, “A wristband device for detecting human pulse and motion based on the internet of things,” Measurement, vol. 163, 2020.

Kelati, A. “Biosignal monitoring platform using Wearable IdO,” in Proceedings of the 22st Conference of Open Innovations Association FRUCT, pp. 9–13, Petrozavodsk, Russia, May 2018.

Almusaylim, Z.A., Zaman, N., "A review on smart home present state and challenges : linked to context-awareness internet of things (IoT)". Wirel. Netw. 25 (6), 3193–3204, 2019.

S.A. Celtek, M. Durgun, H. Soy. "Internet of things based smart home system design through wireless sensor/actuator networks". In : 2nd International Conference on Advanced Information and Communication Technologies (AICT) , IEEE, 2017, pp. 15–18, 2017.

K. Guravaiah, R. Leela Velusamy, Prototype of home monitoring device using Internet of Things and river formation dynamics-based multi-hop routing protocol (RFDHM), IEEE Trans. Consum. Electron. 65 (3), pp : 329–338, 2019.

Dipankar, C., Athman, B., Sajib, M.. "A Conflict Detection Framework for IoT Services in Multi-resident Smart Homes". CoRR abs/2004.12702, 2020.

S. Canale, A. Di Giorgio, F. Lisi, M. Panfili, L. Ricciardi Celsi, V. Suraci and F. Delli Priscoli. "A Future Internet Oriented User Centric Extended Intelligent Transportation System," in 24th Mediterranean Conference on Control and Automation (MED), 2016.

Yang, J. ; Han, Y. ; Wang, Y. ; Jiang, B. ; Lv, Z. ; Song, H. Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city. Future Gen. Comput. Syst. in press, 2017.

Al-Dweik, A. ; Muresan, R. ; Mayhew, M. ; Lieberman, M. "IdO-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems". In Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), Windsor, Canada, pp. 1–6, 2017.

Hari Baabu, V., Senthil Kumar, G., Deb, P., Rai, A. "Smart Parking Assist System using Internet of Things". International Journal of Control Theory and Applications, 9(40), 2016.

Z. Chen, S. Chen and X. Feng, "A design of distributed storage and processing system for Internet of Vehicles," in 8th International Conference on Wireless Communications Signal Processing (WCSP), 2016.

O. Kaiwartya, A. Abdul Hanan, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin and X. Liu, "Internet of Vehicles : Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," IEEE Access, vol. 4, pp. 5356 - 5373, 2016.

Kouicem, D.E., Abdelmadjid, B., Hicham, L. "Internet of things security : A top-down survey". Computer Networks, Elsevier, Computer Networks Volume 141, Pages 199-221, 4 August 2018.

E. Leloglu, A review of security concerns in internet of things, J. Comput. Commun. 5 (1), pages : 121–136, 2017.

Abomhara, M. ; Koien, G.M. "Cyber Security and the Internet of Things : Vulnerabilities, Threats, Intruders and Attacks". J. Cyber Security. Mobil, 4, 65–88. 2015.

Aumasson, J. P., Henzen, L., Meier, W., Naya-Plasencia, M. "Quark : A lightweight hash". Journal of cryptology, 26(2), 313. 2013.

Makhdoom, M. Abolhasan, J. Lipma n, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019.

Sowmya Ravidas, Alexios Lekidis, Federica Paci, Nicola Zannone, Access control in Internet-of-Things : A survey, Journal of Network and Computer Applications, Volume 144, Pages 79-101, ISSN 1084-8045, 2019.

R. Santos, K. Bennett, E. Lee, Blockchain : Understanding its Uses and Implications, The Linux Foundation, 2021.

Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications 126,pp : 45–58, 2019.

Kapil Sharma, Deepakshi Jain. "Consensus Algorithms in Blockchain Technology : A Survey". ICCCNT 2019 : 1-7

Eric Y., and Jin, T. "Attributed based access control (ABAC) for Web services". In IEEE International Conference on Web Services (ICWS'05). IEEE, 2005.

Nonita Sharma , Monika Mangla , Sachi Nandan Mohanty, Deepak Gupta, Prayag Tiwari , Mohammad Shorfuzzaman , Majdi Rawashdeh : A smart ontology-based IoT framework for remote patient monitoring. Biomed. Signal Process. Control. 68 : 102717, 2021.

