UNIVERSITE CHEIKH ANTA DIOP DE DAKAR (UCAD)

ECOLE DOCTORALE MATHS-INFORMATIQUE (EDMI)

Année : 2020 N° ordre : 00007277

THESE DE DOCTORAT UNIQUE

Spécialité : Télécommunications

Présentée par :

Jeanne Roux NGO BILONG

Titre : **Optimisation des modèles de contrôle d'accès des systèmes d'information basés sur la délégation de rôle**

Soutenu publiquement le 14/11/2020 devant le jury composé de :

Président :	Claude LISHOU, Professeur, UCAD de Dakar
Rapporteurs :	Ousmane THIARE, Professeur, UGB de Saint Louis
	Tegawendé F. BISSYANDE, Professeur, Université du Luxembourg
Examinateurs :	Samuel OUYA, Maître de conférences CAMES, UCAD de Dakar
	Ahmed Dooguy KORA, Professeur, ESMT de Dakar
Directeur de thèse:	Gervais MENDY, Maître de conférences CAMES, UCAD de Dakar

Thèse effectuée au sein du :

Laboratoire d'Informatique, Réseaux et Télécoms (LIRT)

Dakar, Fann, UCAD

Sénégal

Résumé

Un système d'information est un ensemble de ressources, à la fois humaines, matérielles et immatérielles dont le rôle est de collecter, stocker, traiter et distribuer de l'information. La définition de politiques de sécurité des systèmes d'information repose principalement sur trois critères que sont la confidentialité, la disponibilité et l'intégrité.

Un des aspects de la sécurité des systèmes d'information repose sur le contrôle d'accès aux données d'un système pour lequel différentes politiques de sécurité peuvent être mises en œuvre. Les politiques de contrôle d'accès aux données d'un système d'information reviennent à définir des modèles permettant d'assurer la confidentialité et l'intégrité de l'information.

La question de la délégation des rôles dans les modèles de contrôle d'accès basés sur la confiance reste un enjeu majeur car, au regard de la littérature jusqu'à présent, les critères de sélection permettant à un cédant (utilisateur capable de céder ses droits) de valider le niveau de confiance du bénéficiaire d'une délégation sont encore sous-évalués. Ce qui biaise la délégation et minimise la qualité de protection de la vie privée. En effet, une délégation de rôle sans une appréciation objective de la confiance pourrait exposer les données personnelles.

Une délégation partielle de rôle se conclut en général par la révocation. Les travaux menés jusqu'ici sur la révocation de délégation montrent que cette dernière a ses limites car elle ne se fait pas de façon automatique lorsque le temps imparti pour la délégation arrive à son terme. Ainsi, le cessionnaire qui délègue un rôle avec des cas d'exceptions liés à un contexte temporel ou géo-temporel doit gérer manuellement la révocation au terme de la délégation.
Dans cette thèse, nous proposons une amélioration des modèles de contrôle d'accès basés sur la délégation dynamique de rôle, la confiance et le contexte (temporel, géo-temporel). Nous faisons une évaluation quantitative de la confiance sur la base de critères de définitions de la confiance préalablement classifiés. Pour ce faire, nous avons utilisé des algorithmes d'apprentissage pour la classification des critères d'évaluation de la confiance afin de prédire l'erreur de confiance. Cette prédiction nous a permis de proposer un algorithme de scoring (score) afin d'afficher le bénéficiaire le plus digne de confiance.
En outre, nous proposons une amélioration du système de révocation et de préservation de la vie privée via la définition d'axiomes.

Nous utilisons la logique non-monotone T-JCLASSICδε pour effectuer une interprétation axiomatique des modèles et UML (Unified Modelling Language) pour l'analyse et l'implémentation du système. Le langage UML nous permet de représenter plusieurs diagrammes tels que le diagramme de cas d'utilisation et le diagramme de séquence. Nous implémentons les modèles dans des environnements appliqués à l'E-learning et à l'E-santé. Ces environnements, pour le cas de l'E-learning, permettent aux enseignants de déléguer des rôles soit aux tuteurs pour des besoins de prise en charge des travaux dirigés, soit à leurs collègues de la même spécialité en cas d'indisponibilité. La délégation tient compte de la disponibilité du bénéficiaire et s'étend sur une période déterminée. Pour le cas de l'E-santé, le modèle prend en compte la protection de la vie privée des patients, en faisant intervenir l'internet des objets (l'IdO). Le médecin est seul habilité à accéder aux données du patient collectées via les capteurs et stockées dans une base de données. Les différents modèles proposés dans cette thèse contribuent à la mise en place de systèmes d'informations collaboratifs.
Les technologies utilisées dans le cadre de nos travaux de recherche sont WebRTC, Node.js et Kurento Media Server pour faciliter la communication en temps réel. Notre contribution améliore la notion de confiance dans le modèle de contrôle d'accès dynamique basé sur les rôles et la délégation. De plus, la composante dynamique de la délégation et de la révocation des rôles offre des plateformes efficaces, fiables, faciles à utiliser et stables. Les systèmes mis en place améliorent le travail collaboratif.

Mots-clés : contrôle d'accès, délégation, rôle, niveau de confiance, vie privée, organisation virtuelle, système intelligent

Contribution to information system access control models: minimizing trust errors and protecting privacy in a delegated role

Abstract

The definition of access control policies for information systems is mainly based on the concepts of authentication, confidentiality, trust, availability and integrity. The question of role delegation based on trust remains a major issue because, according to the literature, the selection criteria enabling an assignee to validate the level of trust of the beneficiary of a delegation are still under-evaluated. This biases the quality of delegation and limits the quality of privacy protection. Because, a delegation of role without an objective assessment of trust could expose the subject's personal data.

A partial delegation of role always ends in revocation. The work carried out so far on the revocation of delegation shows that the revocation of delegation has its limits because it does not happen automatically when the time limit for the delegation comes to an end. Thus, the assignee who delegates a role with exceptions related to temporal or geo-temporal contexts must manually manage the revocation at the end of the delegation.

In this thesis, we propose an improvement of access control models based on dynamic role delegation, trust and context (temporal, geo-temporal). We make an objective evaluation of trust based on previously classified trust definition criteria. To do so, we used learning algorithms for the classification of the trust evaluation criteria in order to predict the trust error. This prediction allowed us to propose a scoring algorithm in order to display the most trustworthy recipient.

In addition, we propose an improvement of the revocation and privacy system through the definition of axioms.

We use T-JCLASSICδε non monotonous logic to perform axiomatic interpretation of models and UML for analysis and implementation of the system. The Unified Modelling Language (UML) allows us to represent several diagrams such as use case diagram and sequence diagrams. We implement the models in environments applied to E-learning and E-health. These environments, in the case of E-learning, allow teachers to delegate roles either to tutors for the purposes of tutorials or to their colleagues in the same specialty in case of unavailability. The delegation takes into account the availability of the beneficiary and extends over a fixed period of time. In the case of E-Health, the model takes into account the protection of patients' privacy,

using the Internet of Things (IoT). Only the doctor has access to the patient data collected via the sensors and stored in a database. The different models proposed in this thesis contribute to the implementation of collaborative decision-making systems.

The technologies used in our research are WebRTC, Node.js and Kurento Media Server to facilitate real-time communication. Our contribution improves the notion of trust in the dynamic access control model based on roles and delegation. In addition, the dynamic component of role delegation and revocation provides efficient, reliable, easy to use and stable platforms. The systems put in place enhance collaborative work.

Keywords: access control, delegation, role, trust level, privacy, virtual organization, intelligent system

Remerciements

Mon aventure dans la recherche commence il y a de cela cinq ans. J'avais alors décidé de quitter mon poste de Directrice des études dans une école supérieure de la place à Dakar. Ne disposant que d'un master professionnel en informatique, je m'étais rapprochée alors du Professeur Samuel OUYA qui m'avait encouragé à faire un Master Recherche et acceptait de m'accueillir à cet effet dans le Laboratoire d'Informatique, Réseaux et Télécoms. Ce fut le début d'une belle aventure qui fut néanmoins très laborieuse. Après avoir validé mon Master Recherche en 2015, j'ai obtenu un an après, mon inscription en thèse, sous la direction Professeur Gervais MENDY. Cette grande personnalité au caractère très modeste et sympathique, n'a ménagé aucun effort, du haut de son grade, pour m'initier et m'accompagner durant ce long parcours. Sous votre Direction, trois années de ma thèse sont passées comme trois mois, car c'est allé très vite finalement. En plus de l'interminable stress dû à mon état de santé précaire, je vivais la peur et la pression de ne jamais arriver à bout de mes travaux. Mais, vous avez su me mettre en confiance. Vous aviez les mots qui m'ont donné d'y croire. Mon statut de mère de famille et d'enseignante à l'Université Catholique de l'Ouest ne vous a pas empêché de croire en l'engouement et en la soif de challenge de ma modeste personne. Seule, je ne s'y serais jamais arrivée.

Je voudrais tout d'abord remercier le Seigneur DIEU qui nous donne le souffle de vie et sans qui ce travail n'aurait jamais pu être réalisé.

A vous mon cher Directeur Pr. Gervais MENDY, je voudrais manifester toute ma reconnaissance, et ne saurai jamais trouver les mots adéquats pour vous dire un merci infini.

Je voudrais aussi remercier toutes les personnes qui de par leurs marques d'affection, leurs conseils, leurs encouragements, leurs soutiens, leurs accompagnements, leur disponibilité, ont contribué à l'aboutissement de cette thèse :

Pr. Claude LISHOU, Président du jury

Pr. Samuel OUYA, Examinateur

Pr. Ahmed Dooguy KORA, Examinateur

Pr. Ousmane THIARRE, Rapporteur

Pr. Tegawendé BYSSYANDE, PhD de l'Université du Luxembourg, Rapporteur

Les Chercheurs du département génie informatique de l'ESP pour l'esprit collaboratif,

Mes collègues doctorants du LIRT pour le partage d'expériences,

Mes Collègues de master de recherche des laboratoires LEA, LER (Babacar DIALLO, Prince Momar GUEYE, Boubacar DIALLO),

Dr Jean Marie SENE, Directeur Général de l'UCAO / Saint Michel,

Les Directeurs pédagogiques de l'UCAO, Particulièrement Mr Rémy BASS Pour son soutien et ses encouragements,

Tout le personnel enseignant et ou de recherche, tout le personnel administratif et de service de l'UCAO Saint Michel,

Dr Aliou NDIAYE, enseignant chercheur à l'UCAD, département de biologie végétale,

Dr Yao Gaspard Magnificat BOSSOU,

Pr Barthélémy YOMI pour sa généreuse contribution dans les traductions de mes travaux,

Adjudant Demba FALL, Commandant du corps urbain du Commissariat de Mbacké,

Moussa BOB, Yvan KALIA pour le partage d'expérience.

El hadji Oumar DIALLO et Destin DIBANTSA pour leur disponibilité.

Ma reconnaissance à la famille Coly, qui m'a accueillie et adoptée au Sénégal.

Toute ma gratitude à ma famille qui, depuis ma tendre enfance, m'a accompagnée et encouragée dans ce long cheminement. Mention Spéciale à Etienne Eric NEMI, Joseph Bilong mon frère aîné bien aimé qui m'a encouragé à faire l'informatique après mon Baccalauréat et a financé mon premier cycle, à mes filles Geneviève NGOP et Monique Gabrielle BILONG NEMI que j'aime de tout de mon cœur.

Dédicace

A

Mes parents Monique NGOP et Joseph BILONG, de regrettées mémoires

Table des matières

Liste des figures

Politique de sécurité et modèles de contrôle d'accès

Contribution au modèle de contrôle d'accès basé sur la délégation dynamique de rôles

Contribution à l'évaluation de la fonction de confiance dans les modèles de contrôle d'accès

Proposition d'un modèle de contrôle d'accès basé sur la protection de la Vie Privée et l'IoT

Implémentation des modèles proposés

Liste des tableaux

Liste des acronymes

ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
API REST	Application Programming Interface representational state transfer
ARBAC	Administrative Role Based Access Control
CA	Contrôle d'Accès
CPU	Central Process Unit
CRBAC	Contextual role based access control
CSV	Comma-separated values
DAC	Discretionnary Access Control
DORBAC	Delegation and organisation Based Access Control
DRBC	Délégation de Rôle Basé sur la Confiance
ENO	Espace Numérique Ouvert
FAD	Formation à Distance
FOAD	Formation Ouverte à Distance
FTP	File Transfert Protocol
GD	Grant Dependancy
GEORBAC	Geographical Role Base Access Control
GID	Grant Independancy
GNU	GNU is Not Unix
HRU	Harrison Ruzzo Ullman
HTML	HyperTexte Markup Langage
HTTPS	HyperText Transfer Protocol Secure
IdO	Internet des objets
Ilbc	Internet Low Bitrate Codec
IMS	IP multimedia subsystem
IoT	Internet of Thing
iSAC	Internet Speech Audio Codec
JEE	Java Enterprise Edition
JSON	JavaScript Object Notation
KMS	Kurento Media Server

LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MySQL	My Structured Query Language
NoSQL	not only SQL
OMS	Organisation Mondiale de la santé
ORBAC	Organization Based Access Control
OV	Organisation Virtuelle
PHP	PHP Hypertext Preprocessor
P-RBAC	Privacy Role Base Access Control
RBAC	Role Based Access control
RDBDAC	Role and delegation base dynamique Access Control
RTC	Real Time Communication
SAML	Security Assertion Markup Language
SDP	Session Description Protocol
SDSI	Simple Distributed Security Infrastructure
SIP	Session Initiation Protocol
SOBS	Sensitive Objects
SPKI	Simple Public Key Infrastructure
SVC	Support Vector Classifier
SVM	Support Vector Machine
SVR	Support Vector Regression
TBAC	Temporal Based Access Control
TCSEC	Trusted Computer System Evaluation Criteria
TDL	temporal description logic
TIC	Technologies de l'Information et de la communication
TLT	Treshold Level Trut
TRBAC	Temporal Role Based Access Control
TRUST-RBAC	Trust Role Based Access Control
RFID	Radio Frequency Identification
UCAD	Université Cheikh Anta Diop
UML	Unified Modelling Language
UNESCO	United Nations Educational, Scientific, and Cultural Organization
UVS	Université Virtuelle du Sénégal

W3C	World Wide Web Consortium
WEBRTC	Web Browsers With Real-Time Communications
WEKA	Waikato Environment for Knowledge Analysis
WIFI	Wireless Fidelity
WoT	Web of Thing
XML	L'Extensible Markup Language
UDP	User Datagram Protocol

Introduction générale

Les organisations virtuelles sont apparues suite aux développements qu'ont connus les technologies de l'information et de communication durant ces dernières années. Ces technologies devront non seulement changer notre façon de travailler, mais pourraient également jouer un rôle dans la gestion dans certains domaines clés tels que la santé, l'éducation et les finances. Le développement rapide des technologies de communication, des réseaux mobiles et des infrastructures intelligentes favorise la mise en place de systèmes de sécurité, afin de préserver l'intégrité et la confidentialité des données utilisateurs.

Plusieurs pays à travers le monde, en particulier ceux de l'Afrique, s'accordent selon le principe que leur développement passe nécessairement par des infrastructures et services en ligne [1]. Les nombreux travaux de recherche effectués actuellement et supportés par certains gouvernements africains, visent à faciliter l'accès aux soins de santé à distance ou à la formation en ligne dans les zones rurales et même urbaines. A cet effet, les travaux de virtualisations dans le domaine de l'éducation et de la santé connaissent un essor très remarquable.

Dans le domaine de l'éducation, le nombre croissant de nouveaux bacheliers a entraîné des effectifs pléthoriques dans les universités ces dernières années au Sénégal. En 2014, les étudiants inscrits dans l'enseignement supérieur sont estimés à 143097 apprenants dont 39521 nouveaux bacheliers. L'Université Cheikh Anta Diop (UCAD) a concentré 58,4%9 des étudiants. En 2016, le nombre d'étudiants inscrits dans l'enseignement supérieur est estimé à 151 989 apprenants contre 147 957 en 2015, soit une augmentation de 2,7%. Le taux de réussite au baccalauréat est passé de 44,99% en 2017 à 46,09% en 2018 [2].

Ces taux d'inscription en perpétuelle croissance dans les universités d'Etat justifient la politique du gouvernement du Sénégal à mettre sur pied l'Université Virtuelle du Sénégal (UVS). Cette dernière permettra de résoudre les problèmes de massification et donc de désengorger les amphis[1].

L'UVS s'organise autour d'un réseau d'espaces numériques ouverts (ENO) dans chacune des régions du Sénégal et au sein des universités publiques. L'ENO est un bâtiment équipé, connecté et ouvert. Il permet de disposer de relais physiques pour un bon déploiement de l'UVS

pour les enseignements présentiels et pour les travaux collaboratifs selon le site web de l'UVS [3].

Dans le domaine de la santé, l'accessibilité aux soins a impulsé la mise en place des infrastructures virtuelles conçues principalement autour de la e-santé ou santé électronique. L'objectif de la mise en place de ces infrastructures de plus en plus intelligentes vise à faciliter l'accès des patients aux soins médicaux, même dans les zones les plus reculées du pays. De plus, elles stockent des informations qui nécessitent d'être hors de portée de toute intention malveillante.

La virtualisation des systèmes liés à l'éducation et à la santé exige un cadre d'infrastructures des technologies de l'information et de la communication (TIC) telles que la téléphonie, l'internet et les objets connectés. Le Sénégal dispose actuellement d'un niveau de couverture téléphonique et d'internet satisfaisant. Le taux de pénétration des services Internet est de 57,59% en juin 2017 [4]. Le Sénégal compte 8 965 507 abonnés à l'internet dont 8 679 507 abonnés au puce 2G + 3G soit un taux de 96,81%, 161625 abonnés aux clés Internet pour un taux 1,80%, 106126 abonnés ADSL représentant le taux de 1,18% et 18418 abonnés à une connexion bas débit pour un taux de 0,21%.

Les taux de pénétration à l'internet évoqués ci-dessus justifient de la mise en place des organisations virtuelles liées à l'éducation et à la santé au Sénégal. A cet effet, la sensibilité de l'information qui pourrait être stockée dans les systèmes d'e-learning ou d'e-santé permet de déduire de la nécessité de prendre les questions de sécurité en compte.
Selon Pfleeger [5], la sécurité informatique se définit comme la protection des éléments valorisés appelés les actifs informatiques ou les actifs des systèmes d'information. Ces systèmes se complexifient et connaissent plusieurs formes de menaces pouvant les rendre vulnérables. La sécurité comprend les politiques, les procédures et les mesures techniques visant à prévenir tout accès non autorisé, toute altération de données, ainsi que les vols et les dommages.
Une menace pour un système d'informations représente l'ensemble de circonstances ayant le potentiel de causer des pertes d'information ou des dommages du système [5], tandis qu'une vulnérabilité est une faiblesse du système disposant de failles de sécurité et ouverte aux intentions malveillantes [6]. Ainsi, exploiter la vulnérabilité d'un système revient à l'attaquer. Les causes de la vulnérabilité des systèmes sont nombreuses. Nous pouvons citer entre autres le mauvais fonctionnement du matériel informatique (panne du matériel informatique,

configuration inadéquate, usage abusif ou acte criminel), le mauvais fonctionnement des logiciels (erreurs de programmation, installation ou configuration défectueuse, changements non autorisés), les désastres (pannes de courant, inondations, incendies et autres catastrophes naturelles), l'impartition (appeler des sous-traitants locaux ou à l'étranger) [7].

Une sécurité mal définie ou un contrôle inadéquat du système peuvent engendrer plusieurs types d'attaques, en l'occurrence les programmes malveillants, le cybervandalisme, le vol d'identité, l'hameçonnage (fishing), etc. Sécuriser un système d'information revient donc à intégrer des propriétés telles que l'authentification, la non-répudiation (l'information transférée entre l'envoyeur et le récepteur ne peut être remise en cause), l'intégrité et la confidentialité.

Selon Goncalves [8], trois techniques sont couramment utilisées pour garantir la sécurité du système d'information à savoir l'authentification basée sur l'identité de l'utilisateur, le contrôle d'accès qui détermine les permissions de chaque utilisateur authentifié, le traçage de l'accès au système d'information.

Au vu de la littérature, les modèles de contrôle d'accès basés sur les rôles proposés jusqu'ici présentent des limites dans l'appréciation et le choix d'un délégataire de privilèges lors d'un processus de délégation de rôle. Ce qui pourrait biaiser les propriétés portant sur la confidentialité et l'intégrité de l'information stockée dans le système. De plus, ces modèles sont moins malléables en sens qu'ils ne facilitent pas la mise à jour des droits d'accès.

Le travail de notre thèse portera spécifiquement sur l'étude et l'analyse des modèles de contrôles d'accès basés sur les rôles déjà existants. Les résultats de l'analyse nous permettront de proposer des modèles plus flexibles (malléables facilement) mettant en exergue le principe de délégation qualitatif et pouvant être adaptés aux organisations virtuelles complexes.

La délégation est un élément qui demeure important dans la gestion du contrôle d'accès. Bien que largement utilisée, la délégation est très peu prise en compte dans les politiques de sécurité en raison de sa complexité. Les modèles proposés jusqu'à présent sont des extensions du modèle RBAC (Role Based Access Control). La documentation concernant les contrôles d'accès basés sur les rôles ne révèle pas suffisamment d'études sur les exigences en matière de délégation.

La délégation d'un rôle peut s'avérer très nécessaire dans les situations où l'utilisateur autorisé à exécuter ce rôle est indisponible. Ce dernier peut alors solliciter un autre utilisateur qui agirait en son nom.

Au regard de l'expérience de l'université virtuelle du Sénégal, le suivi des enseignements peut être très contraignant et donc, le retard de l'exécution d'une tâche peut entrainer des limites sur le temps imparti. La violation des contraintes de temps peut alors impacter négativement sur la

productivité tant des enseignants que des apprenants. Cela peut entrainer des conséquences majeures à savoir le prolongement de l'année scolaire et les abandons des apprenants.
Par conséquent, la délégation demeure une approche très appropriée pour traiter les cas d'exceptions et garantir des scénarios alternatifs en rendant le travail plus fluide, plus flexible et plus efficace.
Pour éviter toute forme de délégation basée sur des critères arbitraires, il est impératif de tenir compte de la notion de confiance. La délégation des rôles en fonction du niveau de confiance reste encore peu fiable car, au regard de la littérature, l'évaluation de la confiance demeure partiale. A cet effet, les modèles de contrôle d'accès basés sur la délégation et la confiance restent un problème complexe quant à la fiabilité du bénéficiaire d'une délégation de rôle.
Le niveau de confiance du délégataire peut varier une fois que la délégation est effective. Une évaluation permanente du niveau de confiance du délégataire s'impose afin d'optimiser la délégation et minimiser les erreurs de confiance par la même occasion.

L'objectif de notre thèse est de proposer des modèles permettant aux organisations virtuelles de sécuriser les accès aux données utilisateurs et donc de protéger leur vie privée. Ces modèles devront améliorer le contrôle d'accès et permettre le travail collaboratif en toute confiance. En application au e-learning, nous évaluerons les critères de confiance à l'aide du modèle SVR (Support Vector Regression) afin de minimiser les erreurs de confiance lors d'une délégation de rôle.

La méthodologie adoptée pour résoudre notre problème comporte les phases conceptuelles, algorithmiques et expérimentales. Nous utilisons le langage UML (Unified Modeling Langage) pour l'analyse et la conception du système d'information. Pour prendre en compte les notions de contexte et d'exception, nous utilisons la logique non monotone T-JCLASSIC$\delta\varepsilon$ afin de faire une description axiomatique des modèles proposés dans cette thèse. Nous utiliserons les technologies WebRTC, Node.js et Kurento Media Server pour l'implémentation afin de faciliter la communication en temps réel entre les utilisateurs. Le Nano ordinateur nommé Raspberry pi, aidera à la collecte des informations biométriques reçues des capteurs.

Le manuscrit de notre thèse s'articulera autour de cinq chapitres. Le premier chapitre a pour objectif de définir la terminologie en rapport avec les politiques de sécurité et de contrôle d'accès ; puis de faire l'état de l'art des différents modèles de contrôle d'accès.

Le deuxième chapitre fait d'abord une description des différents types de délégations. Puis il propose un modèle de contrôle d'accès dynamique basé sur la délégation et la confiance (RDBDAC). Ce modèle améliore la gestion des autorisations dans les applications web Java dont le système de sécurité est statique (Java EE security Realm) et basé sur RBAC. Ainsi, l'administrateur de telles applications web n'aura plus besoin de manipuler le code source pour effectuer les mises à jour des politiques de contrôle d'accès.

Le troisième chapitre traite des questions de confiance et de délégation. L'objectif consiste à faire une classification (score) des critères de confiance afin de minimiser les erreurs confiance.

Le quatrième chapitre traite de la protection de la vie privée des sujets ainsi que des contraintes liées à la délégation en tenant en compte des autorisations octroyées à un délégataire.

Le cinquième chapitre est consacré à la description des outils et à l'implémentation. Tout d'abord, nous définirons la terminologie sur les organisations virtuelles liées au domaine de l'éducation et de la santé. Puis, nous implémenterons les modèles de contrôle d'accès proposés après avoir décrit et testé les outils utilisés dans nos travaux.

CHAPITRE 1

Sécurité des systèmes et modèles de contrôle d'accès

1 Politique de sécurité et modèles de contrôle d'accès

1.1 Introduction

Les modèles de contrôle d'accès ont connu une évolution remarquable au fur et à mesure que les systèmes d'information ont migré vers des environnements dynamiques. Un environnement est dynamique lorsque l'ensemble des positions occupées par les obstacles est susceptible de changer dans le temps [9]. Du fait de cette complexité (système variant), l'environnement dynamique exige la prise en compte de technologies évoluées, pour la mise en place de politiques de contrôle d'accès efficaces et fiables permettant de gérer la confidentialité et l'intégrité des données.

Le contrôle d'accès est l'ensemble des mesures mises en place pour restreindre l'accès aux ressources du système suivant des contraintes préétablies. Il existe de nombreux modèles de contrôle d'accès à savoir, les modèles de contrôle d'accès statiques et les modèles de contrôle d'accès dynamiques. L'objectif de ce chapitre est de comprendre les politiques de sécurité, les besoins en sécurité des systèmes, ainsi que la conception et les démarches suivies dans les modèles de contrôle d'accès. A cet effet, nous allons définir les concepts de base liés à la sécurité. Nous ferons ensuite l'étude des modèles de contrôle d'accès.

1.2 Sécurité des Systèmes d'information

La sécurité des systèmes d'information (SSI), représente l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher la modification ou le détournement du système d'information. Selon Sandhu [10], il devient primordial de protéger le système d'information contre toutes modifications abusives ou encore contre les accès non autorisés.

1.2.1 Terminologie sur le périmètre de sécurité des systèmes d'information

La sécurité dans les systèmes d'information repose sur un ensemble de concepts bien établis et clairement définis que sont la limite du système, le périmètre de sécurité, le système d'exploitation, le moniteur de référence etc. Chacun de ces concepts peut être défini comme suit :

→ Limite du système : désigne l'ensemble des ressources sur lesquelles l'administrateur exige un minimum de contrôle.

→ Périmètre de sécurité : il est constitué par le système d'exploitation et l'ensemble des serveurs vitaux pour la sécurité.

→ Système d'exploitation : c'est un logiciel destiné à faciliter l'utilisation d'un ordinateur [11]. Il est constitué d'un ensemble de programmes chargés de diriger l'utilisation des ressources d'un ordinateur par des logiciels applicatifs.