Mehdi Gheisari, Hamid Esmaeili Najafabadi, Jafar Ahmad Abed Alzubi, Jiechao Gao , Guojun Wang, Aaqif Afzaal Abbasi, Aniello Castiglione : OBPP : An ontology-based framework for privacy-preserving in IoT-based smart city. Future Gener. Comput. Syst. 123 : 1-13, 2021.

Yasir Imtiaz Khan , Maryleen U. Ndubuaku : Ontology-based automation of security guidelines for smart homes. WF-IoT, 35-40, 2018.

Xing Wu, Fengxia Han, Hao Deng. "An Ontology Based Resource Description Model for Blockchain-IoT". QRS Companion : 935-940, 2021.

Paulo Henrique Cardoso Alves , Isabella Zalcberg Frajhof, Fernando A. Correia, Clarisse S. de Souza, Hélio Lopes. "Controlling Personal Data Flow :

An Ontology in the COVID-19 Outbreak using a Permissioned Blockchain". ICEIS (2) 2021 : 173-180, 2021.

Junjian, L., Zhengxing, H., Xudong, L., Huilong, D. "An ontology-based real-time monitoring approach to clinical pathway". In : 2014 7th International Conference on Biomedical Engineering and Informatics. IEEE, 2014. p. 756-761, 2014.

Elsaleh, T., Enshaeifar, S., Rezvani, R., Thomas Acton, S., Janeiko, V., Bermúdez-Edo, M. "IoT-Stream : A Lightweight Ontology for Internet of Things Data Streams and Its Use with Data Analytics and Event Detection Services". Sensors 20(4) : 953, 2020.

Kuster, C., Hippolyte, J.L., Et Rezgui, Y. "The UDSA ontology : An ontology to support real time urban sustainability assessment". Advances in Engineering Software, vol. 140, p. 102731, 2020

Sai, S.L.C., Aritran, P., Sudip, M., Maanak, G., Anupam, J. "A Smart-Farming Ontology for Attribute Based Access Control". BigDataSecurity. HPSC/IDS 2020 : 29-34, 2020.

Toumia, A., Szoniecky, S., Saleh, I."ColPri : Towards a Collaborative Privacy Knowledge Management Ontology for the Internet of Things". FMEC pp : 150-157, 2020.

Serrano, M., Gyrard, A., Tragos, E.Z., Hung, Dang, N. "FIESTAIoT Project : Federated Interoperable Semantic IoT/cloud Testbeds and Applications". WWW (Companion Volume), 425-426, 2015.

Agarwal, R., Elsaleh, T., Et Tragos, E. "GDPR-inspired IoT Ontology enabling Semantic Interoperability, Federation of Deployments and Privacy-Preserving Applications". CoRR abs/2012.10314, 2020.

BrÍoring, A. Schmid, S., Schindhelm, C.K., Khelil, A., Käbisch, S., Kramer, D., Phuoc, D., Mitic, J., Anicic, D., Teniente, E. "Enabling IoT Ecosystems through Platform Interoperabilityé. IEEE Softw. 34(1) : 54-61, 2017.

Shulong, W., Yibin, H., Fang, G., Songsong, M. "Ontology-Based Resource Description Model for Internet of Things". CyberC, pp : 105-108, 2016.

Gheisari, M., H.E., Najafabadi, Alzubi, J.A., Gao, J., Wang, G., Abbasi, A.A., Castiglione, A. "OBPP : An ontology-based framework for privacy-preserving in IoT-based smart city". Future Gener. Comput. Syst. 123 : 1-13, 2021.

Schwee, J.H., Sangogboye, F.C., Johansen, A., Kjærgaard, M.B. "Ontology-Based Modeling of Privacy Vulnerabilities for Data Sharing". Privacy and Identity Management, pp : 109-125, 2019.

Mitrevski, A., Plöger, P.G., Lakemeyer, L. "Ontology-Assisted Generalisation of Robot Action Execution Knowledge". IROS pp : 6763-6770, 2021.

Akkaoui, R. "Blockchain for the Management of Internet of Things Devices in the Medical Industry". In IEEE Transactions on Engineering Management, pp :1-12, 2021.

Alsboui, T .A. A., Qin, Y., Hill, R., Al-Aqrabi, H. "Enabling distributed intelligence for the Internet of Things with IOTA and mobile agents". Computing 102(6) : 1345-1363, 2020.