→ Moniteur de référence : c'est un médiateur incontournable dans toutes les relations entre sujets et objets dans un contrôle d'accès. Le moniteur de référence est responsable de l'autorisation de l'accès à un objet par un sujet. Un sujet peut être représenté par un système ou toute entité informatique pouvant représenter un utilisateur au sein du système. Un objet est une entité du système qui peut être représentée par un tuple, une table, un objet ou un fichier.

L'auteur Damsgaard [12] propose le système de sécurité sur la figure 1.1 ci-dessous.

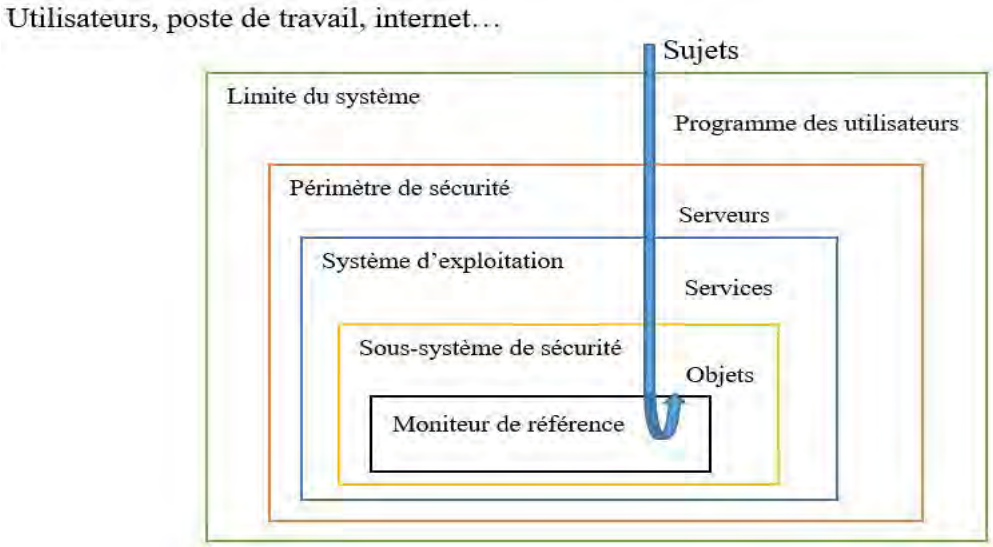

Figure 1.1 : Périmètres de sécurité

La figure 1.1 décrit l'accès aux objets par des sujets. Ces derniers doivent impérativement accéder aux différents périmètres du système pour accéder à la ressource. Le noyau d'un système est représenté par le moniteur de référence qui contrôle l'accès à toutes les ressources du système. Le système d'exploitation fournit un ensemble de primitives (vitales pour la sécurité du système) qui permet de réaliser des services. Le sous-ensemble de ces primitives s'appelle le sous-système de sécurité. Les primitives mises en œuvre par le système d'exploitation permettent de réaliser les serveurs qui gèrent les objets. Le système d'exploitation et l'ensemble des serveurs vitaux pour la sécurité constituent le périmètre de sécurité. La limite du système définit la frontière entre les entités manipulées directement par le système et le monde extérieur.

1.2.2 Politique de Sécurité dans les systèmes d'information

Selon Rihaczek [13], la politique de sécurité constitue l'ensemble des lois, des règles et des pratiques qui régissent la gestion, la protection et la distribution des informations sensibles ainsi que d'autres ressources dans un système donné. Il identifie les objectifs de sécurité du système et les menaces qui pèsent sur le système.

Le concept de politique de sécurité requiert la prise en compte de certains paramètres comme la confidentialité, l'intégrité, l'authentification, l'autorisation, la non-répudiation. Avec l'intégration des objets connectés aux systèmes, des paramètres supplémentaires tels que la confiance (Trust), la disponibilité et la protection de la vie privée (privacy) représentent un atout considérable pour l'amélioration des politiques de sécurité. Chacun de ces paramètres représente un objectif de sécurité.

1.2.2.1 Objectifs de la Sécurité

La sécurité repose sur un ensemble d'objectifs que sont la confidentialité, le confinement, le bon usage, l'authenticité, l'intégrité et la disponibilité. Dans cette section, nous allons définir chacun de ces objectifs.

→ La confidentialité garantit l'accessibilité de l'information uniquement aux utilisateurs autorisés. La garantie de la confidentialité des informations stockées dans un système informatique est généralement considérée comme la plus importante caractéristique d'un système fiable. Les utilisateurs du système ont besoin d'être rassurés que le système ne

divulgue pas leurs informations (secrets industriels, dossiers médicaux, secrets d'État) à des personnes non autorisées [14].

→ Le bon usage s'assure et garantit que les informations sont utilisées uniquement pour le but dans lequel elles sont données. Cette notion se rapproche du secret professionnel dans certains métiers sensibles (santé, justice, finance...), où l'information obtenue ne peut pas être divulguée à quelqu'un qui n'en a pas légitimement besoin.

→ L'authenticité garantit qu'un sujet (utilisateur, processus, système, etc.) est celui qu'il prétend être et que les informations reçues de lui sont identiques à celles fournies par le système. L'authenticité permet de garantir que les données livrées à un utilisateur sont celles qu'il a demandées [15], [16],[17].

→ L'intégrité évite la corruption ou la destruction des données traitées par le système. Nicomette [18], définit l'intégrité comme "la capacité du système informatique à empêcher la corruption des informations par des fautes accidentelles ou intentionnelles". Pour assurer l'intégrité de l'information, il faut que le système mis en place empêche les utilisateurs malveillants d'accéder aux données non autorisées (confidentialité et l'isolation des informations).

→ La disponibilité garantit que les données et les services du système sont disponibles aux utilisateurs autorisés. Il faut pour cela empêcher un utilisateur malveillant d'arrêter ou de bloquer un service ("Denial of Service attacks"). La disponibilité est une fonction qui rend le système disponible ainsi que les informations qui y sont stockées.

1.2.2.2 Catégories des politiques de sécurité

Les politiques de sécurité peuvent être définies par catégorie en fonction des propriétés qui leur sont assignées. Les trois types pouvant être assignés à une politique de sécurité sont consignés dans le tableau 1.1 ci-dessous.

Tableau 1.1 : catégories des politiques de sécurité

Type	Description	Exemples
Physique	restrictions d'accès physiques aux ressources	▪ barrières ▪ coffres ▪ clefs
Administrative	règles et procédures pour le renforcement de la sécurité	▪ enquêtes, audits ▪ responsabilisation ▪ bonnes pratiques
Logique	restrictions des accès logiques aux ressources informatisées mises en œuvre par des logiciels et matériels	▪ authentification ▪ identification ▪ cryptage ▪ cloisonnement ▪ organisation des droits

L'authentification et l'autorisation sont deux aspects primordiaux des politiques de sécurité logiques :

- **l'authentification** permet de se connecter et de prouver une identité. Le but de l'authentification est de vérifier l'identité de tous les utilisateurs qui souhaitent utiliser le système, de leur attribuer un identificateur système et de garantir la validité de cet identificateur.
- **l'autorisation** ou **contrôle d'accès**, assure la vérification de la légitimité des opérations demandées. L'autorisation vise à fixer les règles pour les relations entre sujets et objets dans le système et à garantir que ces règles sont respectées. Un *sujet* est une entité active (utilisateur, programme, système, etc.) et un *objet* est une entité passive (fichier, écran, ressource de calcul, etc.) qui peut être manipulée par des sujets autorisés.

Ayant présenté les différents types de politiques de sécurité, nos travaux porteront essentiellement sur les politiques de sécurité logique (portant sur la gestion des authentifications et des autorisations) tout au long de notre thèse. En plus de la politique de sécurité logique, il est nécessaire de définir des politiques contrôle d'accès pour la protection et la fiabilité des systèmes d'informations. Dans la section suivante, nous allons définir ce qu'est une politique de contrôle d'accès et expliquer ensuite comment la mettre en œuvre.

1.2.3 Définition et mise en œuvre d'une politique de contrôle d'accès

Les contrôles d'accès demeurent incontournables dans la gestion des structures ou organisations virtuelles précisément dans les secteurs de la santé, de la finance et de l'éducation [19], [20], [21]. Ces environnements intègrent divers appareils miniaturisés ainsi que la technologie de communication mobile. Cela permet de déployer les services n'importe où, n'importe quand et pour n'importe qui. Cette évolution impose de nouvelles exigences et de nouveaux défis en termes de sécurité à ces environnements dynamiques et sensibles au contexte [20]. Thion définit une politique de contrôle d'accès autour de deux propriétés fondamentales de la sécurité que sont la confidentialité et l'intégrité.

Contrôler les accès, c'est déterminer si un sujet peut effectuer une action demandée sur un objet. La définition des règles du contrôle d'accès a connu une évolution remarquable au regard de la littérature. La notation initiale était constituée du triplet (sujet, objet, ressource). Ces règles sont devenues de plus en plus complexes (sujet, objet, service, contexte) avec la richesse des données contextuelles et l'exploitation des techniques de traitement de données. L'intégration du paramètre « *contexte* » ainsi que celui de la « *confiance* » est sujette à différents challenges sur différents niveaux à savoir la modélisation, l'interprétation et le stockage. Une règle de contrôle d'accès est composée d'un ensemble de paramètres parmi lesquels on peut citer :

→ Sujet : peut être considéré comme un utilisateur, une machine, un processus, un programme, etc.

→ Objet : il peut être un fichier, une base de données, une machine, un programme, etc.

→ Action : représente les différentes manipulations qu'un sujet autorisé peut mener sur un objet.

→ Permission : désigne le droit d'action d'un sujet sur un objet (lire, écrire, modifier, etc.).

→ Contexte : est une contrainte qui lie le sujet, le droit d'accès et l'objet (contexte temporel, contexte spatial, etc.).

Les paramètres ci-dessus cités sont assignés à des ensembles de base pour définir une politique de contrôle d'accès. Parmi ces ensembles nous avons :

→ ***U* :** représente l'ensemble des utilisateurs connus du système. Les utilisateurs utilisent le système par l'intermédiaire d'un sujet.

→ ***S* :** c'est l'ensemble des sujets connus du système. Les sujets peuvent être des processus, des machines (toute entité informatique qui représente l'utilisateur au sein du système et se comporte selon sa volonté).

→ ***O* :** c'est l'ensemble des objets connus du système. Un objet est une entité du système comme un tuple, une table (cas des systèmes de gestion de bases de données), un objet ou un fichier (cas des systèmes de fichier).

→ ***A* :** représente l'ensemble des actions connues du système, que l'on peut effectuer sur les objets. Les actions correspondent par exemple aux opérations de sélection, de suppression, de modification et de création de tuples dans un système de gestion de bases de données.

Le contrôle d'accès renforce particulièrement la confidentialité, l'intégrité et la disponibilité de l'information. Le contrôle d'accès est généralement mis en œuvre par un moniteur de référence qui joue le rôle d'intermédiaire entre les utilisateurs et les ressources auxquelles ces derniers essaient d'accéder.

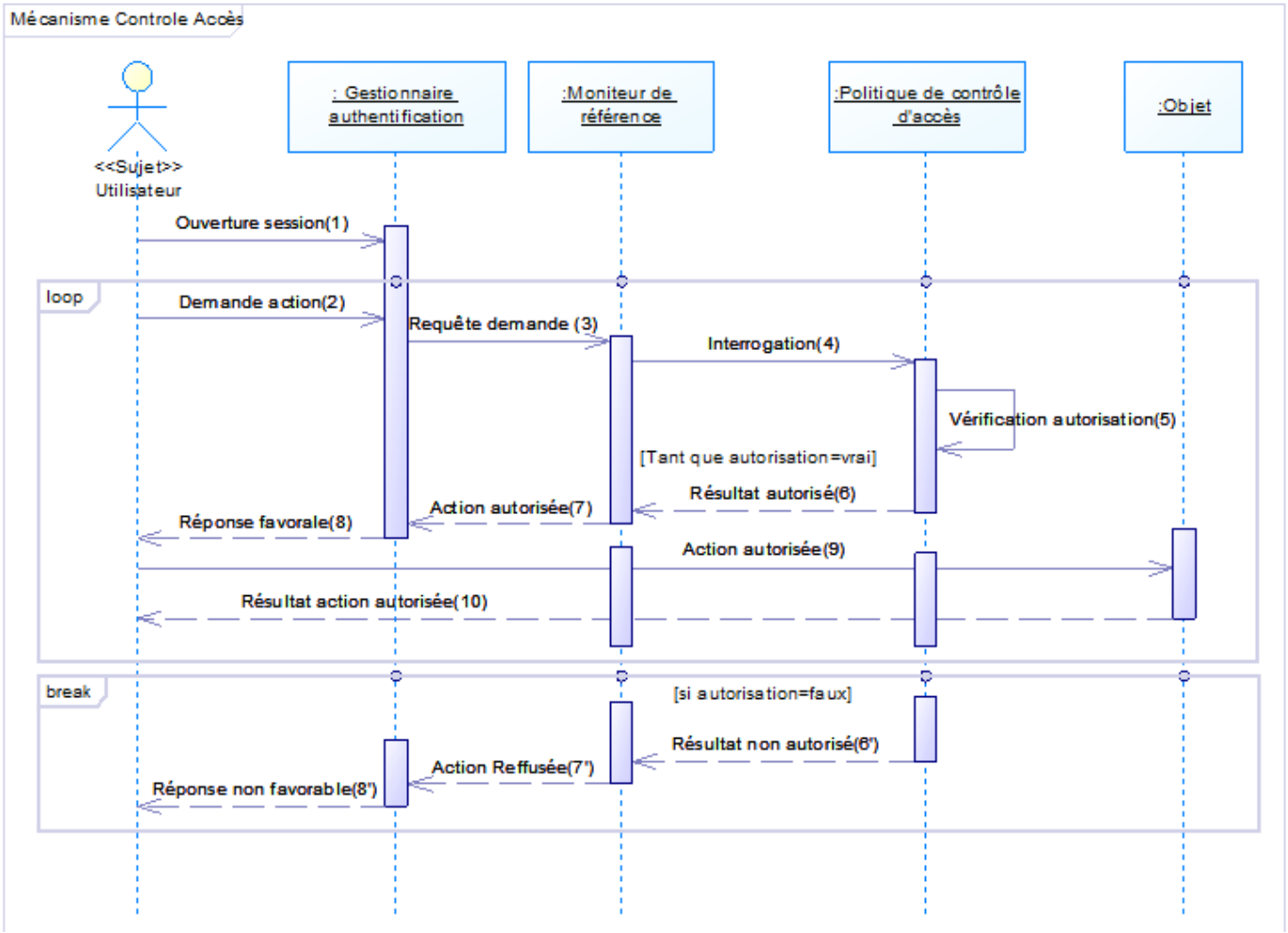

Figure 1.2 : mécanisme de mise en œuvre d'un contrôle d'accès

Le principe de fonctionnement et de mise en œuvre d'un contrôle d'accès tel qu'illustré par la figure 1.2 peut être décrit comme suit :

1. Authentification de l'utilisateur via le gestionnaire d'authentification
2. Envoi d'une demande d'action par l'utilisateur.
3. Requête transmise au moniteur de référence qui se charge de contrôler tout accès aux objets stockés dans le système. Le moniteur de référence interroge le système de gestion des politiques de contrôle d'accès.
4. Le système de gestion des politiques de contrôle d'accès vérifie que les actions demandées par l'utilisateur lui sont permises.
5. Retour de réponse de vérification d'autorisation. Tant que l'utilisateur est actif dans sa session et qu'il bénéficie de permission requise pour l'action demandée, il pourra alors agir sur l'objet et obtient le résultat escompté.
6. Si la vérification ne confirme pas de permission pour l'action demandée par l'utilisateur, le système rejette la requête de l'utilisateur.

Dans la section suivante, nous ferons une étude détaillée des modèles de contrôle d'accès. Le choix des modèles étudiés est lié à la problématique des contrôles d'accès basés sur la délégation et l'évaluation de la confiance.

1.3 Etat de l'art sur les modèles de contrôle d'accès

Contrôler les accès revient principalement à gérer les autorisations et l'intégrité de l'information. Dans le but de limiter des attaques contre les systèmes d'information, plusieurs auteurs ont proposé des modèles de contrôle d'accès. L'évolution de ces modèles de contrôle d'accès part des modèles de base ou modèles statiques aux modèles dérivés encore appelés modèles dynamiques. Les modèles dérivés sont des extensions des modèles de base, qui ont été proposés dans le but de corriger les limites des modèles dits statiques. Dans cette section, nous faisons une revue de la littérature des modèles de contrôle d'accès statiques et des modèles de contrôle d'accès dynamiques.

1.3.1 Modèles de contrôle d'accès statiques

Entête sur le contrôle d'accès statique

1.3.1.1 DAC (Discretionary Access Control)

Les premiers formalismes de contrôle d'accès ont été mis en place par Lampson [22], qui a défini les concepts de sujets, d'objets et d'actions.

Les politiques de contrôle d'accès discrétionnaire (DAC) sont basées sur les concepts de sujets, d'objets et d'actions mis en place lors de la définition des premiers formalismes de contrôle d'accès.

Les droits d'accès à chaque information sont manipulés par le propriétaire de l'objet. Le modèle de contrôle d'accès discrétionnaire est flexible car, un sujet avec des droits d'accès peut accorder des privilèges à tout autre utilisateur. En d'autres termes, le propriétaire de l'objet peut accorder des droits sur son objet à d'autres sujets [23].

L'octroi ou la révocation de privilèges est régularisé par une politique administrative décentralisée [6]. Le Trusted Computer System Evaluation Criteria (TCSEC) du département de la défense Américaine, donne la définition du DAC comme suit : *« le contrôle est discrétionnaire lorsqu'un sujet avec une certaine autorisation d'accès est capable de transmettre cette permission à n'importe quel autre sujet »*. Selon Thion [21], le modèle de contrôle d'accès discrétionnaire « Discretionary Access Control » (DAC) permet à un sujet d'attribuer des permissions à d'autres sujets. Ce modèle de contrôle d'accès est flexible, mais il peut générer des erreurs du fait que l'administration n'est pas centralisée. La gestion des accès aux fichiers du système d'exploitation UNIX constitue un exemple classique de mécanisme de contrôle d'accès basé sur une politique discrétionnaire.

Plusieurs modèles sont associés au DAC en l'occurrence, le modèle de Lampson, le modèle HRU(Harrison Ruzzo Ullman), le modèle Take-Grant et le modèle TAM [23].

Le modèle de contrôle d'accès discrétionnaire peut être représenté par la matrice de contrôle d'accès introduit par le modèle de Lampson. Cette matrice permet de représenter le triplet d'autorisation ACCESS entre sujets, actions et objets $ACCESS \subseteq S \times A \times O$.

Tableau 1.2 Matrice de contrôle d'accès

	Fichier 1	**Fichier 2**	**Fichier 3**	**Fichier 4**
Alice	rw	r	r	
Bob	r	rw	r	rwx
Demba	r	r	rw	rwx
Eric			r	r

Le tableau 1.2 est un exemple du jeu de matrice de contrôle d'accès, impliquant quatre sujets représentés par Alice, Bob, Demba et Eric ; quatre objets respectivement Fichier1, Fichier2, Fichier 3 et Fichier 4 et trois actions (r pour read, w pour write et x pour execute). Chaque sujet dispose des actions précises à mener sur l'objet. Dans ce cas de figure, ALICE a le droit de lecture/écriture sur le l'objet Fichier 1, droit de lecture essentiellement sur les objets Fichier 2 et Fichier 3, et aucune action possible sur l'objet Fichier 4.

L'adjectif discrétionnaire reste imprécis et peut être défini sous deux angles :

→ soit que les droits sont organisés selon une matrice de contrôle d'accès, dans laquelle on peut lire les permissions des utilisateurs en lignes ou en colonnes, mais sans préciser si c'est une autorité qui définit les droits ou s'ils sont définis par les utilisateurs. Pour cette interprétation, certains auteurs préfèrent traiter de contrôle d'accès basé sur l'identité (Identity-BAC) [24].

→ soit que les utilisateurs peuvent eux-mêmes définir les droits d'accès sur les ressources dont ils sont propriétaires. Pour cette interprétation, les sujets sont eux-mêmes propriétaires des objets et il existe une action supplémentaire propriétaire (owner) dans la matrice de contrôle d'accès [21].

Le modèle discrétionnaire a une faiblesse importante car, il repose sur une politique d'administration décentralisée. Il est difficile de contrôler le traitement fait de l'information une fois que celle-ci a été accédée par un utilisateur légitime. Le problème majeur de la transitivité de la lecture qui en découle peut être une source de diffusion de chevaux de Troie. Le modèle DAC est difficile à administrer dans les structures vastes. Lorsque les organisations comportent de nombreux sujets et objets, avec des changements fréquents des droits, il devient impossible

de dégager une vision globale de l'organisation des droits et de garantir la sécurité du système. La décentralisation engendre un problème de perte de confidentialité de l'information. C'est en réponse à ces problèmes que les modèles à niveaux sont apparus.

1.3.1.2 MAC

Le modèle MAC (Mandatory Access Control) a une politique de sécurité qui est définie et gérée par une autorité et ne peut être modifiée par les utilisateurs. Il permet le regroupement ou le marquage des ressources conformément à un modèle de sensibilité. L'affectation des privilèges d'une ressource aux utilisateurs dépend essentiellement du niveau d'habilitation et classification de ces derniers. Cela exclut les problèmes liés aux fuites d'information (à l'aide de chevaux de Troie) observées dans le modèle DAC. Ceci est principalement grâce au fait que les utilisateurs ne sont pas autorisés à interférer avec la politique de contrôle d'accès [6].

Contrairement aux politiques de contrôle d'accès discrétionnaire, les sujets d'une politique de contrôle d'accès obligatoire ne sont pas propriétaires des informations auxquelles ils ont accès. Le modèle d'autorisation obligatoire (MAC) centralise l'autorité d'administration. Par ailleurs, l'opération permettant la délégation des droits est contrôlée par les règles de la politique. Les sujets n'ont plus de pouvoir sur les informations qu'ils manipulent. Le sujet n'a accès à l'information que s'il y est autorisé par le système [20]. Il s'agit d'une restriction des politiques de sécurité où les sujets ne peuvent altérer l'accès aux objets. A cet effet, le problème de perte de confidentialité décrit dans le modèle discrétionnaire ne peut exister. Le modèle MAC a une politique de sécurité qui est définie et gérée par une autorité et ne peut être modifiée par les utilisateurs. Dans ce modèle, toutes les ressources informatiques sont la propriété exclusive de l'organisation.

Le modèle MAC a montré des limites liées à la complexité de son utilisation. Cela est dû à sa politique trop restreinte et donc difficile à déployer dans le cadre pratique. Les utilisateurs n'ont pas accès à tous les privilèges pour gérer leurs propres besoins de sécurité, notamment ceux concernant leur vie privée.

1.3.1.3 RBAC

Le modèle RBAC est considéré comme une approche alternative au contrôle d'accès obligatoire (MAC) et discrétionnaire (DAC). Sa politique de sécurité ne s'applique pas directement aux utilisateurs [19]. Il permet à un administrateur d'attribuer à un utilisateur un ou plusieurs rôles en fonction du travail qu'il effectue au sein de l'organisation. Le modèle RBAC est centré sur le rôle. Ce dernier représente de façon abstraite une fonction ou une profession au sein d'une organisation, qui associe l'autorité et la responsabilité confiées à une personne qui joue ce rôle (par exemple, professeur, directeur, ingénieur, technicien...). A Chaque rôle correspondent des permissions (ou privilèges), qui sont un ensemble de droits correspondant aux tâches qui peuvent être exécutées par ce rôle. Un rôle peut avoir plusieurs permissions et une permission peut être associée à plusieurs rôles. Tout comme un sujet peut avoir plusieurs rôles, un rôle peut être joué par plusieurs sujets [6].

Pour les auteurs Ray et Toahchoodee [25], le modèle de contrôle d'accès basé sur les rôles est utilisé pour répondre aux besoins de contrôle d'accès des organisations commerciales. Dans RBAC, les permissions sont attachées aux rôles et les utilisateurs doivent être assignés aux rôles pour obtenir les permissions. Les autorisations déterminent les opérations qui peuvent être effectuées sur les ressources sous contrôle d'accès. Un utilisateur doit établir une session pour activer un sous-ensemble de rôles auxquels il est affecté. Chaque utilisateur peut activer plusieurs sessions, mais chaque session est associée à un seul utilisateur. Les opérations qu'un utilisateur peut effectuer dans une session dépendent des rôles activés dans cette session et des autorisations associées à ces rôles. RBAC supporte également les hiérarchies de rôles.

La hiérarchie de rôles définit une relation d'héritage entre les rôles. Pour prévenir les conflits d'intérêts qui surgissent dans une organisation, le modèle RBAC permet de spécifier les contraintes de Séparation Statique et Dynamique des Tâches.

Selon Coma et al.[26], le rôle est une notion permettant de décrire facilement les fonctionnalités des organisations. Un rôle désigne une entité intermédiaire entre utilisateurs et privilèges. On associe à chaque rôle un ensemble de permissions. Tous les sujets ayant reçu l'autorisation de jouer un rôle héritent alors des permissions associées à ce rôle. Ainsi, les rôles peuvent être organisés de manière à former une hiérarchie [27], permettant de raffiner les différentes permissions attribuées à chaque rôle.

Lorsqu'un nouveau sujet est inséré dans le système d'information, il suffit d'affecter des rôles à ce sujet pour que ce dernier puisse accéder au système d'information conformément aux permissions accordées à cet ensemble de rôles [23].

Le modèle RBAC sous-entend que la définition des rôles, l'affectation des permissions aux rôles et la distribution des rôles aux utilisateurs sont effectuées par une autorité centrale [20].

En effet, dans une organisation telle qu'un hôpital, on peut souhaiter qu'un médecin n'ait accès qu'aux dossiers des patients dont il a le privilège d'accès. L'expression des aspects contextuels liés aux autorisations d'accès n'est pas appropriée au modèle RBAC. Il en résulte une multiplicité des rôles non justifiés voire sémantiquement incorrects

Plusieurs modèles à rôles ont été proposés, et constituent la famille RBAC composée de quatre modèles présentés sur la figure 1.3 [28] :

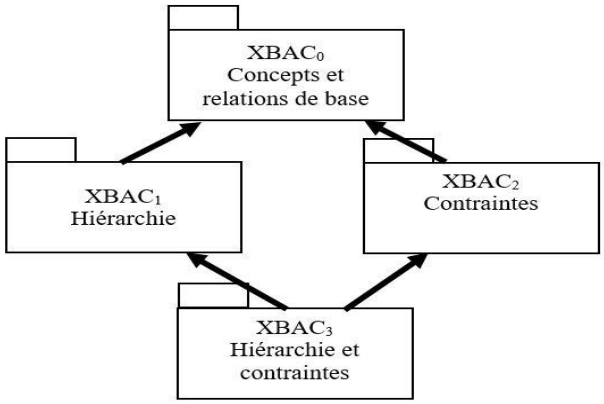

Figure 1.3 : représentation UML de la Famille X-BAC

→ Le modèle RBAC0, qui présente les concepts et relations de base – le noyau – du modèle

→ Le modèle RBAC1 reprend le modèle RBAC0 et introduit la notion de hiérarchie.

→ Le modèle RBAC2 reprend le modèle RBAC0 et introduit la notion de contrainte

→ Le modèle RBAC3 reprend les modèles RBAC1 et RBAC2 et prend en compte les interactions entre contraintes et hiérarchie.

Ces raffinements successifs illustrent une orientation générale des recherches sur les modèles de contrôle d'accès : à partir d'un noyau, introduisant les concepts et relations principales du modèle, des enrichissements supplémentaires sont proposés. Cette structuration de la famille des modèles RBAC a été reprise dans les modèles TBAC (Temporal Based Access Control) de Sandhu et al. [29] et GEORBAC de Bertino et al. [30]. C'est la raison pour laquelle le terme x-BAC a été utilisé, confère figure 1.3.

Le tableau 1.3 fait la synthèse des concepts et relations introduits dans le modèle de contrôle d'accès RBAC0. Ces concepts et relations sont à la base de la formalisation ensembliste de la famille des modèles RBAC [21].

Tableau. 1.3 : concepts et relations du noyau RBAC

	Notation	Description
Concepts	U	Ensemble fini d'utilisateurs
	R	Ensemble fini de rôles
	A	Ensemble fini d'actions
	O	Ensemble fini d'objets
	S	Ensemble fini de sujet (session)
Relation	$P \subseteq O \times A$	Permission est une action sur un objet
	$URA \subseteq U \times R$	Affectation plusieurs-à-plusieurs de rôles aux utilisateurs
	$PRA \subseteq R \times P$	Affectation plusieurs-à-plusieurs de permissions aux rôles
	$SU \subseteq S \times U$	Relation plusieurs-à-un entre sessions et utilisateurs
	$SR \subseteq S \times R$	Relation plusieurs-à-un entre sessions et rôles

RBAC atteint rapidement ses limites dès que les utilisateurs sont géographiquement dispersés, ou que l'entreprise est composée de services indépendants. De plus, les utilisateurs associés au même rôle possèdent forcément les mêmes privilèges. Ce qui réduit la flexibilité des politiques de sécurité ainsi modélisées.

1.3.2 Modèles de contrôles d'accès dynamiques

Un modèle de contrôle d'accès dynamique est un modèle qui doit prendre au moins un certain nombre de critères entre autres la sensibilité liée au contexte (temporel, géographique, géo-temporel ...), les faits par défauts et d'exceptions, avec possibilité d'activation et de désactivation de rôle.

Les modèles de contrôle d'accès dynamiques sont généralement des extensions du modèle RBAC. Ils sont classés en plusieurs catégories de modèles à savoir : les modèles de contrôle d'accès basés sur la sensibilité au contexte, la gestion de la confiance, la gestion de la vie privée, l'aspect sémantique ou les technologies d'intelligence artificielle. Dans cette section, nous nous

concentrerons sur l'étude de chacune des catégories des modèles de contrôle d'accès en rapport avec notre problématique.

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

Les modèles de contrôle d'accès basés sur la sensibilité au contexte présentent des extensions du modèle RBAC, dans lesquelles l'activation des rôles est dynamique. Le contexte est défini comme une information décrivant et caractérisant les situations des entités (personne, place, objet). Il peut être temporel, spatial ou environnemental. Les différentes évolutions du modèle RBAC sont décrites dans les huit extensions de modèles décrites ci-dessous.

1.3.2.1.1 Modèle ARBAC

Les concepts de rôles administratifs et de permissions administratives sont introduits dans ARBAC. Les permissions administratives sont les opérations qui permettent d'ajouter, modifier ou supprimer des concepts et relations « classiques » dans les politiques du modèle RBAC. Nous citons comme exemples l'affectation et la révocation de rôles aux utilisateurs, l'affectation et la révocation de permissions aux rôles ou encore l'affectation et la révocation de relations d'héritage entre rôles.
La hiérarchie est l'élément pivot sur lequel vont être opérées la majeure partie des opérations d'administration. Ainsi, disposer d'une bonne hiérarchie est indispensable pour tirer parti des modèles structurés [28].
La majeure partie des failles dans les mécanismes de contrôle d'accès sont dues à des erreurs humaines d'administration. Avec un nombre croissant d'utilisateurs, les politiques deviennent plus grandes, les cas particuliers plus nombreux et la gestion des droits plus complexes. Ceci est vérifié avec les enrichissements ou les extensions de modèles intégrés dans les modèles de contrôle d'accès.
Jayaraman et al. [31] ont illustré la conception d'une politique ARBAC en imposant la séparation des privilèges pour une banque comprenant 18 succursales. La contrainte de séparation des privilèges qu'ils ont utilisée est la preuve des préoccupations réalistes.

L'objectif du modèle de contrôle d'accès basé sur l'administration et les rôles est d'avoir une structuration homogène de l'ensemble des droits [32].

La figure 1.4 ci-dessous est une représentation UML du modèle ARBAC dans lequel, les concepts de rôles administratifs et de permissions administratives sont introduits.

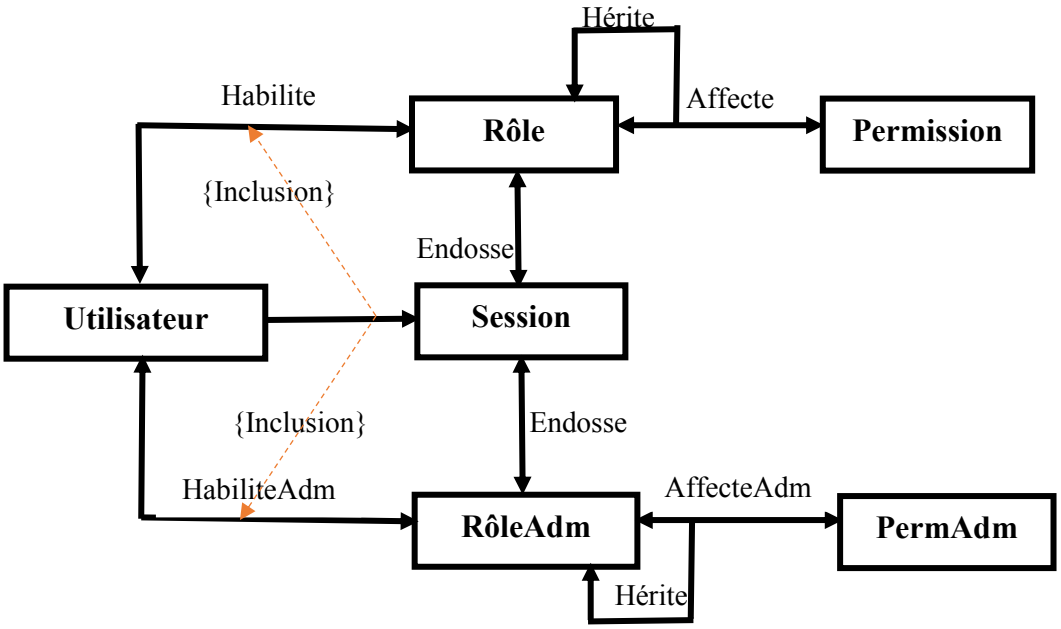

Figure 1.4 : Modélisation UML du modèle ARBAC

1.3.2.1.2 Modèle GeoRBAC

Les spécificités des applications basées sur la localisation ont été prises en compte par les auteurs Bertino et al. [30]. Leur proposition, axée sur la famille des modèles Geographical-RBAC (GEORBAC), étend les modèles RBAC en définissant de nouveaux concepts spatiaux pour représenter la position des sujets et celle des objets. Ces nouveaux concepts sont utilisés pour limiter géographiquement l'utilisation des rôles. L'interaction entre aspects géographiques, contraintes et hiérarchie a conduit Bertino et ses co-auteurs à structurer leur famille de modèles comme celle de RBAC (figure 1.3). Le principe proposé dans le modèle GEORBAC est de comparer une position physique, supposée obtenue de façon fiable (par exemple via la localisation GPS), à des positions logiques (exemple : route, ville, région) auxquelles sont associés des rôles géographiques. Ce principe a été appliqué à d'autres modèles de contrôle d'accès que RBAC.

1.3.2.1.3 Modèle TRBAC

Le modèle TRBAC (Temporal Role Based Access Control) est obtenu en introduisant le facteur temps dans le modèle de contrôle d'accès basé sur les rôles. L'activation et la désactivation des

rôles est temporelle. À cet effet, un rôle peut être actif pendant une certaine période et ne pas l'être sur une autre, grâce au rôle déclencheur. Ce modèle est très adapté aux applications à fortes contraintes temporelles, telles que les systèmes intégrant des workflows dans lesquels la notion de temps est importante. Le modèle TRBAC est recommandé pour les organisations qui souhaitent spécifier des règles d'autorisation valides pour un intervalle de temps donné [33].

Les travaux de Bertino et al. [34], ajoutent la dimension temporelle au modèle RBAC. Les auteurs de cette contribution introduisent le concept d'activation et de désactivation des rôles. Les contraintes temporelles déterminent quand les rôles peuvent être activés ou désactivés. Un rôle ne peut être désactivé que s'il a été activé [25].

1.3.2.1.4 Modèle Spatio-Temporel RBAC

Les progrès croissants des technologies de l'informatique omniprésente mènent vers une ère où l'information spatio-temporelle devient nécessaire au contrôle d'accès. Les auteurs proposent un modèle de contrôle d'accès spatio-temporel, basé sur le modèle RBAC (Role-Based Access Control), qui convient aux applications informatiques omniprésentes. Cette contribution montre l'association de chaque composante du RBAC avec l'information spatio-temporelle et formalise le modèle en énumérant les contraintes. Ce modèle peut être utilisé pour des applications où l'information spatiale et temporelle d'un sujet et d'un objet doit être prise en compte avant d'accorder ou de refuser l'accès. Les auteurs définissent deux types d'emplacements géographiques : physique et logique. Tous les utilisateurs et objets sont associés à des lieux qui correspondent au monde physique. C'est ce qu'on appelle les emplacements physiques. Un emplacement physique est formellement défini par un ensemble de points dans un espace géométrique tridimensionnel. Un emplacement logique est une notion abstraite pour un ou plusieurs emplacements physiques [25].

Toahchoodee et al. [25] distinguent deux types d'informations temporelles dans leur modèle : le premier est connu sous le nom d'instant et l'autre est l'intervalle de temps. Le temps peut être représenté par un ensemble de points discrets sur la ligne de temps. Un instant est un point discret sur la ligne du temps. La granularité exacte d'un instant dépend de l'application. Dans une certaine application, un instant dans le temps peut être mesuré en nanoseconde et dans une autre, il peut être spécifié en milliseconde. Un intervalle de temps est un ensemble d'instances de temps. Quand les instances de l'heure constituant un intervalle sont consécutives, on parle d'intervalle continu ; sinon, l'intervalle est dit non continu. Ils ont défini plusieurs prédicats dans leur modèle :

- Le prédicat UserRoleAssign (u, r, d, l) indique que l'utilisateur u est affecté au rôle r pendant l'intervalle de temps d et l'emplacement l. Pour que ce prédicat se maintienne, l'emplacement de l'utilisateur lorsque le rôle a été affecté doit être dans un des emplacements où l'attribution des rôles peut avoir lieu. En outre, le moment de l'affectation des rôles doit se situer dans l'intervalle lorsque le rôle peut avoir lieu. Le prédicat a été défini comme suit :

  $$\text{UserRoleAssign}(u, r, d, l) \Rightarrow (\text{UserLocation}(u,d) = l) \wedge (l \subseteq \text{RoleAllocLoc}(r)) \wedge (d \subseteq \text{RoleAllocDur}(r)) \quad \textbf{(1.1)}$$

- Le prédicat UserRoleActivate(u, r,d, l) est vrai si l'utilisateur u a activé le rôle r pour la fonction intervalle d à l'emplacement l. Ce prédicat implique que l'emplacement de l'utilisateur au cours de l'opération doit être un sous-ensemble des emplacements autorisés pour le rôle activé et toutes les instances de temps où le rôle reste activé doivent appartenir à la durée pendant laquelle le rôle peut être activé et le rôle ne peut être activé que s'il est affecté.

  $$\text{UserRoleActivate}(u, r,d, l) \Rightarrow (l \subseteq \text{RoleEnableLoc}(r)) \wedge (d \subseteq \text{RoleEnableDur}(r)) \wedge \text{UserRoleAssign}(u, r,d, l) \quad \textbf{(1.2)}$$

1.3.2.1.5 Modèle CRBAC

Park et al. [35] ont été motivés par l'inclusion du concept contexte dans le modèle CRBAC (Contextual role based access control). Ce dernier a été proposé pour faire face aux exigences des applications des systèmes omniprésents, avec la prise en compte de la location ou emplacement de l'utilisateur, son état et horaire d'utilisation. Selon [20], la prise en compte du contexte dans les politiques à base de rôles est un domaine de recherche très actif de nos jours. Le modèle CRBAC est composé des éléments suivants :

→ Utilisateurs, Rôles, Sessions, Permissions, Operations et Objets. Ces éléments représentent les mêmes notions que dans le modèle RBAC.

→ Règle contextuelle (CR) : représente un ensemble de règles contextuelles. La règle contextuelle est utilisée pour récupérer des informations de contexte de sécurité pertinentes sur l'environnement. Cette récupération est faite dans le but d'une utilisation pour les politiques de contrôle d'accès. La règle contextuelle peut être liée au temps, à la localisation, etc.

→ Contexte (C) : sert à regrouper les informations contextuelles du système. L'ensemble « C » capture toutes les informations de contexte qui sont utilisées pour définir la règle contextuelle «CR – context rule». Les informations peuvent être le temps, la localisation, la température etc.

1.3.2.1.6 Modèle organisationnel OrBAC

Dans toute organisation, l'administrateur est responsable de gérer l'accès de chaque utilisateur à une ressource, en appliquant les règles de sécurité. Mais la gestion des droits d'accès devient complexe à mesure que le nombre d'utilisateurs, de ressources et d'activités augmente. Le modèle OrBAC résout ce problème en créant des entités abstraites (rôle, vue, activité) séparées en des entités concrètes (sujet, objet, action). L'objectif de cette séparation est d'appliquer les règles de sécurité aux entités abstraites, et à chacune de ces entités, une entité concrète est associée.

OrBAC définit quatre types de règles de sécurité : Permission, obligation, interdiction et recommandation M. Ghorbel-Talbi et al [36]. Le principe du modèle OrBAC est résumé à la figure 1.5 ci-dessous et met en relation ses différentes composantes.

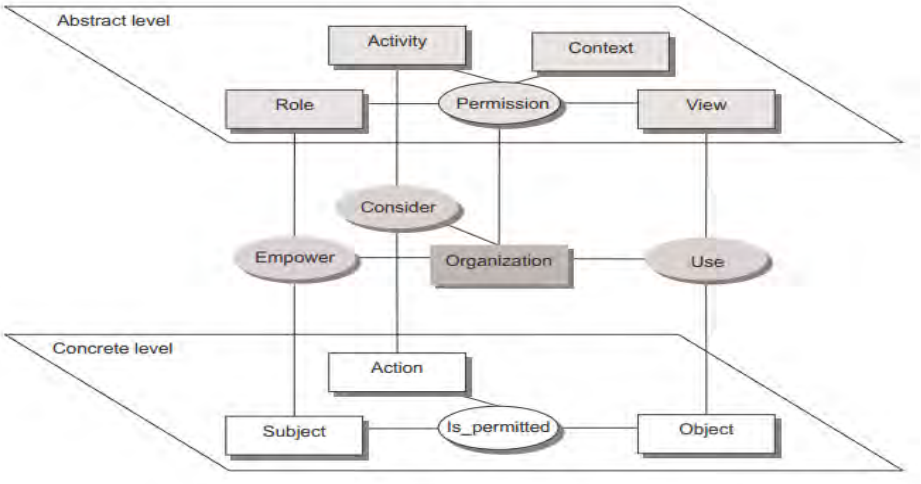

Figure 1.5 : modèle OrBAC

Un sujet est associé à un rôle en fonction du rôle qu'il joue dans une certaine organisation et obtient les permissions associées à ce rôle. Dans le modèle OrBAC, la structuration va au-delà des sujets et touche également les actions et les objets. Ainsi, l'entité activité est une abstraction

d'un ensemble d'actions l'implémentant et l'entité vue est une abstraction des objets ayant des propriétés de sécurité communes avec une seule règle dans OrBAC.

On peut exprimer que si un patient est opéré par une équipe médicale, tous les membres de cette équipe peuvent avoir accès au dossier du patient en question. L'organisation est au cœur du modèle OrBAC. Ainsi, l'équipe médicale opérant le patient est associée à une entité hospitalière particulière, une organisation, à laquelle on aura attribué un ensemble de privilèges qui peut différer de celui qu'aurait eu la même équipe dans un autre centre de soins. Grâce à ce formalisme, on peut ainsi mieux faire coopérer entre elles des organisations et des sous-organisations ayant des politiques de sécurité différentes. On voit apparaître sur la figure 1.5**,** le contexte comme entité [37]. Celui-ci est défini pour une organisation, un sujet, une action et un objet donnés. Les contextes permettent d'exprimer des permissions ou des interdictions dans certaines circonstances (urgence à l'hôpital...). Les contextes peuvent être temporels, spatiaux, liés à un historique, à l'usage fait par son utilisateur ou à l'environnement de l'utilisateur. OrBAC permet d'exprimer aussi bien les autorisations, que les interdictions ainsi que les obligations et les recommandations.

OrBAC permet de définir dans quel cadre peut s'effectuer cette délégation (contexte exprimant la personne à qui on peut déléguer,...). Le modèle OrBAC est simple à gérer grâce à l'abstraction, au contexte, à l'héritage et à la délégation [26].

Le contrôle d'accès basé sur l'organisation (OrBAC - Organization Based Access Control) est un modèle qui permet de spécifier des politiques de sécurité contextuelles relatives aux permissions, interdictions, obligations et recommandations [23], [38]. C'est un modèle qui permet d'exprimer une politique de sécurité au niveau organisationnel, c'est-à-dire indépendamment de l'implantation qui sera ensuite faite de cette politique. Il est ainsi possible d'exprimer l'ensemble des exigences de sécurité du système d'information et ensuite de distribuer ces exigences sur les différents composants de sécurité, vu comme un ensemble de sous-organisations de l'organisation que constitue le système d'information. Cette distribution porte également sur les responsabilités d'administration que l'on peut confier à des sujets affectés à des rôles différents.

Le modèle OrBAC utilise la notion de hiérarchie de rôle c'est-à-dire un mécanisme d'héritage de permission à travers la hiérarchie de rôle. Ceci peut être applicable dans le cas d'une organisation ayant des sous organisations ; les organisations se succèdent de père en fils. Dans le cas des organisations évoluant indépendamment et se situant au même niveau de hiérarchie, on ne peut pas appliquer cette notion de hiérarchie de rôle d'OrBAC, mais plutôt chercher un autre moyen pour faire une extension. OrBAC fournit un cadre pour exprimer les politiques de

sécurité d'organisations, cependant il ne répond pas aux besoins de distribution, de collaboration et d'interopérabilité entre organisations. La technologie des services Web est un exemple pour fournir quelques mécanismes en particulier pour la collaboration [39].

1.3.2.1.7 Modèle multi-OrBAC

Le modèle Multi-OrBAC est défini comme une extension du modèle OrBAC pour les systèmes multi organisationnels complexes, hétérogènes, interopérables et distribués [23]. C'est un modèle de sécurité dynamique et adaptable, permettant d'une part de spécifier des politiques de sécurité différente dans chaque organisation, et d'autre part d'imposer des règles pour les interactions entre organisations. Ainsi, pour décrire les primitives OrBAC dans la multi organisation, l'utilisation du modèle Multi-OrBAC permet de faire une extension. Cette extension est la modification des concepts de rôles, vues, et activités. Le modèle Multi-OrBAC a introduit une nouvelle notion rôle dans l'organisation qui est simplement une extension de rôle dans OrBAC. Il en est de même pour les vues et activités qui sont des extensions respectivement des vues et activités dans le modèle OrBAC.

1.3.2.1.8 Modèle Poly-OrBAC

Ce modèle est également basé sur OrBAC et sur les interactions par services web. PolyOrBAC est une plateforme de contrôle d'accès collaboratif basée sur OrBAC et la technologie web services [39]. Cette plateforme est applicable dans le contexte d'une infrastructure critique en général et plus particulièrement dans le cadre d'un réseau électrique.

1.3.2.2 Modèles de contrôle d'accès basés sur la confiance

Grâce aux données contextuelles, la gestion de la confiance a eu de nouvelles opportunités lors de la conception de nouveaux modèles de confiance. Ces modèles servent à évaluer le niveau de confiance d'une personne anonyme ou d'une personne dont on n'est sûr de rien. Dans la littérature, la gestion de la confiance a fait l'objet de plusieurs travaux. Cette multiplicité de contributions est à l'origine de différentes définitions de la confiance. Pour J. Goepel, «*La confiance est la probabilité subjective par laquelle un individu (A) attend qu'une autre personne (B) effectue une action donnée sur laquelle son bien-être dépend »* [40].

La confiance (ou, symétriquement, la méfiance) est un niveau particulier de la probabilité subjective avec laquelle un agent évalue qu'un autre agent ou groupe d'agents accomplira une action particulière à la fois, avant de pouvoir surveiller cette action (ou indépendamment de sa capacité à la surveiller) et dans un contexte où elle affecte sa propre action [41]. Selon ce dernier, lorsque nous disons que nous faisons confiance à quelqu'un ou que quelqu'un est digne de confiance, nous voulons implicitement dire que la probabilité qu'il accomplisse une action bénéfique ou du moins pas préjudiciable pour nous est suffisamment élevée pour que nous envisagions d'engager une certaine forme de coopération avec lui.

Grandison et ses collaborateurs [42] définissent la confiance comme la ferme conviction de la compétence d'une entité à agir de façon sécurisée et sure dans un contexte précis (en supposant que la sureté couvre la fiabilité et l'actualité). Pour ces derniers auteurs, la méfiance (manque de confiance) est le manque de conviction de la compétence d'une entité à agir de façon sécurisée et sure dans un contexte spécifié. La gestion de la confiance est répartie en trois catégories : confiance en service, confiance en information et confiance en utilisateurs.

→ La confiance en service : est évaluée et validée par le moyen de la qualité de service.

→ La confiance en informations : Cette mesure est assurée par le moyen des services de sécurité : l'intégrité et la confidentialité des informations.

→ La confiance en utilisateurs : le niveau de confiance est évalué sur la base des paramètres tels que l'identité, le comportement et l'historique de l'utilisateur.

1.3.2.2.1 Modèle Trust-BAC

Le modèle Trust-BAC est basé sur l'évaluation de la fiabilité des utilisateurs. La valeur de cette évaluation est déduite dynamiquement en fonction du changement observé dans le comportement de l'utilisateur. Le modèle tient compte de trois (3) principales entités que sont les utilisateurs, les rôles et les permissions.

- Utilisateurs : ils sont affectés à des rôles après évaluation de leur niveau de confiance.
- Rôles : ils sont associés au niveau de confiance requis pour leur affectation.
- Permissions : sont associées au niveau de confiance, nécessaire pour son assignation à un utilisateur [20].

Le modèle Trust-BAC définit le niveau de confiance comme un ensemble de nombres réels compris entre -1 et +1. L'ensemble TL (TRUST LEVELS) ou NDC (Niveau de confiance) est l'ensemble des sous-ensembles possibles S de l'intervalle [-1, 1].

NDC = {S | S [-1, 1]. Le niveau de confiance devient ainsi un ensemble infini où chaque membre S peut être discret ou continu Chakraborty et al. [43].

1.3.2.2.2 Modèle Trust-RBAC

M. Toahchoodee et al. [44] proposent le modèle Trust-RBAC qui est basé sur l'évaluation du niveau confiance (trustworthiness) des utilisateurs. Cette valeur est déduite d'une façon dynamique suivant le changement identifié dans le comportement de l'utilisateur. Ils schématisent le modèle Trust-RBAC dans la figure 7 ci-dessous :

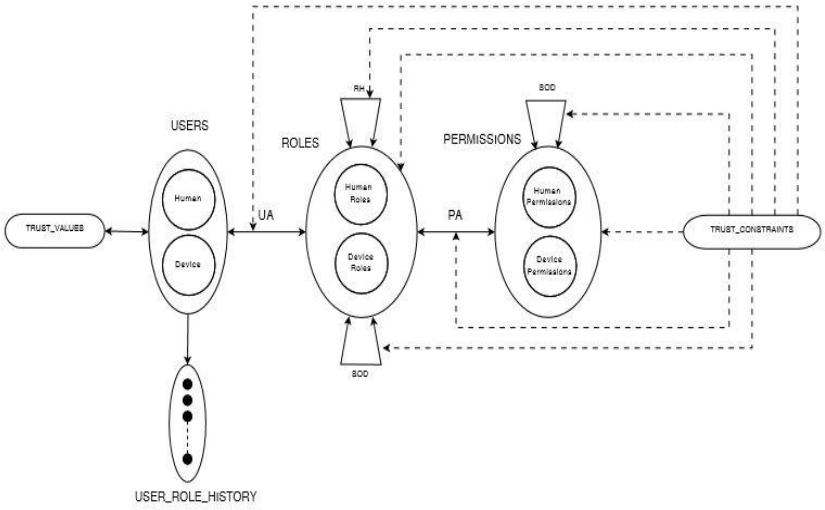

Figure 1.6 : Modèle Trust-RBAC

Les entités principales du modèle sont :

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

Les auteurs adaptent le modèle de confiance proposé par Chakraborty et al. dans [45]. Initialement, une entité A ne fait pas entièrement confiance à une nouvelle entité B. L'entité A, doit évaluer une relation de confiance avec l'entité B dans un contexte précis. Dans le modèle Trust-RBAC, le contexte est représenté par le rôle auquel un utilisateur est assigné. Le contexte est donc appelé contexte du rôle rc. Les utilisateurs peuvent être associés à plusieurs rôles. Pour déterminer l'autorisation entre un utilisateur et un rôle, la valeur de confiance d'un utilisateur est évaluée en fonction de chaque contexte de rôle séparément. La relation de

confiance entre l'utilisateur humain ou l'utilisateur du dispositif et le système dans le contexte du rôle rc dépend de trois facteurs que sont propriétés, expérience et recommandations.
La sémantique de ces trois facteurs est différente pour l'homme et l'utilisateur de l'appareil. Nous représentons formellement une relation de confiance entre truster, A, et trustee, B, sur un certain rôle contexte rc, comme un triple ($_{A}b^{rc}B$, $_{A}d^{rc}B$, $_{A}u^{rc}B$), où $_{A}b^{rc}B$ resprésente La croyance de A sur B au sujet de la fiabilité de ce dernier, $_{A}d^{rc}B$ est l'incroyance de A sur B, et $_{A}u^{rc}B$ est l'incertitude de A sur B. Chaque composante a une valeur comprise entre [0, 1] et la somme de ces composantes est 1.

1.3.2.2.3 Délégation de rôle basée sur la confiance (DRBC)

De nombreux chercheurs de la communauté scientifique se sont intéressés aux questions liées à la confiance et à la délégation. Toutefois, la question de la confiance dans la gestion des délégations doit faire l'objet d'une réflexion plus approfondie. Selon Barka et Sandhu dans [46], l'idée de base de la délégation est d'avoir des entités actives qui délèguent leur pouvoir à d'autres entités actives dans un système.