Tahir, M., Sardaraz, M., Muhammad, S., Saud Khan, M. "A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics". Sustainability. 12(17) :6960, 2020.

Zhitao, G., Guanlin, S., Xiaosong, Z., Longfei, W., Nadra, G., Xiaojiang, D., Yinglong, M. "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities". IEEE Commun. Mag. 56(7) : 82-88, 2018.

Javier, H. "Attribute-based encryption implies identity-based encryption". IET Inf. Secur. 11(6) : 332-337, 2017.

Maulana, F. I., Febriantono, M. A., Raharja, D. R. B., Sofiani, I. R. and Al Hadid Firdaus, V. "Two Decade Mapping the Scientific Research of Internet of Things on Education - A Bibliometric Analysis". International Conference on Electrical and Information Technology (IEIT), pp. 114-119, 2021.

Afreen, H., Bajwa, I. S. "An IoT-Based Real-Time Intelligent Monitoring and Notification System of Cold Storage". In IEEE Access, vol. 9, pp. 38236-38253, 2021.

Morisset, C., Willemse, T.A.C., Zannone, N. "A framework for the extended evaluation of ABAC policies". Cybersecur. 2(1) : 6, 2019.

Gang, L. Wenxian, P., Yumin, T., Chen, L., Shancang, L. "A novel conflict detection method for ABAC security policies". J. Ind. Inf. Integr. 22 : 100200, 2021.

Al-Zubaidie, M., Zhang, Z., Zhang, J. "PAX : Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system". International Journal of Environmental Research and Public Health, vol. 16, no 9, p. 1490, 2019.

Shantanu, P., Michael, H., Vijay, V., Rabehaja, T.M. "Policy-based access control for constrained healthcare resources in the context of the Internet of Things". J. Netw. Comput. Appl. 139 : 57-74. 2019.

Nimalaprakasan, S., Jason, R., Farzad, S., Dawson, Ed. "A policy model for access control using building information models". Int. J. Crit. Infrastructure Prot. 23 : 1-10, 2018.

Rezvani, M., Rajaratnam, D., Ignjatovic, Ignjatovic, A., Pagnucco, M., Jha, S. "Analyzing XACML policies using answer set programming". Int. J. Inf. Secur. 18, 465–479, 2019.

Turkmen, F, Hartog, J.D., Ranise, S., Zannone, N. "Formal analysis of XACML policies using SMT". Comput. Secur. 66 : 185-203, 2017.

Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, G., Patiniotakis, I., Gouvas, P., Mentzas, G. "Achieving security-by-design through ontology-driven attribute-based access control in cloud environments". Future Gener. Comput. Syst. 93 : 373-391, 2019.

Riad, K. and Cheng, J. "Adaptive XACML access policies for heterogeneous distributed IoT environments". Information Sciences.Volume(548) : 135-152, 2021.

Nisha, P., Shantanu, S., Sharad, M., Lukasz, K. and Nalini, V. "Smart Home Survey on Security and Privacy", journal CoRR, volume /abs-1904-05476, 2019.

Rafal, K., Michal, C., Marek, P., Witold, H., Dirk, P., Wilmuth, M., Ernst-Josef, B., Ioannis, L., Konstantinos, D., Roxana, H., Claire, L. and David, F. "Common Representational Model and Ontologies for Effective Law Enforcement Solutions", Vietnam Journal of Computer Science, 7(1), 1-18, 2020.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S. "Internet of Things security and forensics : Challenges and opportunities". Futur. Gener. Comput. Syst., vol. 78, pp. 544–546, 2018.

Zarpelão,B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C. " A survey of intrusion detection in Internet of Things". Journal of Network and Computer Applications, 2017, 84, 25–37, 2017.

Bradshaw, J., Uszok, A., Breedy, M., Bunch, L., Eskridge, T., Feltovich, P., Samuelson, M., Lott, J. and Vignati, M. "The KAoS Policy Services Framework". In Eighth Cyber Security and Information Intelligence Research Workshop (CSIIRW), 2013.

V. C. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations". National Institute of Standards and Technology (NIST) SP-800-162, 2014.