Cependant, les modèles mettant l'accent sur les relations de confiance et les délégations se sont multipliés timidement. Li, M., Sun, X., et al [47] proposent un modèle de délégation à plusieurs niveaux avec gestion de la confiance dans les systèmes de contrôle d'accès. Ils organisent les tâches de délégation en trois niveaux, faible, moyen et élevé, en fonction de la sensibilité des informations contenues dans les tâches de délégation. Dans ce modèle, plus la tâche déléguée est délicate, plus le délégué doit être digne de confiance. Les auteurs ont élaboré des méthodes d'évaluation de la confiance pour décrire l'historique de confiance d'un délégué et faire des prévisions.

Les auteurs Bilong et al [48], ont proposé un modèle hybride avec plusieurs paramètres tels que la délégation, le niveau de confiance et le contexte temporel. Sur ce modèle, la confiance prend essentiellement deux valeurs possibles, "0" ou "1". Il gère les exceptions en définissant le temps nécessaire à l'exécution du rôle délégué.

Malgré de nombreux efforts fournis par les chercheurs sur la question de délégation basée sur la confiance, des défis restent à être menés quant à l'évaluation réelle de la confiance. Ce problème reste une des questions essentielles que nous allons essayer de résoudre dans les prochains chapitres de notre travail.

1.3.2.3 Modèles de contrôle d'accès basé sur la préservation de la vie privée

Clifton [49] présente une discussion complète sur la façon de définir la protection de la vie privée dans le cadre de l'exploration de données. Selon lui, la protection de la vie privée correspond à la protection des données personnelles et celle de la vie privée de l'entreprise. L'atteinte de la vie privée correspond à la divulgation d'informations sur une collecte de données ou sur un élément de données individuelles. L'objectif du modèle PRBAC réfère à la vie privée de l'individu. Dans ce modèle, le type de stratégie est basé sur les rôles étant donné que les utilisateurs sont affectés à des rôles et que les rôles ont certaines autorisations pour les objets. Le modèle PRBAC est conçu pour résoudre le problème de recherche de schémas qui ne sont pas censés être découverts par l'ajout d'objets sensibles SOBS.

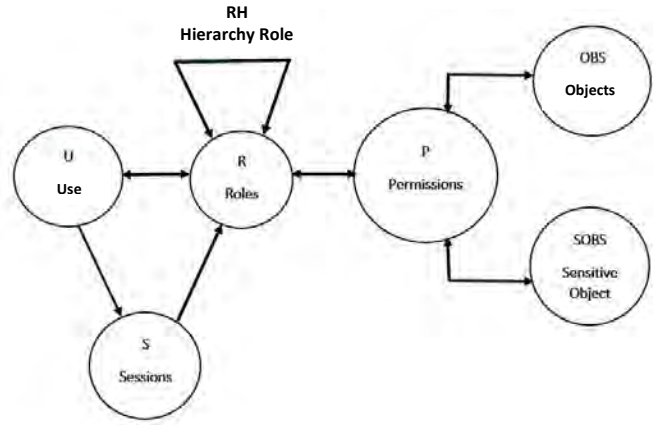

Figure 1.7 : modèle PRBAC

Le modèle PRBAC est défini par un ensemble d'entités définis comme suit :

→ Utilisateur **U :** Un utilisateur dans ce modèle est un être humain, des agents autonomes intelligents tels que des robots, des ordinateurs immobiles, ou même des réseaux d'ordinateurs. Par souci de simplicité, le modèle considère l'utilisateur en tant qu'être humain.

→ Rôle **R** et hiérarchie des rôles **RH :** un rôle est une fonction ou un titre de poste au sein de l'organisation avec une certaine sémantique associée concernant l'autorité et les responsabilités conférées à un membre du rôle (par exemple, chef de service). La hiérarchie des rôles (SR) est une façon naturelle d'organiser les rôles de manière à refléter les lignes hiérarchiques et les responsabilités de l'organisation.

→ Permission **P :** c'est l'approbation d'un mode particulier d'accès à un ou plusieurs objets dans le système. Un utilisateur établit une session au cours de laquelle il active un sous-ensemble de rôles dont il est membre.

→ Object **OBS :** est une entité qui contient ou reçoit des informations, ou qui dispose de ressources système épuisables documents texte, fichiers audio et vidéo, fichiers PowerPoint etc.).

→ Objets sensibles **SOBS :** ils sont prédéterminés par l'administrateur de la base de données ou l'administrateur système.

Une attribution de l'autorisation dans P-RBAC est une cession de l'autorisation de données de la vie privée à un rôle. Les contraintes et les obligations conditionnelles dans ce modèle permettent une définition de politique de confidentialité plus concise. P-RBAC nécessite de spécifier explicitement toutes les conditions lorsque les données sensibles de la vie privée peuvent être accessibles Dafa-alla et al.[49].

1.4 Synthèse sur l'étude des modèles de contrôles d'accès

Le tableau 1.2., résume les avantages et les limites de plusieurs modèles de contrôle d'accès. Nous y avons décrit deux catégories de modèles à savoir les modèles de contrôle d'accès statiques ou basiques et les modèles de contrôle d'accès dynamiques ou dérivés. Les modèles de contrôle d'accès basiques composés de DAC, MAC et RBAC ont abouti à plusieurs contributions, du fait de leurs limites respectives. Le modèle RBAC est le plus évolué des modèles basiques. Son aspect statique caractérisé par l'absence de prise en compte des cas d'exception et du contexte lors de l'assignation d'un rôle, constitue l'une de ses plus grandes faiblesses. De plus, la hiérarchisation des rôles devient difficile à gérer lorsque les sujets actifs du système sont dispersés géographiquement. Cela a amené les chercheurs à proposer des modèles dérivés tels ARBAC, GeoRBAC, TRBAC, Spatio-temporel RBAC, CRBAC, OrBAC, Multi-OrBAC, Poly-OrBAC, afin d'améliorer et par la même occasion corriger les limites observées dans le modèles RBAC. Ces modèles dérivés communément appelés des « extensions de RBAC » ont corrigé son côté statique et ont pris en compte le contexte au sens large du terme, afin de gérer les limites géographiques, temporelles et organisationnelles du modèle RBAC. Les modèles dérivés font partie des modèles de contrôle d'accès dynamiques basés sur la sensibilité au contexte. Le tableau présente aussi une étude d'autres types de

modèles de contrôle d'accès dynamiques basés sur la confiance et d'autres basés sur la préservation de la vie privée. Bien que l'ensemble des modèles présentés dans le tableau ci-dessus contribuent à améliorer les limites des modèles basiques, ils présentent des limites notamment dans l'administration dynamique des rôles en ce qui concerne le modèle RBAC, l'appréciation des critères de confiance en ce qui concerne les modèles de contrôle d'accès basés sur la délégation de rôle et la confiance.

Tableau 1.4: synthèse de l'état de l'art des modèles de contrôle d'accès

	Modèles	Avantages	Limites
Modèles de contrôle d'accès de basiques	DAC	• Administration décentralisée	• Intégrité de l'information non garantie
	MAC	• Administration centralisée • Les sujets ne sont pas propriétaires de l'objet.	• Intégrité de l'information assurée • Rigide
	RBAC	• Autorisations centrées sur le rôle • Hiérarchie de rôle avec relations d'héritage	• Modèle statique comme DAC et MAC
Modèles de contrôle d'accès basés sur la sensibilité au contexte	ARBAC	• Structure homogène des droits des utilisateurs	• Erreurs d'administration possibles • Assister les administrateurs pour identifier et hiérarchiser les rôles
	GeoRBAC	• définit la position des sujets et des objets	Ces modèles sont des extensions de RBAC. Ils présentent les mêmes limites de RBAC qu'ils ne corrigent pas.
	TRBAC	• Active et désactive les rôles temporellement	
	STRBAC	• Les utilisateurs sont associés au temps et à l'espace	
	CRBAC	• règles contextuelles réfèrent le temps, lieu, température • s'applique aux environnements pervasifs	
Modèles de contrôle d'accès basés sur la	OrBAC	• mise à jour facile de la politique de sécurité • exprime les autorisations, interdictions, recommandations et obligations sous forme de règles	• vulnérable aux canaux cachés • manque d'aspect administratif • pas de délégation de rôles et de tâches • confiance non pris en compte

	Multi-OrBAC	• mêmes avantage que dans OrBAC • applicable aux systèmes multi-organisationnels complexes, hétérogènes, interopérables et distribués • politiques de sécurité différentes dans chaque organisation	• les mêmes que celles observées dans le modèle OrBAC
	Poly-OrBAC	• basé sur les technologies de web service • applicable dans le contexte d'une infrastructure critique (les services réseaux)	• les mêmes que celles observées dans le modèle OrBAC
Contrôle d'accès basés sur la confiance	TrustBAC	• évalue la fiabilité des utilisateurs • the confidence level validates the assignment of a subject to a role	• évaluation de la confiance du sujet par déduction • valeur du niveau de confiance comprise entre -1 et 1
	TrustRBAC	• évalue le niveau de confiance des utilisateurs. • relation déterminant la fiabilité, l'incroyance et l'incertitude.	• évaluation subjective de la confiance • valeur de niveau de confiance comprise entre 0 et 1.
	MBRC	• raisonnement avec certitude et évaluation du risque	
	DRBC	• délégation de rôles entre entités actives du système. • transfert de droits d'accès • révocation de rôle • rôles hiérarchique avec délégation en plusieurs étapes	
Contrôle d'accès basé sur la vie privée	P-RBAC	• autorisation à un rôle d'accéder aux données de la vie privée d'un sujet	Toutes les conditions ne sont pas spécifier pour protéger les données sensibles

1.5 Conclusion

Dans ce chapitre, nous avons fait une étude détaillée des modèles de contrôle d'accès les plus célèbres et les plus proches de la problématique de notre thèse.

Les premiers modèles basiques (DAC et MAC), centrés essentiellement sur le sujet (utilisateur) et l'objet (ressource à modifier dans le système) ont été améliorés avec l'introduction du rôle comment élément central du contrôle d'accès (RBAC).

Dans la politique du modèle de contrôle d'accès discrétionnaire (DAC), les règles expriment quels sont les types d'accès autorisés par utilisateur et par objet. La propagation des droits d'accès d'un utilisateur à un autre est souvent basée sur la notion de propriétaire de l'objet. L'inconvénient de cette politique est qu'elle ne gère pas le contrôle de flux. Le contrôle d'accès peut être alors mis en défaut par l'utilisation abusive de la délégation des droits. Pour résoudre ce problème, la politique du modèle de contrôle d'accès mandataire a été proposée. Cette dernière est basée sur la classification des objets et des sujets. Le niveau de sécurité associé à un objet reflète le niveau de sensibilité de l'information contenue dans l'objet alors que le niveau de sécurité associé à un sujet représente le niveau de confiance qu'accorde le système d'information au sujet. L'introduction du modèle de contrôle d'accès basé sur les rôles fait l'objet d'une attention particulière depuis quelques années et est considéré comme une alternative aux contrôles d'accès discrétionnaire et mandataire. Ainsi, au lieu d'affecter directement les permissions aux utilisateurs, elles sont affectées aux rôles dans un premier temps. Un rôle représente une compétence ou un profil dans un système d'information. Ici, La gestion des permissions est simplifiée car le nombre de rôles est réduit par rapport au nombre d'utilisateurs. Le modèle RBAC n'intégrant pas le contexte et les cas d'exception dans la définition de sa politique, plusieurs contributions de modèles de contrôle d'accès dérivés intégrants les questions d'administration de rôles, de contexte (temporel, géographique, Géo-temporel…) d'exception et de confiance ont été proposées.

Dans la section 1.3.2.2, nous observons que les modèles de contrôle d'accès basés sur la confiance ont fait l'objet de plusieurs travaux. Ces derniers, bien que très pertinents, présentent des limites au niveau de l'évaluation et de l'appréciation de la confiance. La synthèse dans le tableau 1.2 montre les limites de l'évaluation de la confiance. Cette évaluation se fait par observation du comportement du sujet, puis par déduction, si les valeurs des paramètres permettant de valider ou d'invalider le niveau de confiance sont comprises dans l'intervalle [-1,1]. A la lecture de certaines contributions, la confiance ne peut prendre que deux valeurs possibles que sont « 0 » ou « 1 ».

Pour les modèles de contrôle d'accès basés sur la préservation de la vie privée, les auteurs ont travaillé sur les stratégies d'autorisations assignées à un rôle pour accéder aux données de la

vie privée d'un sujet. Des protocoles de confidentialité ont été proposés. Seulement, toutes les conditions ne sont pas spécifiées pour protéger les données sensibles pouvant être accessibles par des sujets malveillants.

Les systèmes d'informations devenus complexes et très dynamiques (doivent prévoir les situations d'exception, les variations de contexte etc.), il est opportun de proposer des modèles hybrides flexibles (intègrent la logique non monotone gérant les cas par défaut et les cas d'exception) et légers pouvant prendre en compte les aspects essentiels exigés des modèles de contrôle d'accès dynamique. Les limites des modèles de contrôle d'accès observées dans notre état de l'art justifient du choix de la problématique de notre thèse à savoir, améliorer les modèles de contrôle d'accès basés sur la délégation et la confiance. Notre contribution portera principalement sur l'évaluation de la confiance afin d'en minimiser les erreurs. Nous travaillerons aussi sur la question de la protection de la vie privée.

Dans la suite de notre travail, nous allons proposer des modèles qui prennent en compte les forces et corrigent les limites des modèles de contrôle d'accès étudiés dans notre revue de la littérature. Le chapitre suivant propose un modèle hybride basé sur le role et la délégation, intégrant les notions de confiance et de contexte (temporel). Le modèle ainsi proposé est implémenté dans Realm de JAVA Security, afin de rendre dynamique la gestion des rôles via un middleware.

CHAPITRE 2

Contribution au modèle de contrôle d'accès basé sur la délégation dynamique de roles via Realm

2 Contribution au modèle de contrôle d'accès basé sur la délégation dynamique De rôles

2.1 Introduction

La délégation est un élément de l'administration qui demeure important dans les systèmes de contrôle d'accès. Seulement, elle est très peu prise en compte dans les politiques de contrôle d'accès en raison de sa complexité. Les modèles proposés jusqu'à présent sont des extensions du modèle RBAC. La documentation en rapport avec le contrôle d'accès basé sur les rôles ne révèle pas suffisamment d'études sur les exigences en matière de délégation de rôles et de tâches. Pour pallier à ces insuffisances, nous contribuons à mettre en place un modèle hybride nommé Contrôle d'accès dynamique basé sur les rôles et la délégation (RDBDAC - Role and Delegation Based Dynamic Access Control), qui gère dynamiquement les mises à jour des rôles utilisateurs et la délégation des tâches, en tenant compte des paramètres tels que le niveau de confiance et le contexte temporel. Pour une meilleure expressivité de notre modèle, nous utilisons la logique non monotone T-JClassic$\delta\varepsilon$ qui permet de spécifier des autorisations non monotones avec des cas par défaut et des cas d'exceptions. Elle permet aussi de représenter des aspects temporels spécifiques à une délégation donnée.

2.2 Principes de délégation de rôle

Le concept de délégation est à l'origine de nouveaux problèmes. La délégation consiste à donner un privilège à un utilisateur actif du système sans en donner à tout autre utilisateur actif du système ayant le même rôle que le délégataire (utilisateur ayant bénéficié d'un privilège). Ce privilège peut être permanent ou temporaire. Par exemple, un enseignant titulaire dans une université pourrait déléguer une partie de ses droits à un tuteur.

La notion de délégation peut apparaître dans trois types de situations que sont la maintenance de rôle, la décentralisation de l'autorité et le travail de collaboration :

→ la maintenance d'un rôle : elle correspond au cas où un utilisateur doit déléguer une partie de ses permissions pour que toutes ses obligations soient remplies durant son absence.

→ la décentralisation de l'autorité : elle est utile dans le cas où on modifie une partie de l'organisation. Ce cas peut correspondre à l'ouverture d'un nouvel hôpital dans lequel seront transférés certains médecins exerçant déjà dans d'autres hôpitaux. Cette mobilité de personnel pourrait alors déclencher une procédure de délégation.

→ le travail de collaboration : il représente une situation qui nécessite un partage de données dans le but d'obtenir un résultat collaboratif. Par exemple, un médecin peut déléguer des permissions à ses collègues médecins afin de décider sur le cas d'un patient.

Selon E. Barka et al.[46], de nombreux problèmes peuvent se poser lors d'un processus de délégation en l'occurrence la perte de privilèges du cessionnaire, l'omission de révocation, l'erreur de confiance dans le choix du délégataire etc. Exemple : un utilisateur X ayant obtenu tous les droits d'un autre utilisateur Y peut ôter les droits à ce dernier si X possède des droits administratifs. Il peut aussi arriver qu'un cessionnaire (sujet délégant un droit) oublie de révoquer une délégation faite à un utilisateur quelconque. Ce dernier peut alors se faire passer pour quelqu'un d'autre pour accéder à des informations qui ne lui reviennent pas de droit. Ou encore, lors du choix du délégataire, le cessionnaire peut se tromper en faisant un choix subjectif ou sur la base d'une recommandation. Dans ce cas, le délégataire ne garantit pas le rendement escompté.

Suite aux exemples de problèmes de délégation présentés ci-dessus, il est important de définir le type de permission accordée lors de la définition de la délégation. Il existe deux types de permissions à savoir, des permissions délégables et des permissions non délégables. La délégation étant liée à une multitude de notions (permanente, temporaire, totale, cascade…), il est nécessaire de préciser le type de délégation. La figure 2.1 de Céline Coma et al. [26], présente l'arbre récapitulatif des notions liées à la délégation, ainsi que leurs possibles imbrications.

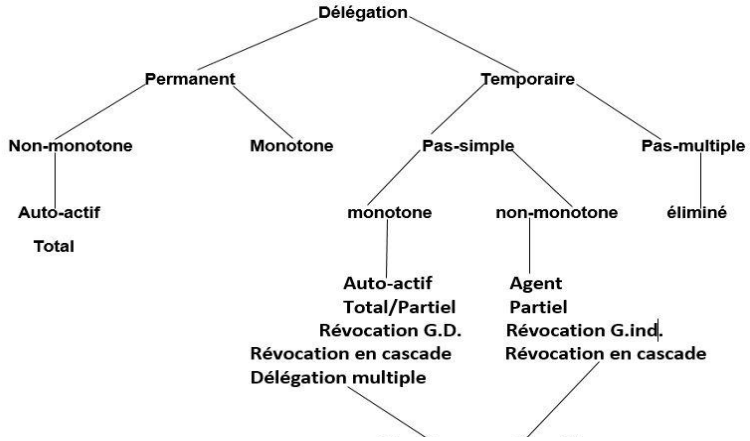

Figure 2.1 : Arbre récapitulatif des notions de délégation

2.3 Classification des différents types de délégations

Nous définissons dans cette section, des concepts et expressions liés à la délégation de privilèges. Une délégation autorise le sujet qui délègue à conserver le pouvoir de son rôle. Ce dernier peut continuer d'effectuer les mêmes opérations même après la délégation de son rôle. Il peut révoquer les privilèges octroyés à un délégataire pour les assigner à un autre. Il existe plusieurs types de délégations qui diffèrent les uns les autres par des propriétés en l'occurrence la délégation permanente, la délégation temporaire, la délégation non monotone, la délégation multiple, la délégation totale et la délégation partielle.

→ Délégation permanente : elle se réfère à la délégation dans laquelle un utilisateur qui est assigné à un autre rôle remplace de façon permanente l'utilisateur qui délègue. Dans ce type de délégation, une fois que l'utilisateur délègue son rôle, il ne peut plus le reprendre. L'utilisateur ayant reçu la délégation permanente assume l'entière responsabilité qui incombait au cessionnaire.

→ Délégation temporaire : elle fait référence à une délégation dans laquelle l'action du bénéficiaire est limitée dans le temps. Une fois que le délai de la délégation expire, la délégation n'est plus valide. Si nous nous référons au contexte de l'enseignement à distance, un enseignant peut choisir de déléguer son rôle temporairement à un tuteur pour accomplir une ou plusieurs tâches en son nom. Contrairement à la délégation permanente, l'enseignant ne perd pas son pouvoir dans l'exercice de ses fonctions et peut révoquer cette délégation à sa convenance.

→ Délégation non monotone : dans le cas d'une délégation non monotone, le délégataire perd le pouvoir du rôle délégué au terme de la durée de la délégation. Durant cette période, le cessionnaire ne pourra pas utiliser les permissions du rôle qu'il a délégué. Toutefois, il ne perd jamais le pouvoir de révoquer les rôles qu'il délègue. Par conséquent, une fois que la délégation est révoquée, le cessionnaire reprend le plein pouvoir sur ce rôle.

→ Délégation totale : elle stipule que toutes les permissions affectées au rôle peuvent être déléguées.

→ Délégation partielle : pour ce type de délégation, seuls les sous-ensembles du rôle sont délégués. De plus, il est beaucoup plus aisé d'aborder la question de hiérarchie de rôle avec la délégation partielle. Par exemple, un enseignant chercheur dans une université qui dispose d'un assistant d'enseignement, d'une responsabilité dans le laboratoire et d'un secrétaire ne peut déléguer qu'un sous-ensemble de ses rôles. (Par exemple, il peut déléguer

son rôle d'enseignant à son assistant d'enseignement, son rôle de chercheur à son assistant de laboratoire et son rôle d'administration à sa secrétaire).

→ Délégation multiple : dans ce type de délégation, un concédant peut déléguer le même droit à un groupe de personnes à tout moment. A cet effet, l'administrateur fixe le nombre de bénéficiaires en utilisant le contexte Max-Multi-Délégation.

Parler d'administrateur renvoie à l'administration. En effet, le terme administration décrit l'administrateur de la délégation. Il existe deux types d'administrations pour la délégation : la délégation auto-administrée, dans laquelle le membre qui délègue administre lui-même la délégation ; et la délégation faite par un agent dans laquelle le membre qui délègue désigne un tiers (un agent) pour conduire la délégation en son nom.

Dans les sections 2.4, nous allons décrire respectivement la logique non monotone, la logique temporelle et la logique non monotone T-JClassic$\delta\varepsilon$. Cette dernière étant le langage de description des modèles que nous proposons dans ce travail, nous montrerons comment elle a été conçue en intégrant à la logique non monotone, les connecteurs δ (pour les cas par défaut), ε (pour les cas d'exception), C-classic et le paramètre temporel (logique temporelle)

2.4 Modélisation et description de T-JClassic$\delta\varepsilon$

La modélisation de T-JClassic$\delta\varepsilon$ consiste à combiner la logique non monotone à la logique temporelle modale. Nous allons définir chaque composante afin de comprendre l'évolution et la mise en place de la logique non monotone T-JClassic$\delta\varepsilon$.

2.4.1 Logique non monotone

Selon Baader et al. [50], les logiques de descriptions sont des formalismes pour représenter une base de connaissances. Cependant les formes classiques de représentation de la logique ne permettent de représenter ni les faits par défaut ni les faits d'exception sur les concepts. Par exemple, elles ne permettent pas de représenter le fait que tous les oiseaux volent par défaut, et le pingouin est un oiseau qui exceptionnellement ne vole pas. Le fait de ne pouvoir représenter des exceptions de ce type laisse la base de connaissances définie partiellement. Cette limite affecte le processus d'inférence (raisonnement).

Pour représenter ce type de connaissance, il est nécessaire de s'appuyer sur un raisonnement non monotone basé sur l'utilisation d'une logique de description des faits par défaut Bernhard

Nebel et al. [51], Padgham et al. [52]. Ces approches utilisent une forme limitée de raisonnement par défaut où les concepts sont définis en utilisant des propriétés strictes. En considérant le fait que la plupart des concepts ne peuvent être simplement définis par l'utilisation de propriétés strictes, la base de connaissances reste partiellement définie et par conséquent le processus de classification reste incomplet. Coupey et al.[53], proposent l'approche qui permet de résoudre ce problème. Ils ont développé une nouvelle logique non monotone appelée $AL_{\delta\varepsilon}$, qui a permis d'introduire les notions de défaut et d'exception dans la définition des concepts. Elle a été élaborée en ajoutant deux connecteurs à la logique de description AL: (δ) pour représenter les faits par défaut et (ε) pour représenter les faits d'exception. Ce langage a été amélioré par l'ajout de connecteurs de C-classic qui ont permis d'augmenter son expressivité et donc de le rendre utilisable d'un point de vue pratique. Ce nouveau langage appelé JClassic a été proposé par Boustia et al.[54]. Il a permis de définir le concept Arbre (Tree) comme ayant par défaut des branches (δ With–branches) avec toujours un tronc (With–trunk) et des racines (With–roots). Ce concept est représenté dans l'axiome 2.1 comme suit :

$$\text{Tree} \equiv \delta \text{ With–branches} \sqcap \text{With–trunk} \sqcap \text{With–roots} \quad \textbf{(2.1)}$$

Toujours avec la logique de description JClassic, le concept Scion est défini dans l'axiome 2.2 comme étant un arbre qui a un an par défaut (δOne–year–old) et a exceptionnellement des branches (With–branches$^{\varepsilon}$) :

$$\text{Scion} \equiv \delta\text{One–year–old} \sqcap \text{tree} \sqcap \text{With–branches}^{\varepsilon} \quad \textbf{(2.2)}$$

Dans cet exemple, le concept Scion qui est sous-entendu par le concept Arbre n'héritera que des propriétés Tronc et Racines, mais pas la propriété With-branches puisque cette propriété est une exception pour le concept Scion.

2.4.2 Logique temporelle

Les logiques temporelles sont conçues pour représenter des informations qualifiées en termes de temps. Elles ont été largement utilisées dans plusieurs domaines tels que les bases de données, le traitement du langage naturel, la planification, etc. Dans le domaine de recherche sur la logique de description temporelle (TDL : temporal description logic), deux approches de modélisation de la notion de temps ont été envisagées à savoir : la logique temporelle modale et la logique temporelle réifiée C. Nicolas [55]. La logique temporelle réifiée (Allen, Mc Dermott) propose une logique de support d'un système temporel. Dans un intervalle de temps

donné, elle décrit comment les choses se passent (causalité temporelle), plutôt que les moments où elles se passent. Un système temporel est une représentation temporelle concrète associée à des règles de déduction. Il décrit des scénarios et assure leur cohérence P. Loor [56].

La logique temporelle modale quant à elle est une logique de raisonnement sur le temps. Elle permet la mise en place d'un système formel cohérent prenant en compte les notions de futur, de granularité, de possibilité. Une logique modale réfute l'implication logique pure et la remplace par l'implication stricte « > ». Elle intègre la notion de possibilité représentée par l'opérateur ◊ et la notion de nécessité (Toujours) représentée par l'opérateur □. La notion de possibilité (Parfois) implique que la valeur de vérité d'un énoncé peut évoluer.

T- JClassic$_{\delta\varepsilon}$ a été modélisé avec l'approche modale pour représenter les notions de « toujours» et « parfois » dans le futur. Les différentes approches de la logique temporelle basées sur des points ou des intervalles ont été largement diffusées. Artale et Franconi [57], ont mis en évidence un TDL qui permet de gérer la décidabilité. La partie temporelle TL (Logique Temporelle) utilisée pour la conception de T-JClassic est celle utilisée dans la méthode TDL définie par Artale.

2.4.3 Description de la logique T-JClassic$\delta\varepsilon$

Les auteurs O. Bettaz, N. Boustia et al. [58] sont à l'origine de la logique non monotone T-JClassic$\delta\varepsilon$. Cette logique est un modèle de description temporelle qui intègre la gestion des exceptions. Elle a été développée pour permettre une meilleure gestion du temps dans une variété de domaines tels que le raisonnement des actions et des plans, l'amélioration de la compréhension des langues naturelles et l'amélioration du contrôle d'accès.

T-JClassic$\delta\varepsilon$ permet de représenter des concepts temporels tout en ayant des connaissances par défaut. Sa logique diffère des logiques de description temporelle existantes où les composants temporels sont ajoutés aux logiques de description classiques. Elle se compose d'un ensemble d'éléments où "P" représente un ensemble de concepts atomiques, "R" un ensemble de rôles atomiques, les deux constantes "$\top$" (haut) et "$\bot$" (bas) qui représentent respectivement le concept universel et le concept du bas, l'ensemble d'individus "I" appelés individus classiques, les concepts "C" et "D", les connexions unitaires δ (Default) et ε (Exception), la conjonction binaire ⊓, le quantificateur "$\forall r.C$" qui permet la quantification universelle des valeurs de rôle, le qualificatif temporel "@" qui permet de représenter l'intervalle "X" auquel s'applique un

concept "C", le nombre réel "u" et le nombre entier "n" Bettaz et al. [59]. Les éléments ainsi listés sont consignés dans le tableau 2.1 ci-dessous.

Tableau 2.1 : Symboles de représentation syntaxique de T-JClassicδε

C, D → P	(Atomic concept)
|⊤	(Universal Concept)
|⊥	(Bottom concept)
| ¬P	(Atomic negation)
| C ⊓ D	(Intersection)
| Min u	(u is a real number)
| Max u	(u is a real number)
| ONE-OF{I1,…In}	(Concept in extension)
| R FILLS {I1,…In}	(Subset of value for R)
| R AT-LEAST n	Cardinality for R (minimum)
| R AT-MOST n	Cardinality for R (maximum)
| ∀R.C	(Universal quantifier)
| δ C	(Concept C by default)
| C^{ε}	(Exception to the concept C)
| C@X	(Qualifier)

L'utilisation de T-JClassicδε permet de représenter les aspects temporels et les propriétés telles que défaut, exception, exception d'exception, etc. Dans le cas du contrôle d'accès du domaine médical, Bettaz utilise T-JClassicδε pour définir le concept Médecin comme étant un membre du personnel (Staff–Member) qui exerce officiellement sa fonction par défaut (Exercice) et qui a le droit d'accéder aux dossiers médicaux des patients pendant les heures de travail (Access-Mdb-Records@(working Hours). L'axiome 2.3 décrit ce prédicat comme suit :

Doctor ≡ Staff–Member ⊓ Exercise ⊓ Access-Mdb-Records@(working Hours). **(2.3)**

Le concept de résident (Resident) se définit comme un médecin (Doctor) qui exceptionnellement ne fait pas d'exercice officiellement ($Exercise^{\varepsilon}$) parce qu'il est encore un étudiant :

Resident ≡ Doctor ⊓ $Exercise^{\varepsilon}$ **(2.4)**

Le concept Résident hérite de la propriété Membre du personnel et le droit d'accéder aux dossiers de la base de données médicale pendant les heures de travail, mais pas la propriété Exercice car il s'agit d'une exception pour le concept Résident. Dans un contexte d'urgence, une autre exception au concept Exercice s'applique pour les Résidents :

Resident ⊓ Emergency ≡ Doctor ⊓ (Exercise$^{\varepsilon}$) $^{\varepsilon}$ **(2.5)**

Dans le cas de de l'axiome 2.5, l'exception sur une exception omet l'exception. Ainsi, dans un contexte d'urgence, le résident a le droit de faire de l'exercice.

En considérant qu'un médecin (cessionnaire) délègue des sous rôles à une infirmière : Avant d'assigner la permission au rôle médecin, l'administrateur crée d'abord la vue délégation d'enregistrement dans laquelle il accorde au rôle médecin la permission de déléguer des sous rôles dans la vue délégation d'enregistrement définie précédemment. Cette vue est modélisée dans l'axiome 2.6 comme suit :

Use ⊑ UseL.License–Delegation ⊓ PrivilegeL.Consult ⊓ TargetL.Patient–Records. **(2.6)**

Cet axiome habilite le cessionnaire à déléguer les sous rôles consultation (PrivilegeL.Consult) et accès aux enregistrements d'un patient (TargetL.Patient–Records).

Dans [59], l'axiome 2.7 autorise le médecin (PermissionD.Doctor) à déléguer des licences dans la vue Délégation d'enregistrements :

δPermission ⊑ PermissionD.Doctor ⊓ PermissionDL.Delegate ⊓ PermissionRCDL.Record–Delegation. **(2.7)**

Suite à la description de la mise en place de la logique T-JClassic$\delta\varepsilon$ et de son utilité, nous allons décrire axiomatiquement un modèle de contrôle d'accès basé sur la délégation. Cette description se fera en référence du modèle OrBAC décrit dans la section 1.3.2. A cet effet, T-JClassic$\delta\varepsilon$ nous permettra de gérer les cas par défaut et les cas d'exception du modèle en question.

2.5 Délégation de rôle dans les contextes par défaut ou d'exception

Dans la modélisation de délégation, nous avons deux vues principales qui sont les vues administratives et les vues de délégation représentées sur la figure 2.2. Les vues administratives sont réservées aux administrateurs, chargés d'assigner les licences et les rôles aux potentiels cessionnaires. Les vues de délégation permettent aux différents cessionnaires de déléguer des permissions, en fonction du type de délégation. Chacun de ces types de délégation peut se faire soit dans un contexte par défaut(δ), soit dans un contexte d'exception(ε). L'axiome 2.8 représente le contexte par défaut Est-permis comme suit :

Est-permis ⊑ (δpermission) ⊓ (habilite) ⊓(Utilise) ⊓ (considère) **(2.8)**

Cet axiome habilite le sujet à utiliser et à considérer la permission par défaut tandis que l'axiome 2.9 habilite le sujet à utiliser et à considérer la permission dans un contexte d'exception. Cet axiome est représenté comme suit :

Est-permis ⊑ (ε permission) ⊓ (habilite) ⊓(Utilise) ⊓ (considère) **(2.9)**

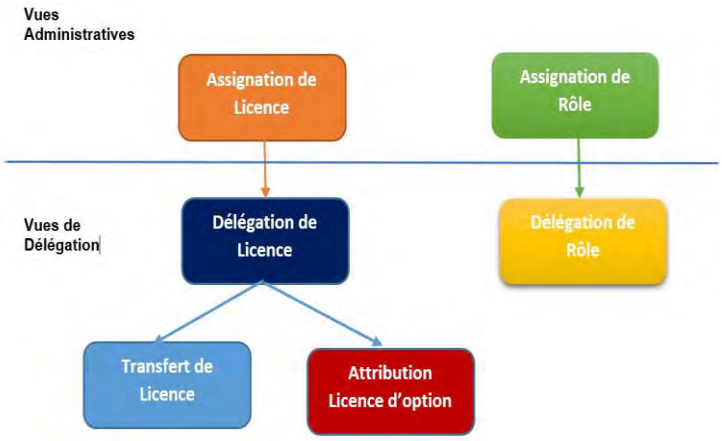

Figure 2.2 : Vues administratives et de délégation

Les types de délégations qui peuvent être faits dans les vues de délégation sont : la délégation partielle, la délégation totale, la délégation monotone etc. Bettaz et al.[59].

→ Délégation partielle : ce type de délégation permet de déléguer essentiellement une partie du rôle ou sous-rôle.

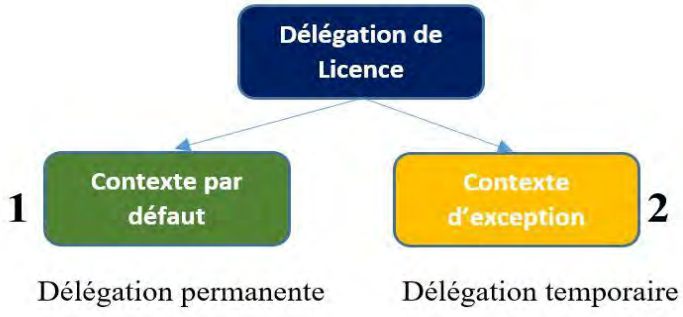

Figure 2.3 : délégation partielle

Ci-dessous, l'axiome 2.10 décrit la délégation partielle par défaut et utilise le connecteur (δ). Le prédicat permissionδ est vrai s'il vérifie à la fois la licence de délégation du cessionnaire (UtiliseL.Licence_Délégation) qui est autorisé à déléguer un sous rôle, le délégataire légitime

(BénéficiaireL.Bénéficiaire) et les privilèges qui ont été définis pour cette délégation (PrivilègeL.Action) et (CibleL.Objet).

1 : Permission ⊑ UtiliseL.Licence_Délégation ⊓ BénéficiaireL.bénéficiaire ⊓ PrivilègeL.Action ⊓ Cible.Objet **(2.10)**

L'axiome 2.11 définit une permission dans un contexte d'exception. La permission d'exception hérite des propriétés du prédicat permission par défaut, en plus du contexte d'exception qui doit être vérifié.

2 : Permission ε ⊑ UtiliseL.Licence_Délégation ⊓ BénéficiaireL.bénéficiaire ⊓ PrivilègeL.Action ⊓ CibleL.Objet **(2.11)**

→ Délégation totale : elle donne la possibilité au cessionnaire de déléguer l'intégralité de son rôle. Cette délégation de rôle se définit selon l'axiome suivant :

Habilite ⊑ UtiliseRD.Rôle_Délégation ⊓ AssigneeRD.Bénéficiaire ⊓

AssignmentRD.Rôle **(2.12)**

L'axiome 2.12 habilite l'utilisation totale des privilèges qu'autorise le rôle (UtiliseRD.Rôle_Délégation) par le bénéficiaire (AssigneeRD.Bénéficiaire) du rôle délégué.

→ Délégation monotone /non-monotone : une délégation est dite monotone lorsque le délégataire d'un rôle peut à son tour déléguer le même rôle. Sinon, la délégation est dite non monotone.

2.6 Révocation de délégation

Dans les sections précédentes, nous avons défini la terminologie en lien avec la délégation de rôle. Nous avons ensuite défini les types de délégation. Nous avons décrit comment les utilisateurs disposant d'une licence de délégation de rôle peuvent déléguer leurs droits à d'autres utilisateurs. Cependant, la cession d'un rôle peut impliquer dans certains cas la révocation de privilèges. Par exemple, dans le contexte des organisations virtuelles (e-learning, e-santé) un enseignant titulaire peut octroyer des permissions à un tuteur en cas d'indisponibilité. De même, un médecin peut déléguer des permissions à ses collaborateurs, afin de décider sur le cas du patient. Lorsque la période définie pour la délégation arrive à son terme, le cessionnaire peut retirer les permissions aux délégataires. Dans cette section, nous examinerons les différents types de révocations. Nous examinerons également dans quelles conditions il n'est pas possible

de révoquer une décision antérieure et les questions qui pourraient se poser à la suite d'une révocation.

La révocation est un aspect important dans les modèles de délégation. Il existe deux principaux types de révocations à savoir le Grant Dependency (GD) et le Grant Independency (GID).

→ Grant Dependency : dans ce type de révocation, le cessionnaire est la seule personne habilitée à révoquer les droits ou le rôle délégué.

→ Grant Independency : il donne le droit à tous les membres assignés à un rôle de révoquer le cessionnaire (délégant ayant obtenu le droit de déléguer un rôle) du rôle qui leur a été délégué.

Ces deux situations sont représentées par défaut avec les permissions suivantes, en utilisant le contexte GD ou GID.

GD : δPermission ⊑ PermissionS.Subject ⊓ PermissionR.Revoke ⊓ PermissionLD.License–Delegation ⊓ PermissionD.GD **(2.13)**

La permission par défaut du GD de l'axiome 2.13 vérifie à la fois que le sujet dispose des privilèges d'action sur des objets (PermissionS.Subject), d'une licence lui donnant le droit de déléguer un rôle (PermissionLD.License–Delegation), d'une permission lui permettant de révoquer une délégation (PermissionR.Revoke) sans être révoqué en retour par le délégataire (PermissionD.GD).

GID : δPermission ⊑ PermissionS.Subject ⊓ PermissionR.Revoke ⊓ PermissionLD.License–Delegation ⊓ PermissionID.GID **(2.14)**

L'axiome 2.14 vérifie toutes les caractéristiques de l'axiome 2.13, à l'exception de PermissionID.GID qui autorise les délégataires du rôle à révoquer le cessionnaire de ce rôle.

→ Révocation en cascade : la chaîne de délégation résultant du processus de délégation en plusieurs étapes devrait pouvoir être indirectement révoquée. Cette opération est possible par l'utilisation d'une licence contextuelle, où la délégation de droit n'est valable que dans le cas où le concédant dispose encore de ce droit.

La vue Délégation en cascade, qui est une sous-vue de la vue Délégation de licence se définit comme suit :

$$\delta\text{Permission} \sqsubseteq \text{UseL.Cascading–Delegation} \sqcap \text{GranteeL.Subject} \sqcap \text{GrantorL.Gr} \sqcap \text{PrivilegeL.Action} \sqcap \text{TargetL.Objet} \sqcap \text{ContextL.C} \quad \textbf{(2.15)}$$

Dans l'axiome 2.15, l'utilisateur a le privilège de révoquer en cascade la délégation (UseL.Cascading–Delegation). Il dispose d'une Licence (GrantorL.Gr) qui lui permet d'autoriser le délégataire (GrantorL.Gr) à agir (PrivilegeL.Action) sur des objets (TargetL.Objet) dans un contexte donné (ContextL.C).

L'insertion d'un objet dans cette vue crée une permission avec un contexte supplémentaire (contexte Valid-Delegation) qui vérifie si le délégataire a toujours son droit.

2.7 Proposition du Modèle RDBDAC

Le modèle RBAC implémenté dans Realm de Java EE Security est un modèle rigide et statique qui nécessite la connaissance du code pour la mise à jour des politiques de contrôle d'accès. De plus, ce modèle n'intègre pas les notions de délégation, de confiance et de contexte. Il ne gère pas non plus les cas d'exception. C'est dans cette dynamique que le modèle RDBDAC a été mis en place, afin de corriger les limites ci-haut évoquées.

Le modèle de contrôle d'accès dynamique basé sur le rôle et la délégation (RDBDAC) est un modèle hybride composé de plusieurs paramètres inspirés des modèles décrits précédemment dans la section 1.3 de notre thèse. Les éléments centraux de notre modèle sont la délégation, la confiance et le contexte temporel Bilong et al. [48].

2.7.1 Contexte et définition des acteurs

2.7.1.1 Contexte

L'accès à l'enseignement supérieur à distance demeure une question récurrente pour les jeunes africains diplômés en quête de formation de qualité. Les orientations pléthoriques dans les universités virtuelles africaines, particulièrement l'université virtuelle du Sénégal créent un souci de disponibilité par rapport aux enseignements. Pour limiter certains manquements liés à l'insuffisance du nombre d'enseignants titulaires disponibles et prendre correctement à charge les apprentissages, nous proposons un modèle hybride qui permettra aux enseignants titulaires de déléguer leurs rôles ou sous rôles aux tuteurs qui leur ont été assignés. Nous décrivons notre modèle dans un environnement virtuel universitaire où les enseignants peuvent déléguer temporairement des tâches aux tuteurs qui travaillent sous leur coupole.

2.7.1.2 Définition des acteurs du système

Nous définissons le concept enseignant (Teacher) comme un membre du personnel (Staff_Member) qui exerce formellement sa fonction par défaut, avec des privilèges d'accès (δPermission) liés à son rôle(Role_Assigment). Il enseigne pendant les heures de travail (@(working_hours)). Nous définissons l'Enseignant dans l'axiome 2.16 suivant :

$$\text{Teacher} \equiv \text{Staff\_Member} \sqcap \text{Licence\_assigment} \sqcap \text{Role\_Assigment} \sqcap \delta\text{Permission} \sqcap @(\text{working\_hours}) \quad \textbf{(2.16)}$$

Le concept de tuteur fait référence à un membre du personnel (Staff_Member) qui est officiellement affecté à son rôle par défaut (δRole_Assigment). Il peut néanmoins bénéficier d'une délégation de tâches sur une période donnée par l'enseignant. Nous définissons le tuteur dans l'axiome suivant:

$$\text{Tutor} \equiv \text{Staff\_Member} \sqcap \delta\text{Role\_Assigment} \sqcap \delta\text{Permission} \quad \textbf{(2.17)}$$

Il n'est pas possible d'attribuer la licence au tuteur parce qu'au regard de l'organisation pédagogique de notre étude de cas, le tuteur n'a pas le droit de déléguer ses tâches, même pas à son homologue.

2.7.2 Assignation de licence et de rôle aux acteurs

2.7.2.1 Assignation de licence et de rôle à l'enseignant

Lors de l'affectation d'un rôle à un enseignant (Assignee), l'administrateur attribue également une licence de délégation qui lui permettra de déléguer son rôle ou des tâches sur une période donnée. Les assignations de licence et de rôle sont définies respectivement dans les axiomes 2.18 et 2.19 comme suit :

$$\delta\text{Licence\_Assigment} \sqsubseteq \text{AssigneeL.assigment} \sqcap \text{LicenceL.assigment} \sqcap \delta\text{PrivilegesL.Action} \sqcap \text{CibleL.Objet} \quad \textbf{(2.18)}$$

L'axiome 2.18 qui décrit une assignation de licence par défaut (δLicence_Assigment) définit d'abord le cessionnaire (AssigneeL.assigment) afin qu'il puisse déléguer son rôle. Ensuite il définit la licence qui lui permettra de déléguer son rôle (LicenceL.assigment), ainsi que les privilèges par défaut (δPrivilegesL.Action) qui lui donnent le droit d'agir sur des objets définis (CibleL.Objet).

δRole_Assigment ⊑ AssigneeL.assigment ∏ RoleL.assigment ∏ δPrivilegesL.Action ∏ CibleL.Objet **(2.19)**

L'axiome 2.19 gère l'assignation de rôle. Elle comprend plusieurs éléments (propriétés) à savoir définition du cessionnaire (AssigneeL.assigment) à qui le rôle sera assigné, définition du rôle qui pourrait être délégué, puis définition des privilèges par défaut décrivant les actions autorisées (δPrivilegesL.Action) sur les objets ciblés (CibleL.Objet)

2.7.2.2 Assignation de rôle au tuteur

Lorsque l'administrateur assigne des tuteurs aux enseignants, il définit la valeur faisant référence au niveau de confiance du tuteur. Seuls les tuteurs disposant d'un niveau de confiance valide seront vus par l'enseignant qui voudrait déléguer son rôle.

δRole_Assigment ⊑ TutorR.assigment ∏ RoleR.assigment ∏ Trust_levelR.assigment =1 ∏ δPrivilegesR.Action ∏ CibleR.Objet **(2.20)**

L'assignation de rôle tel que décrit par l'axiome 2.20 définit d'abord le tuteur qui bénéficiera du rôle (TutorR.assigment), ensuite il assigne le rôle au tuteur (RoleR.assigment), puis il définit le niveau de confiance (Trust_levelR.assigment) qui permettrait au tuteur de bénéficier d'une délégation, et enfin fixe les permissions (δPrivilegesR.Action et CibleR.Objet) propres au rôle du tuteur.

2.7.3 Délégation de rôle et de taches

2.7.3.1 Délégation de rôle

La vue de délégation des rôles permet une délégation totale du rôle. Ce type de délégation est défini par l'axiome 2.21 suivant :

Empower ⊑ UseRD.Role_Delegation ∏ Trust_levelRD.Trust = 1 ∏ AssigneeRD.Grantee ∏ AssignmentRD.Role **(2.21)**

L'axiome 2.21 (Empower) gère la délégation totale du rôle. Il habilite le délégataire (AssigneeRD.Grantee) dont le niveau de confiance doit être vrai (Trust_levelRD.Trust = 1) à utiliser tous les privilèges (UseRD.Role_Delegation) autorisés par le rôle (AssignmentRD.Role).

2.7.3.2 Délégation de tâches

Déléguer des tâches revient à faire une délégation partielle. Il existe deux types de vues de délégation : la vue de délégation de licence et la vue de délégation de rôle. La vue de délégation de licence donne accès à la délégation partielle. Elle permet au cessionnaire de déléguer des tâches durant une période déterminée. En référence au contexte défini dans la section 2.4.1.1, l'enseignant peut choisir de déléguer seulement une partie de son rôle en cas d'indisponibilité. Pour qu'il y ait délégation, le tuteur doit avoir un niveau de confiance valide. Le tuteur peut alors enseigner, évaluer les apprenants et modifier d'autres objets autorisés. Nous définissons la délégation partielle dans contexte d'exception temporelle par l'axiome 2.22 suivant :

$$\text{Permission} \sqsubseteq \text{UseL.Licence\_Delegation} \sqcap \text{Trust\_levelL.Trust=1} \sqcap \text{GranteeL.Grantor} \sqcap \text{PrivilegeL.Action} \sqcap \text{Target.Object} \sqcap \text{DurationL.Time}^{\varepsilon} \quad \textbf{(2.22)}$$

Le prédicat de l'axiome 2.22 est vrai s'il vérifie à la fois la licence de délégation du cessionnaire (UseL.Licence_Delegation), le délégataire (GranteeL.Grantor) qui est chargé d'exécuter les tâches déléguées et dispose d'un niveau de confiance valide (Trust_levelL.Trust=1), les permissions qui ont été définies pour cette délégation (PrivilègeL.Action et CibleL.Objet). Le prédicat Permission vérifiera l'exception (DurationL.Time$^{\varepsilon}$), qui est la durée au bout de laquelle la délégation prendra fin.

2.7.4 Révocation de délégation dans RDBDAC

La révocation est le processus de récupération de la licence ou du rôle délégué. Dans le contexte décrit pour notre modèle, seule la révocation Grant Dependency (GD) est possible. Car, le cessionnaire contrôle tous les privilèges qu'il délègue et seul lui peut révoquer le rôle ou le sous rôle qu'il délègue. Nous nous représentons axiomatiquement la révocation de délégation comme suit :

$$\text{Permission} \sqsubseteq \text{UseL.License\_Delegation} \sqcap \text{AssigneeL\_Assignee} \sqcap \text{PermissionD.GD\_Revoke} \sqcap \text{DurationEndL.Licence\_Delegation} \quad \textbf{(2.23)}$$

Le prédicat défini dans l'axiome 2.23 est vrai s'il vérifie à la fois l'utilisation de la licence de délégation (UseL.License_Delegation), le cessionnaire disposant du droit de délégation (AssigneeL_Assignee), la permission permettant au cessionnaire seul de révoquer la délégation

que lui-même a faite (PermissionD.GD_Revoke). La révocation ne sera effective que durant le temps (DurationEndL.Licence_Delegation) prévu pour la délégation.

2.8 Diagrammes de classe et de séquence du processus de délégation de rôle

Le diagramme de séquence de la figure 2.4 ci-dessus illustre le processus de délégation, dès l'attribution des rôles et des licences jusqu'à la révocation de la délégation :

1. Attribution de licence par l'administrateur à l'enseignant.
2. Attribution des rôles par l'administrateur aux utilisateurs.
3. Délégation de licence au cessionnaire.
4. Si le niveau de confiance est vrai, le cessionnaire délègue une ou plusieurs tâches au tuteur.
5. Si la durée de la délégation = vraie, la délégation de tâches est annulée.

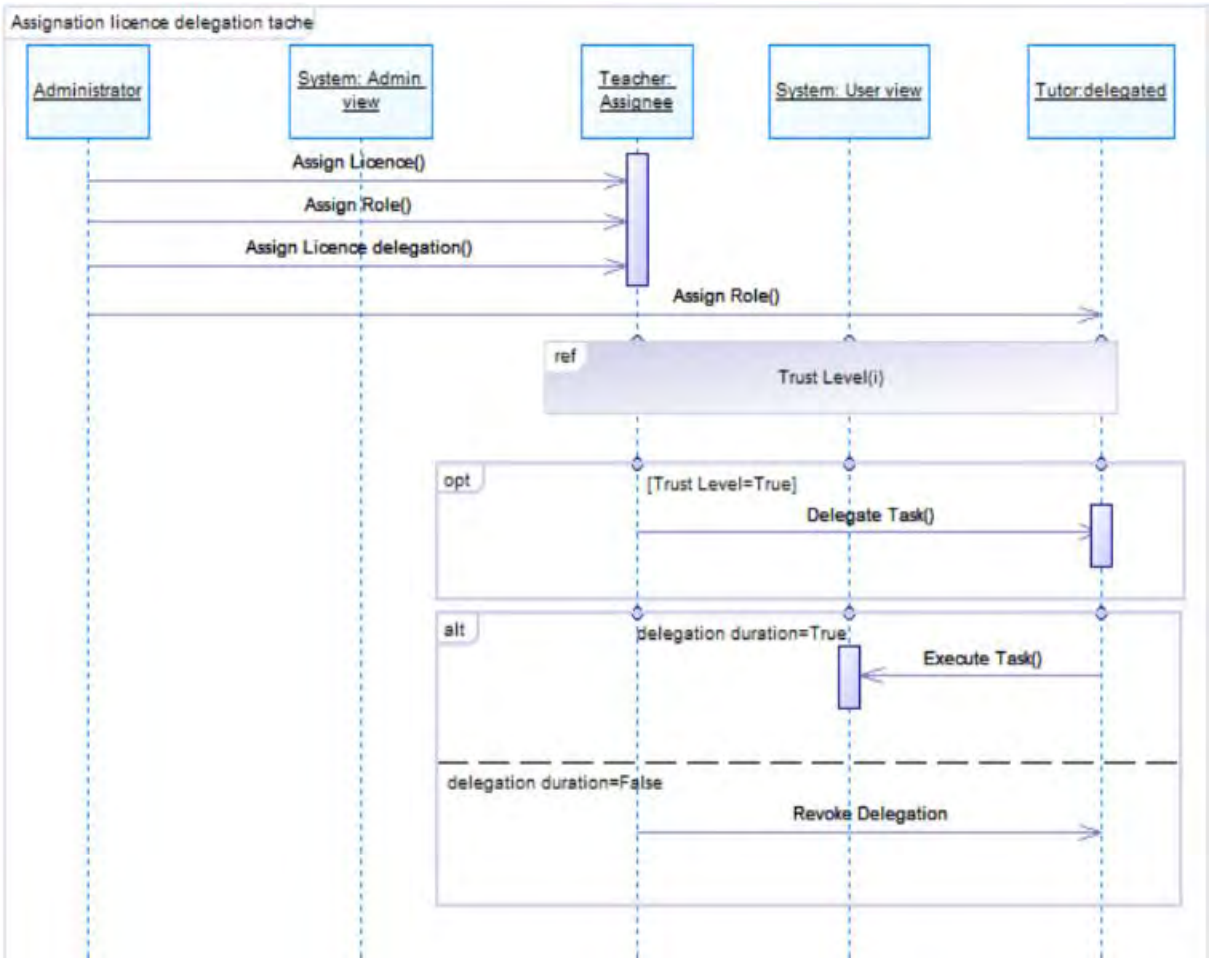

Figure 2.4 : diagramme de séquence du processus de délégation

Le diagramme de classes ci-dessous montre la notion d'héritage dans la relation de dépendance entre le cessionnaire représenté par l'enseignant et l'utilisateur qui représente le tuteur. Le délégataire, ayant un niveau de confiance valide peut exceptionnellement accéder aux tâches qui lui sont déléguées par le cessionnaire.