Tehsin, K., Ather, A.J., Adeel, A., Saif Ur Rehman, M., Abid, K., Naveed, A., Umar, M., Naeem Shehzad, M., Balubaid, M.A. "Privacy-aware relationship semantics-based XACML access control model for electronic health records in hybrid cloud". Int. J. Distributed Sens. Networks 15(6), 2019.

Damiano, D.F.M., Paolo, M., Laura, R. "A blockchain based approach for the definition of auditable Access Control systems. Comput. Secur. 84 : 93-119, 2019.

H. Liu, D. Han and D. Li, "Fabric-iot : A Blockchain-Based Access Control System in IoT". In IEEE Access, vol. 8, pp. 18207-18218, 2020.

Hang, L. ; Kim, D.-H. "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity". Sensors 2019, 19, 2228, 2019.

Dwivedi AD, Srivastava G, Dhar S, Singh R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors (Basel). Jan 15;19(2) :326, 2019.

Deng, F., Yu, Z., Zhang, L., Ge, X., Zhao, R., Li, X., Ma, Y., Yan, Y., Wen, Z. "Clustering and supervised response for XACML policy evaluation and management". Knowledge-Based Systems, Volume 205, 106312, 12 October 2020.

Arunkumar, S., Soyluoglu, B., Sensoy, M., Srivatsa, M., Rajarajan, M. 3Location attestation and access control for mobile devices using GeoXACML". J. Netw. Comput. Appl. 80 : 181-188, 2017.

Beomseok K. Woonseob S., DongYeop H., Ki-Hyung K. "Attribute-Based Access Control(ABAC) with Decentralized Identifier in the Blockchain-Based Energy Transaction Platform". ICOIN 2021 : 845-848, 2021.

Yan Z., Yao Q., Zhiyuan Z., Xiaoxu S., Guowei L., William C.C. "Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control". SCC 2018 : 193-200, 2018.

Xiaofeng L., Songbing F., Cheng J., Pietro L. "A Fine-Grained IoT Data Access Control Scheme Combining Attribute-Based Encryption and Blockchain'. Secur. Commun. Networks 2021 : 5308206 :1-5308206 :13, 2021.

Yingwen C., Linghang M., Huan Z., Guangtao X. "A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection". Wirel. Commun. Mob. Comput. 2021 : 6685762 :1-6685762 :12, 2021.

Sara R., Rafael B, Rui S.C., Ralph D. "Distributed attribute-based access control system using permissioned blockchain". World Wide Web 24(5) : 1617-1644, 2021.

Afnan A., Bradley D. T. "Attribute-based Access Control of Data Sharing Based on Hyperledger Blockchain". ICBCT 2020 : 135-139, 2020.

Daniel, D.L., Ginés, D.T., Félix, G.M., Gregorio, M.P. "Managing XACML systems in distributed environments through Meta-Policies". Comput. Secur. 48 : 92-115, 2015.

Panende, M.F., Prayudi, Y., Et Riadi, I. "Comparison of Attribute Based Access Control (ABAC) Model and Rule Based Access (RBAC) to Digital Evidence Storage (DES)". International Journal of Cyber-Security and Digital Forensics, vol. 7, no 3, p. 275-283. 2018.

Kanwal, T., Anjum, A., Malik, S.R., Khan, A., Khattak, M.A.K. "Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud". Comput. Stand. Interfaces 78 : 103522. 2021.

Drozdowicz, M., Ganzh, M., and Paprzycki, M. "Semantic Access Control for Privacy Management of Personal Sensing in Smart Cities". In Corr 2021, and In IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 1, pp. 199-210, 2020.

Drozdowicz, M., Ganzh, M., and Paprzycki, M. "Semantically Enriched Data Access Policies in eHealth". J. Medical Syst. 40(11) : 238 :1-238 :8. 2016.

Szczekutek, R., Ganzha, M., Paprzycki, M., Fidanova, S., Lirkov, I., Badica, C., Ivanovic, M. "System for semantic technology-based access management in a port terminal". In : AIP Conference Proceedings, Vol. 2025, (1) AIP Publishing LLC, 090002, 2018.

Fensel D., van Harmelen, F., Horrocks, I., McGuinness, LD., Patel-Schneider, PF. OIL : "An ontology infrastructure for the Semantic Web. IEEE Intelligent Systems their applications", 16(2) :38–44, 2001.