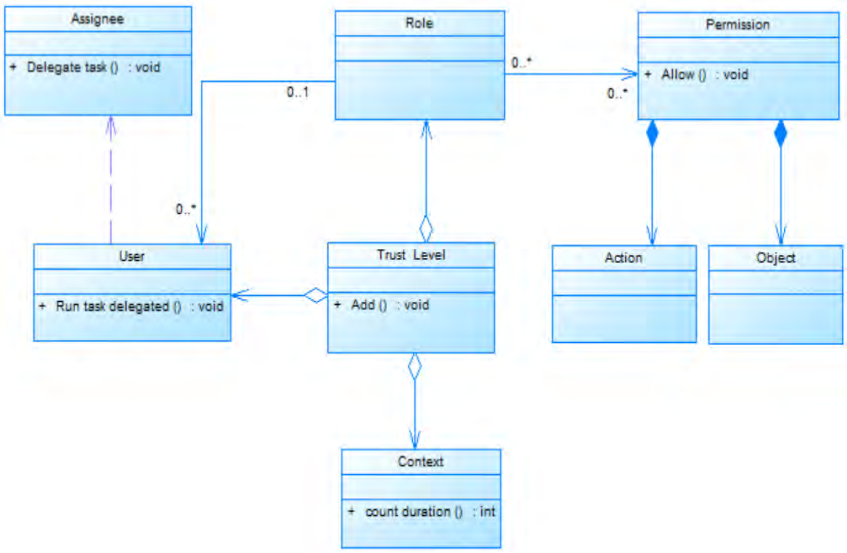

Figure 2.5 : diagramme de classe: Relations de délégation de tâches

Nous avons fait une comparaison du modèle RDBDAC avec les modèles connexes. Le tableau 2.2 ci-dessous montre que le modèle proposé est plus complet, plus souple dans la définition des politiques de sécurité du contrôle d'accès et plus facile à mettre en œuvre.

Tableau 2.2 : Comparaison entre RDBDAC et les modèles antérieurs

Critères de comparaison	DAC	MAC	RBAC	TRUSTBAC	TRBAC	ORBAC	RDBDAC
Contrôle d'accès	✓	✓	✓	✓	✓	✓	✓
Règles Contextuelles	x	x	x	X	✓	✓	✓
Administration centralisée	x	✓	x	X	x	X	✓
Trust Level	x	x	x	✓	x	X	✓
Dynamique	x	x	x	✓	✓	✓	✓
Delegation /révocation	x	x	x	X	x	X	✓
permission, recommandation, prohibition, obligation	x	x	x	X	x	✓	✓

2.9 Modèle et Architecture RDBDAC

La Figure 2.6 ci-dessous représente le modèle RDBDAC composé de trois principales vues à savoir la vue Administrative, la vue de délégation et la vue utilisateur. La vue administrative permet de gérer les assignations de licence et des rôles. La vue de délégation permet au cédant disposant d'une licence de délégation de céder temporairement son rôle au cessionnaire. Ce dernier, dans la vue utilisateur, peut alors, avec un niveau de confiance valide, accéder au rôle qui lui a été délégué après s'être authentifié. Le modèle RDBDAC est défini dans un contexte temporel [48].

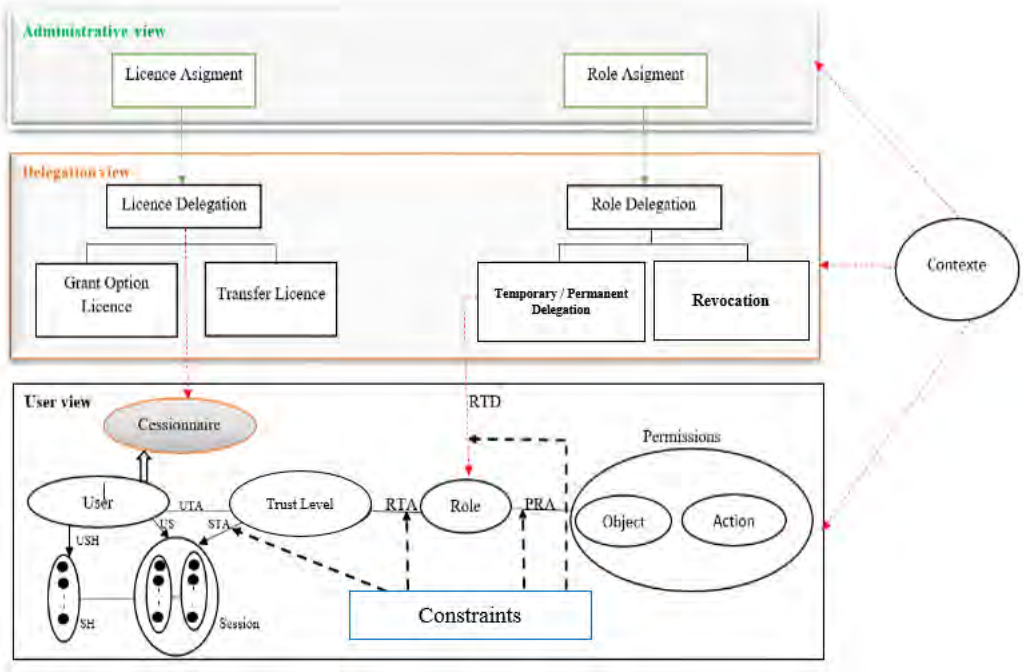

Figure 2.6 : modèle RDBDAC

L'architecture du modèle RDBDAC repose sur le principe de la délégation dynamique des tâches de l'enseignant à un tuteur. Suite à la configuration des fichiers XML via Realm, une base de données est paramétrée pour définir l'ensemble des rôles, des utilisateurs, des permissions via les objets et des actions à entreprendre sur ces objets. Un middleware est interfacé pour permettre aux différents utilisateurs d'interagir avec la base de données et l'automate. Lorsqu'un utilisateur se connecte au middleware, il est redirigé vers sa vue afin d'effectuer les opérations qui lui sont assignées. La mise en œuvre de cette architecture permet de disposer d'un environnement e-learning intelligent. Pour montrer la faisabilité de notre démarche, nous avons mis en place une plateforme dans le cadre de l'Université Virtuelle du Sénégal. Nous avons utilisé le langage de programmation JEE pour développer la plateforme.

La figure 2.7 montre l'architecture du modèle qui permet d'administrer l'ensemble de l'application, y compris la configuration et la gestion du contrôle d'accès. Pour ce faire, l'administrateur attribue dynamiquement des rôles ou des tuteurs à différents utilisateurs en fonction de leurs profils.

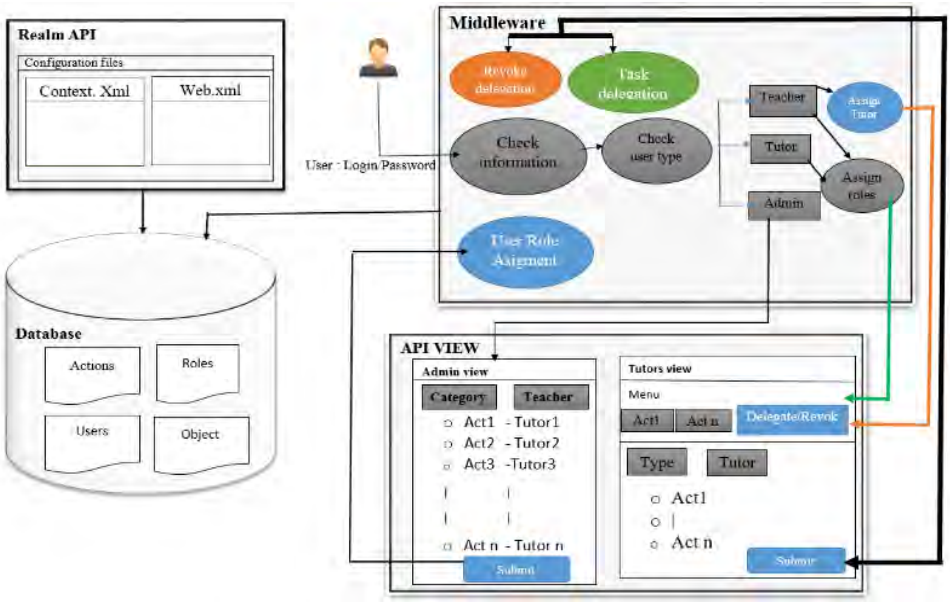

Figure 2.7 : architecture du modèle RDBDAC

2.10 Conclusion

Dans ce chapitre, nous avons proposé le modèle RDBDAC pour la gestion dynamique du contrôle d'accès basé sur les rôles. Ce modèle permet de gérer le côté statique du modèle RBAC dans « Java EE Security de Realm » et offre une interface conviviale permettant de gérer les rôles de façon dynamique, sans avoir à modifier le code source. Le modèle RDBDAC met l'accent sur les paramètres tels que la confiance, la délégation et le contexte temporel. En nous référant au contexte défini dans la section 2.4.1.1, une vue « administrateur » permet d'attribuer des rôles aux tuteurs et aux enseignants. La révocation de délégation est également dynamique, car le tuteur perd les privilèges d'agir sur un objet donné une fois que le temps alloué à la délégation est épuisé. C'est en ce sens que nous avons choisi de décrire notre modèle avec la logique de description non monotone T-JClassic$\delta\varepsilon$. Nous avons vu dans la section 2.4 que T-JClassic$\delta\varepsilon$ découle de la composition de la logique non monotone avec les connecteurs (δ, ε, C-classic) permettant de gérer les faits par défaut ainsi que les faits d'exception et d'améliorer l'expressivité de la logique. En plus des connecteurs, la modélisation de T- JClassic$\delta\varepsilon$ a été

renforcée par la logique modale de description temporelle qui intègre des notions essentielles que sont la possibilité et la nécessité.

Nous avons implémenté le modèle avec JEE et l'outil Realm de Tomcat. La mise à jour des rôles dans l'ensemble est facilitée grâce à l'interface d'administration. Au lieu de faire recours au code source du fichier XML pour changer les politiques de contrôle d'accès, l'administrateur coche des options offertes sur l'interface graphique pour réaliser des mises à jour. Notre modèle présente des limites en ce sens qu'il ne prend pas en compte le paramètre géo-temporel ainsi que les vues abstraites et concrètes présentes dans le modèle OrBAC. La délégation de rôle dans notre modèle n'est pas fiable du fait que l'appréciation du niveau de confiance du délégataire peut être altérée par des préférences arbitraires. Dans le chapitre suivant, nous allons étudier le système de délégation basé sur la confiance. Nous y évaluerons les critères d'appréciation de la confiance afin de minimiser les erreurs de confiance. Le modèle sera décrit dans un environnement d'e-learning où un enseignant pourra déléguer un rôle ou une tache à un tuteur.

CHAPITRE 3

Contribution à l'évaluation de la fonction de confiance dans les modèles de contrôle d'accès

3 Contribution à l'évaluation de la fonction de confiance dans les modèles de contrôle d'accès

3.1 Introduction

La confiance est une notion clé dans la gestion des contrôles d'accès. Contrôler un accès dans un système d'information revient à renforcer la confidentialité, l'intégrité et la protection de l'information. Nous pouvons ainsi dire que contrôler un accès revient à authentifier les utilisateurs désirant se connecter au système d'information. Plusieurs politiques de contrôle d'accès ont permis de proposer des modèles. Ces derniers ont connu une évolution fulgurante grâce à de nombreux travaux de recherche. Nous avons ainsi énuméré des modèles de contrôle d'accès statiques et dynamiques. Ces derniers de par leur fonctionnalité, nécessitent la prise en compte de la confiance. Plusieurs modèles de délégation basés sur la confiance ont été proposés. Selon Ahadipour et al. [60], les modèles de contrôle d'accès et les approches de confiance sont nécessaires pour supporter les fonctionnalités dynamiques et distribuées des systèmes et de leurs composants. Les modèles de confiance appliqués aux contrôles d'accès jusqu'à ce jour sont fondés sur la recommandation et la subjectivité. Par ailleurs, les modèles de contrôle d'accès basés sur la délégation et les rôles requièrent une évaluation de la confiance avec un raisonnement basé sur la neutralité et l'impartialité.

La délégation a pour but de faire exécuter le travail en le cédant à quelqu'un d'autre qui peut être un subordonné ou un sujet ayant les mêmes droits que le cessionnaire. Certains systèmes de gestion de la confiance, tels que KeyNote et Simple Public Key Infrastructure (SPKI) / Simple Distributed Security Infrastructure (SDSI), utilisent des qualifications par sujet ou des références pour déléguer des autorisations.

Plusieurs autres travaux mettant en évidence les notions de confiance et de délégation ont été réalisés. Toutefois, à la lumière de l'analyse de la revue de la littérature, l'appréciation de la confiance demeure arbitraire.

Notre contribution dans ce chapitre consiste à améliorer le modèle de contrôle d'accès dynamique hybride basé sur les rôles (RDBDAC) en utilisant les techniques de l'apprentissage automatique. Nous avons précisé dans le chapitre précédent que le modèle RDBDAC propose

une délégation dynamique de rôle basée sur la confiance. Seulement, cette confiance repose sur des approches abstraites où on ne peut lui assigner que des valeurs booléennes telles que « 0 » ou « 1 ». Dans ce chapitre, nous nous intéresserons à l'évaluation impartiale et neutre de la confiance dans un contexte d'e-learning. Pour cela, nous avons identifié un certain nombre de critères faisant partie des éléments clés de recrutement de tuteur dans l'enseignement supérieur. De ces critères, nous pouvons citer la qualification académique (niveau d'étude), la qualité de la carrière académique (production scientifique), la carrière professionnelle, l'ancienneté, et l'expérience dans la formation à distance.

Dans un premier temps, nous allons pondérer les critères cités ci-haut, afin de minimiser les erreurs de décision. En supposant que nous sommes dans un contexte d'université virtuelle où nous avons des tuteurs à recruter, les critères pondérés nous permettront de minimiser des erreurs de recrutement et donc de minimiser les erreurs de confiance. Ainsi, un tuteur ayant cumulé un ensemble de valeurs supérieures à la valeur seuil de recrutement aura des chances de bénéficier d'une délégation de rôle.

Dans un deuxième temps, nous allons proposer un algorithme de scoring (score) qui permettra d'afficher le tuteur ayant la valeur la plus élevée du niveau confiance. Ce dernier sera considéré comme digne de confiance et bénéficiera en priorité de la délégation.

Pour ce faire, nous utiliserons l'algorithme de régression linéaire et l'algorithme de régression vecteur support (SVR- Support Vector Regression).

L'intérêt de notre contribution consiste à remplacer progressivement l'administration manuelle des contrôles d'accès par l'administration automatique grâce à la prédiction.

Dans la suite de ce chapitre, nous allons tout d'abord définir les différents modèles de l'apprentissage automatique, puis nous présenterons apport de l'apprentissage supervisé dans le contrôle d'accès et enfin, nous ferons une description du modèle de notre contribution.

3.2 Définition des modèles d'apprentissage automatique

L'apprentissage automatique (Machine Learning) est un champ d'étude de l'intelligence artificielle qui se base sur des approches statistiques. Il constitue une catégorie d'algorithme qui permet aux applications logicielles de prédire des résultats sans être explicitement programmées. Il permet de réaliser la prédiction de score ou de classe d'appartenance,

l'identification des tendances cachées ou de classes cachées et la génération de nouvelles stratégies ou de nouveaux modèles à partir de grandes masses de données. Son principe de base consiste à créer des algorithmes capables de recevoir des données d'entrée et de faire une analyse statistique pour prédire un résultat, tout en faisant des mises à jour au fur et à mesure que de nouvelles données deviennent disponibles.

L'apprentissage automatique s'articule autour de trois grandes familles d'algorithme qui sont les algorithmes d'apprentissage supervisé, les algorithmes d'apprentissage non supervisé et les algorithmes d'apprentissage par renforcement :

→ algorithmes d'apprentissage supervisé (régression linéaire, régression vectorielle de support ou SVR, K Nearest Neighbors, SVC linéaire ou classificateur de vecteur de support, regression logistique, arbre de régression, réseaux de neurones, Support vecteurs Machine...);

→ algorithmes d'apprentissage non supervisé (K-means clustering, deep learning, réduction de la dimensionnalité, analyse des composants principaux, analyse des composants indépendants, modèles de distribution, classification hiérarchique…);

→ algorithmes d'apprentissage par renforcement.

3.2.1 Apprentissage supervisé

L'apprentissage supervisé consiste à apprendre le modèle d'un phénomène à partir d'exemples d'apprentissages. Il classe à partir d'échantillons de sortie déjà étiquetés (données catégorisées) et a pour but de faire des prédictions correctes sur des données non présentes dans l'ensemble d'apprentissage [61].

En apprentissage supervisé, l'algorithme d'apprentissage a accès à un ensemble d'apprentissages $S \stackrel{def}{=} \{(x1, y1), \ldots, (x_m, y_m)\}$ de m exemples où chaque exemple est une paire (x, y) et y représente la sortie attendue lorsque l'entrée est x.

Soit X est l'ensemble des entrées possibles et Y l'ensemble des sorties possibles, $S \subseteq X \times Y$. De plus, les exemples d'apprentissages dans S sont générés indépendamment d'une distribution inconnue D. La tâche de l'algorithme d'apprentissage revient donc à produire une fonction h : $X \rightarrow Y$ [62].

En d'autres termes, l'apprentissage est dit supervisé lorsque les données qui entrent dans le processus sont déjà catégorisées et utilisées comme des variables d'entrée dans des algorithmes. Ces derniers se servent de ces données pour prédire un résultat. Les résultats prédits permettront aux algorithmes de continuer la prédiction même si plus tard, les données ne seront plus catégorisées. On peut par exemple donner au système une liste de profils clients contenant des habitudes d'achat, et expliquer à l'algorithme lesquels des clients sont habituels et lesquels sont des clients occasionnels. Une fois l'apprentissage terminé, l'algorithme devra pouvoir déterminer tout seul à partir d'un profil client à quelle catégorie celui-ci appartient.

L'apprentissage supervisé est généralement effectué dans le contexte de la classification et de la régression.

→ Classification:

On parle de problème de classification lorsque la variable de sortie est une catégorie, telle que «couleur», «maladie», «pas de maladie». Exemples :

- En finance et dans le secteur bancaire pour la détection de la fraude par carte de crédit (fraude, pas fraude).
- Détection de courrier électronique indésirable (spam, pas spam).
- En médecine, pour prédire si un patient a une maladie particulière ou non.

→ Régression:

Un problème de régression se pose lorsque la variable de sortie est une valeur réelle, telle que le «prix» ou le «poids». Exemple : prédire le poids d'un critère, prédire le cours de bourse.

3.2.2 Apprentissage non supervisé

L'apprentissage non supervisé est beaucoup plus complexe car, le système doit détecter les similarités dans les données qu'il reçoit et les organiser en fonction de ces dernières. Ce type d'apprentissage présente un avantage indéniable. Son élimination ou sa réduction constitue un frein à l'implémentation de la technologie.

L'apprentissage non supervisé consiste à ne disposer que de données d'entrée (X) et non de variables de sortie correspondantes. Son objectif est de modéliser la structure ou la distribution sous-jacente dans les données afin d'en apprendre davantage sur les données. Contrairement aux algorithmes de l'apprentissage supervisé, les algorithmes de l'apprentissage non supervisé

sont laissés à leurs propres mécanismes afin de découvrir et présenter la structure intéressante des données. Nous représentons ci-dessous l'algorithme 1 Kmeans, qui est l'un des algorithmes de l'apprentissage non supervisé J. Jacques [63].

Algorithm 1 kmeans

1: init. : tirages au hasard de K centres μk parmi les n observations
2: **while** partition non stable **do**
3: affecter chaque observation à la classe dont le centre est le plus proche
4: recalculer r les centres (moyennes) des classes
5: **end while**.

- L'algorithme des kmeans minimise l'inertie intra-classe W(Z) :

T = B(Z) +W(Z)

T = $\sum_{i=1}^{n} d^2(X_i, \mu)$: inertie totale du nuage de point (μ est le centre global)

B(Z) = $\sum_{k=1}^{k} n_k d^2(\mu_k, \mu)$: inertie interclasse (n_k nb. obs. dans classe k)

W(Z) = $\sum_{k=1}^{k} \sum_{i=1,n:z_{i=k}} d^2(X_i, \mu)$: Inertie intra-classe

- l'algorithme des kmeans est convergeant
- la solution peut dépendre de l'initialisation (on réalise plusieurs initialisations et on conserve celle qui minimise W(Z)
- l'inertie intra-classe W(Z) diminue lorsque K augmente

K-means est une méthode de segmentation de données. Étant donnés des points et un entier k, le problème est de diviser les points en k clusters, de façon à minimiser un calcul de distances. Son avantage est que sa complexité est linéaire ce qui le rend applicable à de grands volumes de données. Tandis que son inconvénient est que les clusters dépendent de l'initialisation, de la distance choisie ainsi que de l'équilibre entre les classes [61].

L'apprentissage non supervisé comprend deux catégories d'algorithmes: algorithmes de regroupement et algorithmes d'association.

→ Regroupement ou Clustering : la mise en cluster consiste à séparer ou à diviser un ensemble de données en un certain nombre de groupes, de sorte que les ensembles de données appartenant aux mêmes groupes se ressemblent davantage que ceux d'autres groupes. En termes simples, l'objectif est de séparer les groupes ayant des traits similaires et de les assigner en grappes.

→ Association: l'association consiste à découvrir des relations intéressantes entre des variables dans de grandes bases de données. Par exemple, les personnes dont le revenu augmente ont aussi tendance à relever leur niveau de vie. Probabilité de cooccurrence d'éléments dans une collection.

3.2.3 Apprentissage par renforcement

Aurélia Léon [64] définit l'apprentissage par renforcement comme un domaine de l'apprentissage automatique dans lequel un agent apprend quelles actions effectuer dans un environnement afin de maximiser une récompense. Autrement dit, l'apprentissage par renforcement consiste à apprendre les actions provenant d'expériences, de façon à optimiser une récompense quantitative au cours du temps. L'agent est plongé au sein d'un environnement, et prend ses décisions en fonction de son état courant. En retour, l'environnement procure à l'agent une récompense. Cette dernière peut être positive ou négative. L'agent recherche un comportement décisionnel au travers d'expériences itérées S. Zaidenberg [65]. Ce dernier évolue au sein d'un environnement, et peut recevoir une observation de l'état actuel de l'environnement afin de choisir quelle action effectuer pour atteindre son but. Le but peut être défini par la récompense que l'agent cherche à maximiser.

La figure 3.1 ci-dessous montre les interactions entre l'agent et l'environnement dans un cadre d'apprentissage par renforcement au temps t. L'agent reçoit une observation x_t de l'environnement, qui lui permet de choisir une action a_t et de l'effectuer dans l'environnement. Il reçoit ensuite une récompense r_{t+1}. L'interaction de l'agent se fait dans un environnement inconnu et la décision se fait via un processus d'essais et d'erreurs.

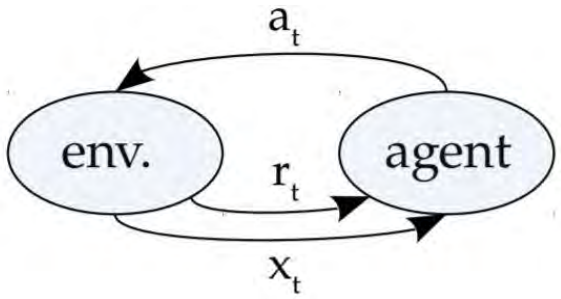

Figure 1 Figure 3.1 : interaction entre l'agent et l'environnement

Contrairement à l'apprentissage supervisé qui apprend à partir de données étiquetées dites ensemble d'entraînement, l'apprentissage par renforcement apprend des données qui sont des

descriptions de situations et associées à un label qui correspond à l'action que devrait prendre le système dans cette situation.

L'apprentissage par renforcement se distingue par deux problématiques principales qui sont la nécessité d'explorer l'environnement afin de découvrir les actions les plus efficaces et l'exploitation des connaissances afin d'obtenir une récompense plus importante.

Nous venons de voir que l'apprentissage automatique repose sur trois grandes familles qui sont, l'apprentissage supervisé, l'apprentissage non supervisé et l'apprentissage par renforcement. Respectivement, l'apprentissage supervisé nécessite des données explicatives à partir desquelles le système va apprendre pour prédire la donnée expliquée ; l'apprentissage non supervisé travaille sur la similarité des données d'apprentissage ; l'apprentissage par renforcement apprend des actions provenant d'expériences afin d'optimiser une récompense quantitative au cours du temps.

Comme nous disposons de données regroupées par catégories, pour la construction de notre modèle de prédiction, nous utiliserons la régression vectorielle de support (SVR) et la régression linéaire, tous deux étant des algorithmes de l'apprentissage supervisé.

→ SVR (Support Vector Regression) : le Modèle SVR est une des catégories des machines à vecteur de support (SVM) qui minimise l'erreur de généralisation afin d'obtenir un rendement généralisé. SVR est basée sur le calcul d'une fonction de régression linéaire dans un espace de caractéristiques de grande dimension où les données d'entrée sont mappées via une fonction non linéaire [66]. Autrement dit, l'algorithme SVR apprend une fonction non linéaire en utilisant l'astuce du noyau, c'est-à-dire qu'elle apprend une fonction linéaire dans l'espace induit par le noyau qui correspond à une fonction non linéaire dans l'espace original.

→ Régression linéaire : c'est un modèle de régression qui cherche à établir une relation linéaire entre une variable, dite expliquée, et une ou plusieurs variables, dites explicatives. Il se base sur la formule des moindres carrées en vue de sélectionner les coefficients optimaux et minimiser (j):

$$\mathrm{j} = \frac{1}{n}\sum_{i=1}^{n}(y_i * x_i\ )^2 \qquad \textbf{(3.1)}$$

3.3 Apprentissage automatique dans le contrôle d'accès

L'apprentissage automatique dans le contrôle d'accès représente un atout indéniable pour la sécurité des systèmes d'information. Il offre des traitements rapides, fiables de données.

L'exposition des applications web sur internet offre des ouvertures d'attaques des systèmes d'informations. Ces attaques se présentent sous diverses formes de menaces qui mettent en péril la sécurité de l'ensemble du système. Pour des besoins de contrôle d'accès, plusieurs solutions faisant appel à l'apprentissage automatique ont été conçues. C'est dans cette dynamique que certains auteurs comme A. Makiou [67] ont travaillé sur la détection d'attaques en utilisant l'approche de l'analyse des comportements malicieux et celle de l'inspection des signatures. Ces travaux ont permis de concevoir des modèles avec l'utilisation des classifieurs basés sur l'apprentissage automatique supervisé. Ces classifieurs utilisent des jeux de données pour apprendre les comportements déviants de chaque classe d'attaques.

D'autres travaux ont mené à la conception d'une une plateforme de génération automatique des données d'entrainement. Ces données générées sont normalisées et catégorisées pour chaque classe d'attaques. Le modèle de génération des données d'apprentissage ainsi développé peut apprendre "de ses erreurs" de façon continue, afin de produire des ensembles de données d'apprentissage de meilleure qualité [67]. La figure 3.2 ci-dessous présente la plateforme permettant l'extraction des logs qui feront l'objet d'analyse.

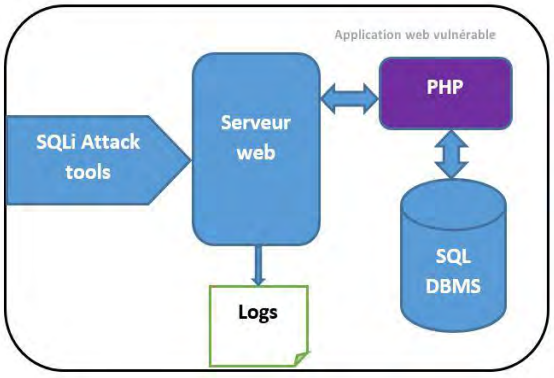

Figure 3.2 : plateforme de création de jeu de données d'apprentissage

Cette plateforme est composée d'un outil d'attaque, d'un serveur Web non protégé et d'une application vulnérable. Les traces des requêtes malicieuses et légitimes sont récupérées à partir du fichier de logs du serveur Web. Le jeu de données d'apprentissage est obtenu après la

normalisation et disséquassions du fichier logs. L'apprentissage automatique, au-delà de la détection d'intrusions dans les applications web, renforce les politiques de contrôle d'accès définies tant en intranet qu'en extranet. Dans la section suivante, nous allons améliorer le contrôle d'accès dynamique, en faisant la classification des critères d'évaluation de la confiance et donc la prédiction des erreurs de confiance.

3.4 Evaluation de la confiance

La relation de confiance exige que l'on tienne compte de l'objet de la relation de confiance, du but ou cible de la confiance et du contenu de la confiance.

3.4.1 Description du contexte

Les systèmes d'enseignements dans les universités virtuelles africaines parmi lesquelles celle du Sénégal, ont montré des limites tant du côté des apprenants que celui des formateurs. Le contexte de notre contribution dans ce chapitre repose sur le cas de l'Université Virtuelle du Sénégal (UVS). A l'UVS, les effectifs pléthoriques des apprenants ne garantissent pas un encadrement de qualité. Ce qui représente la cause majeure des abandons des étudiants souvent observés dans de telles organisations. Le recrutement massif des tuteurs pourrait être une solution d'appoint qui permettrait de limiter l'isolement des apprenants, et par la même occasion de mener un travail collaboratif avec l'enseignant titulaire grâce au modèle de délégation de rôle. Les tuteurs prendraient ainsi le relais en cas d'indisponibilité d'un enseignant titulaire. A cet effet, les apprenants se sentiraient pris à charge par le tuteur en cas d'absence de l'enseignant titulaire.

Vu l'importance du rôle que pourrait jouer un tuteur, il est opportun de faire des recrutements fiables, afin d'assurer un suivi et un encadrement de qualité.

Dans le modèle que nous proposons, l'enseignant représente le sujet de la relation de confiance, car il délègue ses tâches ou son rôle au tuteur dont le niveau de confiance est le plus élevé ; le tuteur représente l'objet de la relation de confiance et le rôle représente le contenu de la relation de confiance. Le niveau de confiance reflète la qualité de la relation de confiance et fait référence à une catégorie quantifiée. Nous représentons le niveau de confiance le plus élevé par la valeur TrustMax et le niveau de confiance seuil est représenté par la valeur TLT. Le seuil de confiance représente le niveau minimum de collaboration de confiance entre le sujet et l'objet. Pour la délégation des rôles ou des tâches, le but de la relation de confiance devra valider le

seuil de confiance et avoir la meilleure valeur du niveau de confiance par rapport aux autres objets qui pourraient être impliqués dans la relation de confiance.

3.4.2 Minimisation de l'erreur de confiance dans le recrutement d'un tuteur

Dans cette section, nous proposons un modèle qui améliore la qualité de recrutement des tuteurs, potentiels délégataires de rôles.

Nous travaillons sur la prédiction de l'erreur de recrutement d'un tuteur. Selon le recueil de l'existant, ce recrutement est basé sur l'évaluation d'un ensemble de critères non pondérés. Les résultats de la prédiction permettent d'effectuer un score, afin de déterminer le tuteur le plus digne de confiance. Ce dernier bénéficiera de la délégation de rôle des enseignants qui seraient indisponibles ou qui voudraient partager un avis pour décider en collégial (une décision collaborative). Les critères utilisés dans ce modèle sont utilisés actuellement pour recruter un tuteur à l'UVS. Nous citons la qualification académique, la qualité de la carrière académique, la production scientifique, la carrière professionnelle, l'ancienneté dans la structure et l'expérience dans l'enseignement à distance. Pour ce travail, nous considérons que cet ensemble de critères ne peut évoluer.

Chaque critère *ci* correspond à une valeur $valc_i$ qui lui est attribuée, avec i, l'index de chaque critère. Nous définissons le niveau de confiance seuil TLT dans l'équation 3.1 :

$$\text{TrustLevel}_{\text{Treshold}} = \text{TLT} = (\sum_{i=1}^{n} valci)/n \quad \textbf{(3.2)}$$

La fonction objectif de la confiance peut être représentée comme le montre l'équation 3.2 :

$$\text{PurptrustLevel}(c_1, c_2, c_3, \ldots, c_n) = \max(\text{valc}_1) + \max(\text{valc}_2) + \max(\text{valc}_3) + \cdots$$

$$+\max(\text{valc}_n),\ n \in N^* \quad \textbf{(3.3)}$$

L'axiome 3.3 : représente la somme des valeurs maximales de chaque critère de confiance.

3.4.3 Evaluation des critères d'appréciation de la confiance

Notre approche consiste à modéliser le processus de sélection des candidats. Le processus de sélection tel que décrit dans l'équation 3.4, est fonction d'un tuple de critères caractérisant un candidat avec un score associé.

$$\text{Sélection}(\{c: \text{c'est le critère du candidat}\}) = \text{score} \quad \textbf{(3.4)}$$

Nous proposons une implémentation de la fonction de sélection, en utilisant un modèle de régression. Ce dernier est obtenu à l'aide de l'algorithme de régression support vecteur (SVR) Basak et al. [66]. SVR est un algorithme de prédiction d'apprentissage automatique supervisé. Il est basé sur une matrice de données $D = (a_{i,j})_{1\leq i\leq m, 1\leq j\leq p+1}$ (où m représente le nombre d'instances, p les critères d'apprentissage et p+1 la colonne des valeurs à prévoir) pour produire un vecteur de p éléments. Chaque élément représente une pondération du critère du même ordre. L'équation 3.5 présente la fonction de régression.

$$y_i = \sum_{j=0}^{p} (w_j * x_j^i) \quad \textbf{(3.5)}$$

Où y^i est la valeur prédite

$x = (1, x_1, x_2, \ldots, x_p)$ représente la valeur explicative

$w = (w_0, w_1, w_2, \ldots, w_p)$ est le vecteur poids avec w_0 représentant une constante

Le Tableau 3.1 présente l'extrait du jeu de données fourni par l'Université virtuelle du Sénégal (UVS) pour la réalisation de l'apprentissage.

Tableau 3.1 : extrait du jeu de données des candidats pour le tutorat

N°	Nom	1.1	1.2	2	3	4.1	4.2	Total points
121	nomcandidat1	0	10	0	5	0	0	15
122	nomcandidat2	10	5	0	0	0	0	15
80	nomcandidat3	0	0	0	5	0	30	35
87	nomcandidat4	10	5	0	10	0	0	25
123	nomcandidat5	10	5	0	0	0	0	15
211	nomcandidat6	0	0	0	5	0	0	5
260	nomcandidat7	0	0	0	0	0	0	0
54	nomcandidat8	0	5	0	5	10	30	50
88	nomcandidat9	10	5	5	5	0	0	25
210	nomcandidat10	0	0	0	5	0	0	5
61	nomcandidat11	0	5	0	5	5	30	45
37	nomcandidat12	10	5	5	5	5	30	60
62	nomcandidat13	0	5	0	5	5	30	45
167	nomcandidat14	0	5	0	5	0	0	10
261	nomcandidat15	0	0	0	0	0	0	0
262	nomcandidat16	0	0	0	0	0	0	0
82	nomcandidat17	0	5	0	10	15	0	30
212	nomcandidat18	0	0	0	5	0	0	5
89	nomcandidat19	10	5	0	10	0	0	25

19	nomcandidat73	0	5	0	5	10	45	0
115	nomcandidat74	0	5	0	10	0	0	30
202	nomcandidat75	0	0	0	5	0	0	0
79	nomcandidat76	20	5	5	5	0	0	30
159	nomcandidat77	0	5	0	5	0	0	30
99	nomcandidat83	10	5	0	5	0	0	30
100	nomcandidat84	0	5	0	10	5	0	0
156	nomcandidat85	0	0	0	10	0	0	30
157	nomcandidat86	0	5	0	5	0	0	0
158	nomcandidat87	0	5	0	5	0	0	0
197	nomcandidat88	0	0	0	5	0	0	30
198	nomcandidat89	0	0	0	5	0	0	0
199	nomcandidat90	0	0	0	5	0	0	0
200	nomcandidat91	0	5	0	0	0	0	0
201	nomcandidat92	0	0	0	5	0	0	0
256	nomcandidat93	0	0	0	0	0	0	0
257	nomcandidat94	0	0	0	0	0	0	0
155	nomcandidat102	0	5	0	5	0	0	0
252	nomcandidat103	0	0	0	0	0	0	0
253	nomcandidat104	0	0	0	0	0	0	0
254	nomcandidat105	0	0	0	0	0	0	0
255	nomcandidat106	0	0	0	0	0	0	0
196	nomcandidat107	0	5	0	0	0	0	0
251	nomcandidat108	0	0	0	0	0	0	0
98	nomcandidat109	0	5	0	5	10	0	0
154	nomcandidat110	0	5	0	5	0	0	0
46	nomcandidat111	0	5	0	10	10	30	0
152	nomcandidat112	0	5	0	5	0	0	0
153	nomcandidat113	0	5	0	0	5	0	0
247	nomcandidat114	0	0	0	0	0	0	0
248	nomcandidat115	0	0	0	0	0	0	0
249	nomcandidat116	0	0	0	0	0	0	0
250	nomcandidat117	0	0	0	0	0	0	0
195	nomcandidat118	0	5	0	0	0	0	0
151	nomcandidat119	0	5	0	5	0	0	0

Les labels 1.1, 1.2, 2, 3, 4.1, 4.2 représentent les valeurs explicatives et correspondent respectivement aux critères suivants : Qualification académique, qualité du parcours académique, production scientifique, parcours professionnel, ancienneté à l'UVS, expérience dans l'enseignement à distance.

La colonne « total points » représente la valeur à prédire (valeur expliquée).

La génération du modèle de prédiction a été réalisée avec l'outil Weka (Waikato Environment for Knowledge Analysis) version 3.8.3.

Cette génération est obtenue par l'une des implémentations SVR appelée SMOReg.

```
------------------------------------------------------------------------------------------------
----------------------
Résultat de l'algorithme SMR :
=== Run information ===

Scheme:       weka.classifiers.functions.SMOreg -C 1.0 -N 0 -I
              "weka.classifiers.functions.supportVector.RegSMOImproved -T 0.001 -V -P 1.0E-12 -L
               0.001 -W 1" -K "weka.classifiers.functions.supportVector.PolyKernel -E 1.0 -C 250007"
Relation:     BASE DE DONNEES TUTEURS UVS-weka.filters.unsupervised.attribute.Remove-R1-8-
              weka.filters.unsupervised.attribute.Remove-R7, 9
Instances:    266
Attributes:   7
              1.1 Qualification académique (NB : minimum requis : Master 2 ou diplôme équivalent)
              1.2 Qualité du parcours académique
              2. Production scientifique
              3. Parcours professionnel (en relation avec les disciplines enseignées)
              4.1 Ancienneté à l'UVS
              4.2 Expérience dans l'enseignement à distance
              Total des points
Test mode:    10-fold cross-validation

=== Classifier model (full training set) ===

SMOreg
weights (not support vectors):
 +       0.1987 * (normalized) 1.1 Qualification académique
 +       0.102 * (normalized) 1.2 Qualité du parcours académique
 +       0.0504 * (normalized) 2. Production scientifique
 +       0.1504   * (normalized) 3. Parcours professionnel
 +       0.4492 * (normalized) 4.1 Ancienneté à l'UVS
 +       0.4501 * (normalized) 4.2 Expérience dans l'enseignement à distance
 -       0.0014
Number of kernel evaluations: 33533 (95.714% cached)
Time taken to build model: 0.12 seconds

=== Cross-validation ===
=== Summary ===

Correlation coefficient                  0.9868
Mean absolute error                      1.8353
Root mean squared error                  4.1552
Relative absolute error                  3.8959 %
Root relative squared error             16.3315 %
Total Number of Instances              264
Ignored Class Unknown Instances                2
 ------------------------------------------------------------------------------------------------
-----------------------
```

Les résultats de cette prévision sont présentés dans le tableau 3.2 ci-dessous.

Tableau 3.2 : Paramètres d'évaluation du niveau de confiance classifiés

Qualification académique	**Qualité du parcours académique**	**Production scientifique**	**Parcours professionnelle**	**Ancienneté à l'UVS**	**Expérience dans l'enseignement à distance**
0.1993	0.1006	0.0499	0.15	0.4492	0.4509

3.5 Algorithme d'évaluation de la confiance

Nous définissons un algorithme (voir algorithme 2) qui permet d'évaluer la confiance du délégataire. Pour ce faire, l'algorithme réalise un score et détermine quel délégataire obtient la plus grande valeur du niveau de confiance. La contribution de cette méthode limite la pratique de la délégation basée sur un sentiment personnel, au profit de la délégation basée sur une appréciation impartiale. Dans le contexte e-learning choisi pour décrire notre modèle, le délégataire est représenté par le tuteur et le cessionnaire est représenté par l'enseignant. La valeur seuil du niveau de confiance ne garantit pas une délégation. Le délégataire doit simplement avoir une valeur de niveau de confiance supérieure à celle de ses pairs au-delà de la valeur seuil. L'algorithme parcourt l'ensemble des tuteurs de la base de données et teste les critères pour chaque tuteur. Il effectue ensuite le cumul des valeurs des critères (catégories) obtenues par un tuteur et le stocke dans le tableau des valeurs affichant le niveau de confiance de chaque tuteur. Le compteur i, ayant permis de parcourir les catégories et les tuteurs, afin d'obtenir les valeurs respectives de niveau de confiance, servira d'index d'identification du tuteur dont la valeur du niveau de confiance vient d'être stockée. Dans les lignes qui suivent, nous ferons une description séquentielle juste après notre algorithme Objectiv_Trust().

Algorithme 2: Objectiv_Trust()

```
For i:=1 to |tutor| do
    Sum_value[i].value:= 0;
    Sum_value[i].tutor:= i;
    For j:= 0 to |cat| do
        if tutor [i] valid cat[j] then
            sum_value[i].value:= sum_value[i].value + cat[j].value;
        endif
    endfor
endfor
For i:= 1 to |sum_value| do
    Max:= sum_value[i].value;
    For j:=i to |sum_value| do
        If sum_value[j].value > max then
            Sum_value[i].value := sum_value[j].value;
            sum_value[j].value = max;
            max := Sum_value[i].value;
        endif
    endfor
endfor
i:=0;
j:=0;
While (i <> number_tutor_position) and (j<|tutor|) do
    If (j=0) OR (sum_value[j-1].value <> sum_value[j].value) then
        If number_tutor_position == |best_candidate_list| then
            i:= number_tutor_position;
        else
            best_candidate_list add tutor[sum_value[j].tutor];
            i++;
        endif
    else
        best_candidate_list add tutor[sum_value[j].tutor];
    endif
    j++;
enddo
return best_candidate_list;
```

3.5.1 Description séquentielle de l'algorithme 2 Objectiv_Trust()

→ Le premier bloc de l'algorithme procède au calcul d'un score pour chaque tuteur. Ce score s'obtient en additionnant la valeur pondérée du critère auquel le tuteur est éligible :

```
For i:=1 to |tutor| do
        sum value[i].value := 0;
        sum value[i].tutor := i;
```

```
        For j:=0 to |cat| do
                if tutor[i] valid cat[j] then
                        sum value[i].value := sum value[i].value + cat[j].value;
                endif
        endfor
endfor
```

→ Le block du milieu procède au tri par ordre décroissant des tuteurs sur la base de leur score :

```
For i:=1 to |sum value| do
        max := sum value[i].value;
        For j:=i to |sum value| do
                if sum value[j].value > max then
                        sum value[i].value := sum value[j].value;
                        sum value[j].value := max;
                        max := sum value[i].value;
                endif
        endfor
endfor
```

→ Le dernier block quant à lui, permet de retourner le nombre de candidats souhaités (variable number_tutor_positions) par ordre de mérite. Le principe est que les ex aequo sont considérés comme un unique candidat mais sont tous ajoutés à la liste des meilleurs candidats, même si le nombre d'ex aequo dépasse le nombre des meilleurs candidats que l'on souhaite afficher :

```
i:= 0;
j:= 0;
while (i <> number tutor positions) and (j < |tutor|) do
        if (j = 0) OR (sum value[j-1].value <> sum value[j].value) then
                if number tutor positions == |best candidate list| then
                        i:= number tutor positions
                        else
                        best_candidate_list add tutor[sum value[j].tutor];
                        i++;
                endif
        else
                best_andidate_list add tutor[sum value[j].tutor];
        endif
j++;
enddo
```

Après l'écriture de l'algorithme de confiance, nous présentons sur la figure 3.5, son équivalence sous forme d'algorigramme.

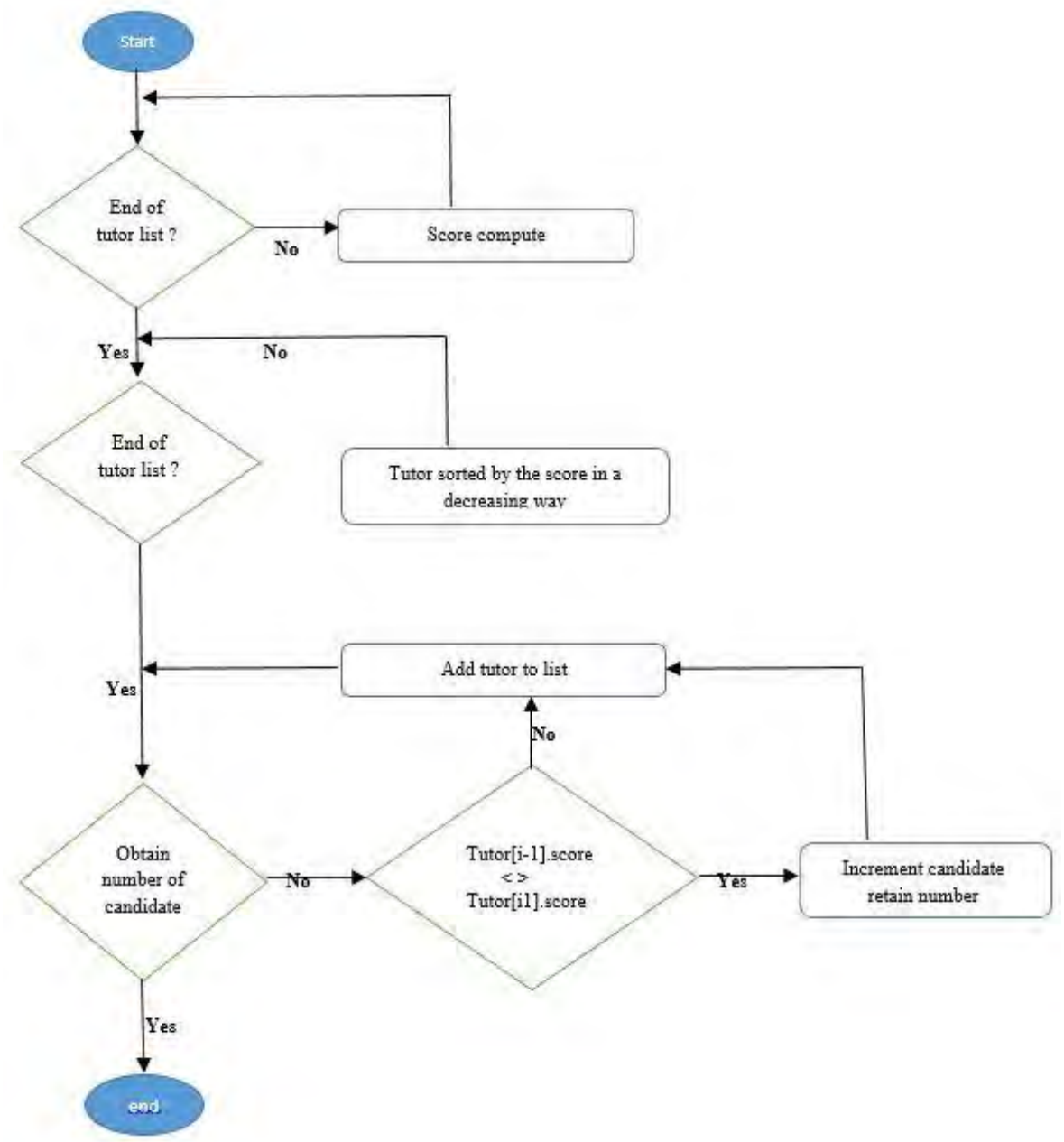

Figure 3.5 : Algorigramme de la confiance objectif

3.6 Suspension et révocation de délégation intégrant les nouveaux critères de confiance

Dans le chapitre 2, nous avons travaillé sur les notions de délégation et de révocation de rôle pour la mise en place du modèle RDBDAC. Dans ce modèle, la question de la confiance a été prise compte.

Seulement, cette dernière a été traitée avec des valeurs booléennes 0 et 1. Pour améliorer le modèle, nous avons procédé à l'évaluation de la confiance. L'objectif de cette section consiste à prendre en compte de nouveaux paramètres de la confiance afin d'améliorer le modèle. Nous introduisons la notion de suspension de délégation. Cette notion permettra une révocation en cascade de la délégation si la valeur du niveau de confiance varie négativement. Nous allons nous référer au contexte décrit dans la section 2.4.1.1 pour la suite de notre travail.

3.6.1 Suspension de délégation

La notion de suspension de délégation consiste à révoquer immédiatement la délégation lorsque les critères qui ont permis de déléguer un rôle ne sont plus vérifiés. Le modèle que nous proposons autorise la suspension de la délégation lorsque, pendant l'exécution de cette dernière, la valeur du niveau de confiance validée précédemment pour le bénéficiaire baisse. Nous pouvons évoquer par exemple le cas où la valeur d'un paramètre ayant permis de calculer le niveau de confiance fait l'objet d'une véracité douteuse. A cet effet, le système suspend en cascade la délégation avant l'expiration du temps imparti. Ci-dessous, nous définissons les axiomes qui permettent respectivement de déléguer des tâches ou des rôles et de suspendre la délégation dans un contexte d'apprentissage et d'évaluation de la confiance.

→ Délégation de tâches :

Tel que mentionné précédemment dans la section 2.4.3, la délégation partielle consiste à déléguer une partie du rôle. Dans l'axiome 2.22, la délégation de tâche exige que la valeur du niveau de confiance(TrustlevelL.Trust) du délégataire (GranteeL.Grantor) soit égale à 1 (c'est-à-dire vrai) pour qu'elle soit effective. Avec la technique d'apprentissage supervisé qui nous a permis d'évaluer la confiance dans la section 3.5, nous redéfinissons la délégation de tâche comme suit :

$$\varepsilon\text{Permission} \sqsubseteq \text{UseL.Licence.Delegation} \sqcap \text{TrustlevelL.Trust} > \text{Threshold\_Trust.Trust} \sqcap \text{GranteeL.Grantor} \sqcap \text{PrivilegeL.Action} \sqcap \text{Target.Object} \sqcap \text{DurationL.Time}^{\varepsilon} \quad \textbf{(3.6)}$$

L'axiome 3.6 vérifie toutes les propriétés de l'axiome 2.22 à savoir la licence de délégation du cessionnaire (UseL.Licence_Delegation), définition du délégataire (GranteeL.Grantor) chargé d'exécuter les tâches déléguées et dispose d'un niveau de confiance(TrustlevelL.Trust) supérieur à la valeur seuil de confiance(Threshold_Trust.Trust), les permissions qui ont été définies pour cette délégation (PrivilègeL.Action et CibleL.Objet). Le prédicat Permission

vérifiera toujours l'exception temps (DurationL.Time$^{\varepsilon}$), qui est la durée au bout de laquelle la délégation prend fin.

→ Délégation de rôle :

La vue de délégation des rôles permet une délégation complète des rôles. Elle est définie par l'axiome suivant :

Empower ⊑ UseRD.Role_Delegation ⊓ Trust_levelRD.Trust > Threshold_Trust.Trust ⊓ AssigneeRD.Grantor ⊓ AssigmentRD.Role ⊓ DurationRD.Time **(3.7)**

→ Suspension de délégation en cas de variation descendante du niveau de confiance:

La suspension de délégation est une forme de révocation anticipée. Elle s'exécute lorsque le niveau de confiance défini pour la délégation (TrustlevelRD.Trust) varie de supérieur à inférieur ou égal au seuil de confiance (Threshold_Trust.Trust). Dans ce cas, la durée prévue pour la délégation ne nécessite pas d'être à son terme (∀DurationEndL.Licence_Delegation. (true ∨ false). L'axiome 3.7 représente une suspension de délégation.

εPermission ⊑ UseL.License_Delegation ⊓ AssigneeL_Assignee ⊓ PermissionD.GD_Revoke ⊓ TrustlevelRD.Trust <=Threshold_Trust.Trust ⊓ (∀DurationEndL.Licence_Delegation.(true ∨ false) **(3.8)**

La propriété PermissionD.GD_Revoke protège le cessionnaire contre toute révocation de son rôle et autorise le système à suspendre la délégation au besoin.

3.6.2 Révocation de délégation

La révocation est le processus de récupération de la licence ou du rôle délégué par le cessionnaire. Nous la représentons dans l'axiome 3.9 suivant:

εPermission ⊑ UseL.License_Delegation ⊓ AssigneeL_Assignee ⊓ PermissionD.GD_Revoke ⊓ TrustlevelRD.Trust >Threshold_Trust.Trust ⊓ DurationEndL.Licence_Delegation=true **(3.9)**

Le processus de révocation n'arrive à son terme que si le niveau de confiance du délégataire (TrustlevelRD.Trust) demeure supérieur au seuil de confiance (Threshold_Trust.Trust) et la durée de délégation arrive à son terme (DurationEndL.Licence_Delegation=true).

3.7 Modélisation de la délégation avec le diagramme de séquence

Le diagramme de séquence de la **figure 3.6** illustre le processus de délégation. Il décrit les étapes à savoir l'attribution des certificats, des rôles, et la révocation de la délégation, en passant par la suspension. Nous décrivons le diagramme de séquence comme suit :

1. Attribution de licence par l'administrateur à l'enseignant.
2. Attribution des rôles par l'administrateur aux utilisateurs.
3. Délégation de licence au cessionnaire.
4. Si trust level=max trust, le cessionnaire délègue une ou plusieurs tâches au tuteur.
5. Le tuteur exécute la tâche Tant que la durée de délégation=vrai et le niveau de confiance = max confiance.
6. Si le niveau de confiance < max confiance et la durée de délégation = vrai alors la délégation de tâche est suspendue.
7. Si le niveau de confiance = confiance maximale et la durée de délégation = faux, la délégation de tâches est révoquée.

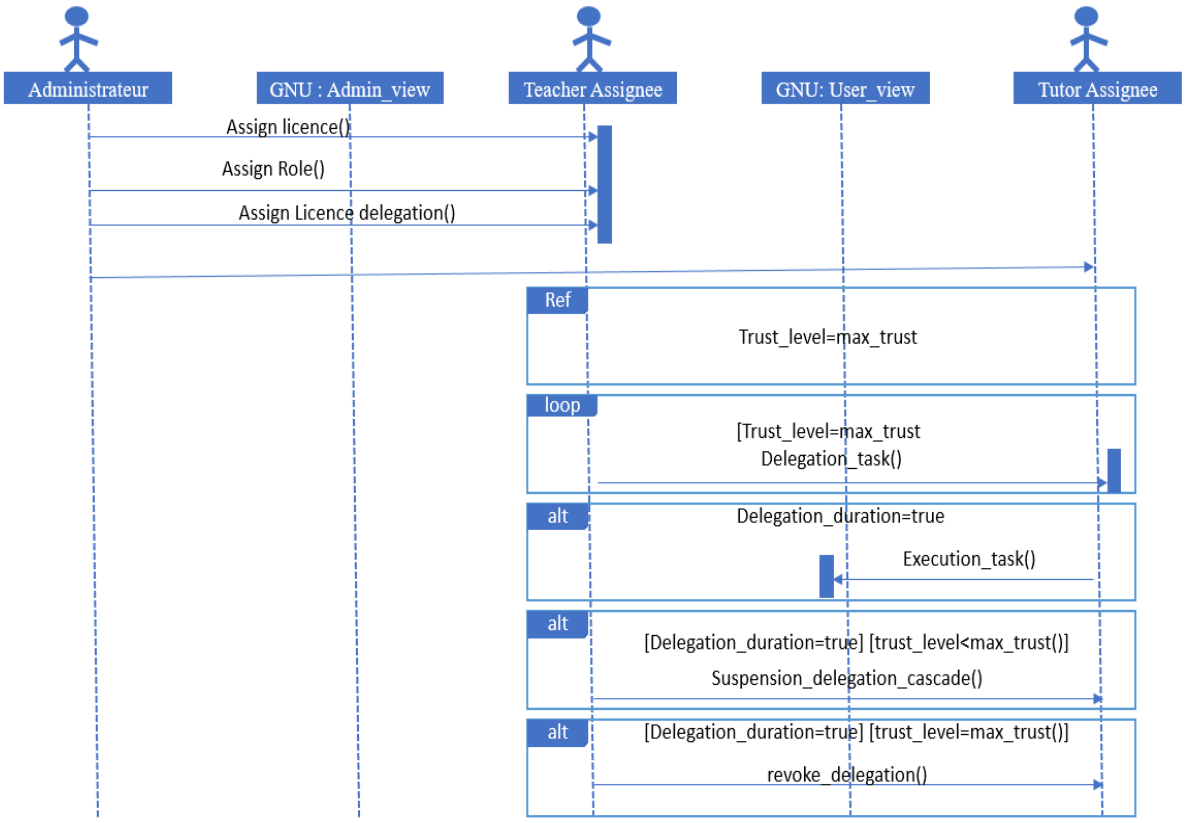

Figure 3.6 : Diagramme de séquence du processus de delegation

3.8 Conclusion

Dans ce chapitre, nous avons proposé une amélioration du modèle de contrôle d'accès RDBDAC qui permet de gérer les délégations dynamiques des rôles, en intégrant les paramètres tels que la confiance et le contexte temporel. Seulement, le modèle RDBDAC n'évalue pas objectivement la confiance car, le niveau de confiance de l'objet de la relation de confiance considère essentiellement deux valeurs booléennes que sont "0" et "1". La contribution dans ce chapitre consiste à évaluer les critères de recrutement d'un tuteur. Cette évaluation se fait à l'aide du modèle des SVR qui a permis de proposer des coefficients minimisant le mieux les erreurs de recrutement. Sur la base des prédictions obtenues, nous avons proposé la fonction objectif qui permet d'évaluer et d'afficher le plus haut niveau de confiance d'un tuteur. Malgré ses résultats exceptionnels, le modèle SVR présente une faible tolérance au bruit, en particulier pour la sélection des vecteurs de support.

Notre modèle va apprendre sur les caractéristiques d'un tuteur, et aider à décider sur une possible délégation de rôle à ce dernier. L'apprentissage automatique vient éliminer le caractère subjectif d'une délégation de rôle. Il a aussi aidé à minimiser les erreurs de confiance dans le processus de délégation de rôle.

La délégation de rôle doit tenir compte des paramètres liés à la protection de la vie privée et aux objets connectés utilisés pour la transmission de l'information lors d'une cession de rôle ou de privilège. Ces deux derniers paramètres n'ayant pas été pris en compte dans la contribution que nous venons de présenter, nous allons dans le chapitre suivant, proposer un modèle de contrôle d'accès basé sur la délégation dynamique de rôle, la préservation de la vie privée et l'internet des objets (IoT), afin d'optimiser la sécurité des données.

CHAPITRE 4

Proposition d'un modèle de contrôle d'accès basé sur la préservation de la vie privée et l'IoT

4 Proposition d'un modèle de contrôle d'accès basé sur la protection de la Vie Privée et l'IoT

4.1 Introduction

Le contrôle d'accès des données personnelles dans les systèmes d'informations reste d'actualité et demeure un enjeu majeur. En effet, les données stockées peuvent entraîner la convoitise d'acteurs malveillants dans le but de générer des profits ou de nuire aux personnes. Dans plusieurs secteurs d'activités tels que les finances, la santé, l'éducation, une menace peut provenir des fournisseurs de services, qui peuvent tirer parti du manque de réglementation pour l'exploitation des données personnelles.

L'utilisation d'objets de plus en plus capables de collecter des données à caractère personnel accroît l'atteinte au respect de la vie privée et par ricochet de la sécurité. Selon Nemri, M. [68], ces objets constituant l'Internet des objets (IdO) et qualifiés de « connectés », « communicants » ou « intelligents », pourraient atteindre le nombre de 50 à 80 milliards dans le monde d'ici 2020. On en dénombre près de 15 milliards aujourd'hui. Ces chiffres peuvent susciter une crainte de détérioration de la protection des données si des politiques de contrôle d'accès adaptées à la complexité de ces nouvelles technologies ne sont pas déployées.

L'IdO favorise le développement de nouvelles plateformes, services et applications qui relient le monde physique au monde virtuel. Définir des politiques de contrôle d'accès pour de telles plateformes reste un défi pour les chercheurs, car le gap de lacunes encore observées en matière de sécurité reste à combler dans plusieurs domaines, surtout celui de la santé.

De nombreux travaux scientifiques ont été effectués sur les systèmes de surveillance à distance des patients et, la plupart d'entre eux ont des limites technologiques dans le contrôle d'accès des informations personnelles et confidentielles des patients. De plus, certains de ces systèmes n'offrent pas le travail collaboratif d'où l'intérêt de la délégation.

L'objectif de ce chapitre est de proposer un modèle de contrôle d'accès basé sur la préservation de la vie privée dans l'environnement de l'IdO. Le modèle proposé prendra le paramètre confiance en compte et permettra de faire des délégations de rôles pour favoriser le travail collaboratif.

Dans la suite de notre travail, nous définirons le concept de l'IdO ainsi que leurs applications. Nous parlerons ensuite de la sécurité de l'internet des objets et présenterons les différents modèles de contrôle d'accès qui y sont définis. Nous terminerons avec la description du modèle de contrôle d'accès que nous proposons.

4.2 Définition de l'Internet des Objets et ses applications

L'internet se transforme progressivement en un HyperRéseau comparable à un réseau formé par des multitudes de connexions entre des Artefacts (physiques, documentaires), des acteurs (biologiques, algorithmiques), des écritures et des concepts (linked data, metadata, ontologies, folksonomie) appelés «Internet des objets (IdO)». Ce réseau pouvant connecter des milliards d'êtres humains et d'objets est considéré par I. Saleh [69] comme l'outil le plus puissant jamais inventé par l'homme pour créer, modifier, et partager les informations.

Lyes TOUATI [70] définit l'IdO comme une technologie qui permettra aux personnes et aux objets du monde physique ainsi qu'aux données et aux environnements virtuels, d'interagir les uns avec les autres afin de créer des environnements intelligents tels que les systèmes de transport intelligents, les villes intelligentes, la santé intelligente, l'énergie intelligente, etc.

L'internet des objets fait appel au monde d'objets, d'appareils et de capteurs qui sont interconnectés. Un objet connecté a une certaine forme d'intelligence, une capacité de recevoir et de transmettre des données via des logiciels (applications IdO) grâce aux capteurs embarqués.

Les applications IdO pourraient contribuer à résoudre certains problèmes auxquels la société d'aujourd'hui est confrontée :

→ la surveillance de la santé à distance pour le suivi de l'autonomie des personnes âgées ;
→ les unités agricoles connectées optimiseraient l'utilisation de l'eau, des engrais et amélioreraient l'agro-industrie ;
→ les véhicules connectés permettraient de contrôler le trafic urbain et de réduire la pollution et les empreintes carbones ;
→ les réseaux intelligents connectés permettront d'optimiser la consommation et la répartition de l'énergie et la maintenance des infrastructures électriques.

Les exemples d'application ci-haut cités illustrent combien l'IdO est susceptible d'améliorer la qualité de vie des usagers. A cet effet, la prise en compte de l'aspect sécurité de l'IdO reste imminente compte tenue de la qualité des informations qui peuvent y être transmises.

4.3 Sécurité de l'internet des objets (IdO)

L'internet des objets soulève des questions pertinentes et offre de nouveaux défis pour la sécurité des systèmes, des processus et de la vie privée des personnes. Certaines applications IdO traitent des informations sensibles sur les personnes, telles que leur localisation, les données sur leur état de santé etc. A cet effet, il devient opportun de traiter la question de confiance dans l'IdO. L'acceptation de ce dernier dépendra de la capacité de la politique de contrôle d'accès définie en son sein, à garantir qu'il est digne de confiance et fiable pour la protection de la vie privée des sujets.

L'internet des objets fait appel au monde d'objets, d'appareils et de capteurs qui sont interconnectés via internet. Un objet connecté doit être adopté à un usage. Il a une certaine forme d'intelligence, une capacité de recevoir, de transmettre des données via des logiciels grâce aux capteurs embarqués. Un objet connecté dispose de trois éléments clés que sont :

→ les données produites ou reçues, stockées ou transmises.
→ les algorithmes pour traiter ces données.
→ l'écosystème dans lequel il va réagir et s'intégrer.

Un objet connecté peut interagir avec le monde physique de façon indépendante sans l'intervention d'un humain. Il possède plusieurs contraintes telles que la mémoire, la bande passante, la consommation d'énergie, etc. Saleh [69].

4.3.1 Vulnérabilités et menaces de l'IdO

Le National Intelligence Council (NIC) des États-Unis, présente l'IdO comme l'une des dix technologies ayant un impact potentiellement profond sur la société [71]. Il prévoit que d'ici l'année 2025, les nœuds de l'IdO se trouveront dans des objets utilisés au quotidien à l'instar des emballages alimentaires, des mobiliers et des documents. Eu égard à cela, les progrès technologiques liés à une forte demande et aux débouchés commerciaux devraient encourager l'adoption et le déploiement de l'IdO à grande échelle. Cependant, l'usage à grande échelle des objets connectés du quotidien pourrait être une menace potentielle pour la sécurité.

L'omniprésence de l'IdO accroîtra assurément le nombre d'attaques contre les données et les réseaux. De plus, la fusion du monde physique et du monde virtuel rendue possible via l'IdO ouvrira la porte à de nouveaux types de menaces qui pèseront directement sur l'intégrité des objets eux-mêmes, des systèmes sous leur contrôle, et sur la vie privée des personnes L. Touati [70].

→ Menaces contre les données et les réseaux

L'absence de protection physique et de surveillance permanente fait des objets communicants dans l'IdO, des cibles faciles pour les attaques matérielles et logicielles. Ces objets peuvent être volés ou corrompus. Sans mesures spéciales de protection, les données qui y sont stockées deviendraient alors accessibles. Les transmissions sans fil peuvent aussi facilement devenir la proie d'attaques d'écoutes clandestines et de déni de service par brouillage W. Xu et al. [72].

→ Menaces contre la vie privée

Les objets du domaine personnel ou privé pourraient être géolocalisés, communiquer avec d'autres objets par le biais de réseaux ad hoc spontanés, écouter ce que dit la personne, filmer la personne et/ou son environnement, enregistrer sa fréquence cardiaque, son rythme respiratoire, sa température voire ses mouvements. Par conséquent, des questions légitimes sur l'avenir de cette immense masse de données personnelles et parfois intimes se posent. Ainsi, toute absence de réglementation stricte sur la protection de la vie privée et de contrôle des objets par les utilisateurs pourrait entrainer le rejet ou l'abandon de l'utilisation de l'IdO. Le rapport de l'UIT sur l'Internet des objets [73] conclut que la protection de la vie privée ne devrait pas se limiter aux solutions technologiques, mais devrait inclure des considérations juridiques, de réglementation du marché et socio-éthiques.

4.3.2 Défis liés à la sécurité et à la protection de la vie privée de l'IdO

La nécessité de développer des systèmes cryptographiques efficaces en termes de ressources (énergie, mémoire, traitement) a déjà été ressentie ces dernières années, avec la prolifération de minuscules réseaux embarqués tels que les réseaux de capteurs, les réseaux d'actionneurs sans fil et les réseaux ad hoc mo-biologiques [70]. L'avènement de l'IdO implique l'interconnexion d'un nombre important d'objets et accentue le problème de la rareté des ressources ainsi que celui de l'évolutivité. Ce qui exige la prise en compte des protocoles

sécurisés pour les réseaux à faible perte de puissance, l'authentification et le contrôle d'accès efficaces.

En ce qui concerne les protocoles sécurisés, l'une des technologies recommandées pour l'interconnexion de l'IdO est IPv6, dont le principal avantage réside dans l'énorme capacité offerte par l'adressage 128 bits. IPv6 répondrait aux besoins d'adressage d'un très grand nombre d'IdO avec potentiellement des dizaines de milliards d'euros.

L'authentification et le contrôle d'accès sont d'une importance vitale pour l'Internet des Objets. Tim Polk et Sean Turner [74] soutiennent qu'en plus des problèmes d'évolutivité, les relations parfois complexes entre objets et utilisateurs rendent difficile la mise en place des politiques de contrôle d'accès. La pluralité des techniques d'identification des utilisateurs et des objets constitue un obstacle pour la mise en place d'un modèle standard d'identification.
Compte tenu de la sensibilité des applications IoT, nous nous y concentrerons pour définir leurs techniques de contrôle d'accès dans la suite du travail.

4.4 Contrôle d'accès dans l'Internet des Objets (IdO)

Un système de contrôle d'accès vise à contrôler qui (sujet) peut faire quoi (opération ou droit) sur quelle ressource (l'objet) Gusmeroli et al. [75]. Il assigne la permission à un utilisateur, l'autorisant à effectuer certaines opérations sur une ressource.

4.4.1 Définition des entités d'un contrôle d'accès dans l'IOT

Etant donné les entités constituées en ensembles S, O et R représentant respectivement :

$S = \{s_i\}$ l'ensemble de tous les sujets du système,

$O = \{o_j\}$ l'ensemble des objets du système,

$R = \{r_k\}$ l'ensemble des opérations ou actions envisagées par le système.

Un système de contrôle d'accès est défini par l'ensemble des règles $\sum_n(s_i, o_j, r_k)$ où $S_i \in S$, $O_j \in O$, $r_k \in r$ pour tout i ; j et k.

La conception d'un système de contrôle d'accès pour un environnement de l'internet des objets requiert certains paramètres fonctionnels à savoir :

→ Délégation de rôle : un sujet peut accorder des droits d'accès à un autre sujet, ainsi que le droit de déléguer tout ou partie des droits accordés.

→ Révocation du droit d'accès : la possibilité de révoquer les droits d'accès précédemment accordés.

→ Granularité : idéalement, le système de contrôle d'accès devrait prévoir une politique de contrôle d'accès en fonction des exigences du niveau d'application.

→ Évolutivité : l'Internet des objets relie des centaines de milliards d'objets qui doivent être pris en compte par le mécanisme de contrôle d'accès.

→ Efficacité temporelle : le mécanisme de contrôle d'accès ne doit pas induire de retards intolérables. Le temps de réponse doit être lié aux attentes en matière de convivialité.

→ Sécurité : le mécanisme de contrôle d'accès doit résister aux différentes attaques possibles dans le scénario IoT, telles que les reprises d'attaques, le déni de service etc.

4.4.2 Solutions de modèles de contrôle d'accès pour l'IdO

Plusieurs modèles de contrôle d'accès pour les environnements IoT ont été proposés. La forme la plus courante de ces systèmes de contrôle d'accès est basée sur des listes de contrôle d'accès (LCA). Ces dernières consistent à attribuer des droits d'accès à des sujets spécifiques. Seulement, les contrôles d'accès basés sur les listes deviennent complexes à gérer lorsque le nombre de sujets et de ressources augmente.

D'autres solutions de contrôle d'accès ont été proposées pour alléger la charge de base des systèmes de contrôle d'accès basé sur les listes. On peut les classer en quatre approches à savoir le contrôle d'accès basé sur les rôles (Role-Based AC), le contrôle d'accès basé sur la confiance (Trust-Based AC), le contrôle d'accès basé sur les certificats (Credential-Based AC) et le contrôle d'accès basé sur le contexte (Contexte-Aware AC). La figure 4.1 montre les quatre approches en question.

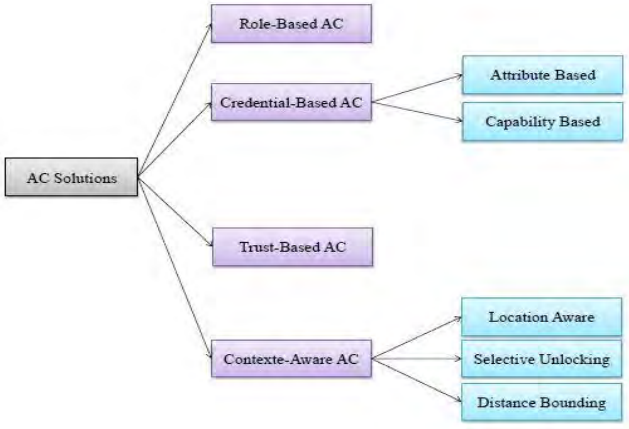

Figure 4.1 : Classification des solutions de contrôle d'accès pour l'IdO

→ Contrôle d'accès basé sur les rôles (RBAC) : J. Liu et al. [49], proposent une approche d'authentification et de contrôle d'accès pour l'IdO. Dans la phase d'authentification, ils ont utilisé un système de cryptage à courbe elliptique avec clé privée éphémère pour établir une clé de session pour un utilisateur et un objet. Pour ce qui est du contrôle d'accès, les auteurs ont adopté le modèle RBAC. L'utilisation de l'approche RBAC entraîne une explosion des rôles lorsque le nombre de ressources et/ou le nombre de domaines administratifs augmente.

→ Contrôle d'accès basé sur les certificats : les solutions dans cette catégorie exigent qu'un utilisateur dispose de certains certificats pour avoir accès à certaines ressources ou données. Cette catégorie dispose de deux sous-catégories à savoir :

- Contrôle d'accès basé sur les attributs : un utilisateur doit posséder certains attributs pour pouvoir accéder à une ressource. Bianchi et al. [76] ont proposé AGREE, un contrôle d'accès pour les réseaux de capteurs sans fil GREEn. Les auteurs Bethencourt et al. [77] réalisent un contrôle d'accès complexe sur des données cryptées appelé Ciphertext Policy Attribute Based Encryption (CP-ABE).
- Contrôle d'accès basé sur les capacités : une capacité (connue dans certains systèmes sous le nom de "clé") est un symbole d'autorité commutable et infalsifiable. Elle fait référence à une valeur qui identifie de façon unique un objet et un ensemble de droits d'accès associés. Le jeton de capacité permet à un processus d'interagir avec un objet d'une certaine manière. IACAC [78], CCAAC [79] et CapBAC [75] sont quelques exemples de solutions basées sur les capacités de contrôle d'accès dans l'IdO.

→ Contrôle d'accès basé sur la confiance : les auteurs Mahalle et al. [80], ont proposé une approche floue de contrôle d'accès basé sur la confiance pour l'Internet des objets. Le niveau de contrôle d'accès d'un appareil à un autre est proportionnel à la confiance qu'il lui accorde. Pour ce modèle, la valeur de confiance est liée à trois composantes que sont l'expérience, les connaissances et la recommandation.

→ Contrôle d'accès contextuel : les solutions susmentionnées sont limitées car elles ne tiennent pas compte du contexte et ne prennent donc pas en charge la définition de politiques d'accès adaptatives.

Les solutions de contrôle d'accès de cette catégorie tiennent compte du contexte pour décider si une entité est autorisée ou non à accéder à une ressource ou à certaines données. Les exemples d'éléments contextuels qui peuvent être pris en compte dans le modèle de contrôle d'accès

contextuel sont : la connaissance de l'emplacement par Di Ma et al. [81], le mouvement par Saxena et Voris [82] et la délimitation de la distance [83].

- Connaissance de l'emplacement : les auteurs dans [81], ont proposé deux approches pour améliorer la sécurité et la protection de la vie privée au moyen de la Radio Frequency Identification (RFID). Ils tiennent compte de l'information contextuelle, de l'emplacement et de la vitesse détectée par l'étiquette RFID, afin de décider de se verrouiller ou se déverrouiller.
- Détection de mouvement : dans ce modèle, une balise ne répondrait que lorsqu'elle est en mouvement [82]. Autrement dit, si l'appareil est immobile, il reste silencieux. Cette approche ne permet pas de discerner si l'appareil est en mouvement en raison d'un geste particulier ou parce que son propriétaire est en mouvement. Par conséquent, le taux de faux déblocage de cette approche est élevé.
- Délimitation de la distance : cette catégorie de solutions a été utilisée pour contrer les attaques par relais. Un protocole limitant la distance est un protocole d'authentification cryptographique challenge-réponse. Par conséquent, il nécessite une ou plusieurs clés partagées entre les balises et les lecteurs comme les autres protocoles cryptographiques. En plus de l'authentification, un protocole de délimitation de la distance permet au vérificateur de mesurer une limite supérieure de sa distance par rapport au prouveur [83]. Les protocoles "sans limite de distance" quant à eux sont complètement inefficaces pour se défendre contre les attaques de relais.

La plupart des systèmes de contrôle d'accès reposent sur un gestionnaire de serveur qui stocke tous les droits d'accès des utilisateurs dans une base de données (ACL, RBAC, AC à capacité, etc.). Lorsqu'un utilisateur demande des données, le serveur vérifie la base de données s'il en a l'autorisation. Si c'est le cas, le gestionnaire de serveur lui accorde l'accès, sinon l'utilisateur est refusé d'accès aux données.
Ces différents modèles de contrôle d'accès constituent un grand atout pour l'IdO où des relations complexes peuvent exister entre les objets intelligents et les utilisateurs.

Dans cette section, nous avons souligné la sensibilité de l'Internet des Objets aux nouvelles menaces relatives à la vie privée des utilisateurs et à la fiabilité des systèmes contrôlés. Nous avons étudié en particulier les solutions de contrôle d'accès et avons montré que le contrôle d'accès est un service primordial pour l'IdO compte tenu de la sensibilité des applications

ciblées et des dommages pouvant résulter des actions sur les objets et de l'accès aux services et/ou données.

L'IdO disposant de modèles de contrôle d'accès permettant de gérer les autorisations, nous proposons dans la section suivante, un modèle de contrôle d'accès basé sur la délégation et l'organisation. Ce modèle a pour éléments centraux la délégation, la confiance, la confidentialité et l'IdO. L'utilisation de l'IdO permettra d'éliminer l'action manuelle lors du stockage des données personnelles des sujets.

4.5 Proposition du modèle DORBAC

4.5.1 Contexte et cas d'utilisation

4.5.1.1 Contexte

Le modèle de contrôle d'accès basé sur la délégation et l'organisation (DORBAC) est une extension du modèle OrBAC. Il permet de gérer les délégations dans une organisation, tout en préservant la vie privée des sujets dont les données sont stockées dans une base de données.

D'une organisation à une autre, la sensibilité des données peut varier. Dans cette contribution, nous décrivons notre modèle dans un environnement e-santé, car la sensibilité des données qui y sont traitées est très élevée et donc, pertinent pour la gestion de la préservation de la vie privée. De plus, ce modèle règle le problème de pénurie de médecins en campagne et favorise l'accès aux soins de santé à distance. Avec le dispositif que nous proposons dans notre architecture, les patients ne seront plus obligés de migrer vers la zone urbaine pour des besoins de soins de santé.

Pour une meilleure gestion de la confidentialité et donc de la préservation de la vie privé, notre contexte e-santé a comme acteurs les médecins, les infirmiers et les patients. Le système intègre des capteurs qui permettront de recueillir l'information concernant la santé du patient. Contrairement au système hospitalier physique dans lequel les infirmiers assistent le médecin traitant et peuvent être en contact avec les données personnelles du patient sans autorisation de ce dernier, notre modèle limite le rôle de l'infirmier à la gestion matérielle des capteurs. Il sera alors responsable de la connexion des capteurs sur les patients. Il pourra néanmoins renseigner les informations basiques liées à l'identité du patient telles que son nom, son prénom, son âge, son adresse, son numéro de téléphone et son email.

Les patients sont géographiquement dispersés et peuvent se rendre au centre de santé le plus proche de la localité en zone rurale pour se faire consulter via les capteurs. Ainsi, les informations du patient recueillies via les capteurs seront stockées directement dans une base de données à laquelle seul le médecin traitant a accès. Le médecin traitant exerce son travail en zone urbaine et est aussi assigné à un poste de santé rural pour lequel il travaille à distance. Ce dernier peut faire une délégation partielle à un ou plusieurs de ses collègues médecins ayant les mêmes attributs que lui, afin de prendre une décision collaborative sur le cas de son patient. Pour accéder aux données personnelles du patient et participer à une décision collaborative, les médecins délégataires doivent avoir l'autorisation de ce dernier. Au cas où le médecin délégataire ne dispose pas de l'autorisation du patient, il n'aura accès qu'à une vue sur les données à interpréter sans en savoir plus sur le patient. Le médecin traitant et le patient peuvent communiquer en temps réel à une heure précise (sur rendez-vous) via l'interface de la plateforme K-2I-E-health proposé par Bilong et al. [85].

4.5.1.2 Description du processus « consultation à distance d'un patient »

Pour qu'il y ait consultation à distance, le patient doit être situé en zone rurale. Le processus se déclenche lorsque le patient se présente au poste de santé pour une consultation.

1. Le patient demande une consultation
2. L'infirmier enregistre les informations basiques concernant l'identité du patient
3. L'infirmier connecte les capteurs sur le patient afin que les données concernant son état de santé puissent être récupérées et stockées dans la base de données via la Rasphberry
4. Le médecin traitant reçoit une alerte et consulte les données stockées.
5. S'il y a besoin de décision collaborative sur la situation du patient, le médecin traitant fait une délégation partielle de rôle à son homologue médecin préalablement disponible, qui n'aura accès qu'à une vue sur les informations stockées du patient et non sur son identité, afin de garder l'anonymat et préserver sa vie privée. Après une analyse collégiale des données stockées du patient, il y a révocation de la délégation.

   Sinon, le médecin traitant fait une prescription médicale qu'il partage avec le patient via la plateforme. Le médecin peut aussi avoir une communication en temps réel avec son patient pour des besoins d'explications et de conseils.

4.5.1.3 Cas d'utilisation du processus Consultation à distance

Dans cette section, nous allons illustrer la description du processus « consultation à distance d'un patient » avec deux principaux diagrammes que sont le diagramme de cas d'utilisation et le diagramme de séquence respectivement sur la figure 4.2 et la figure 4.3.

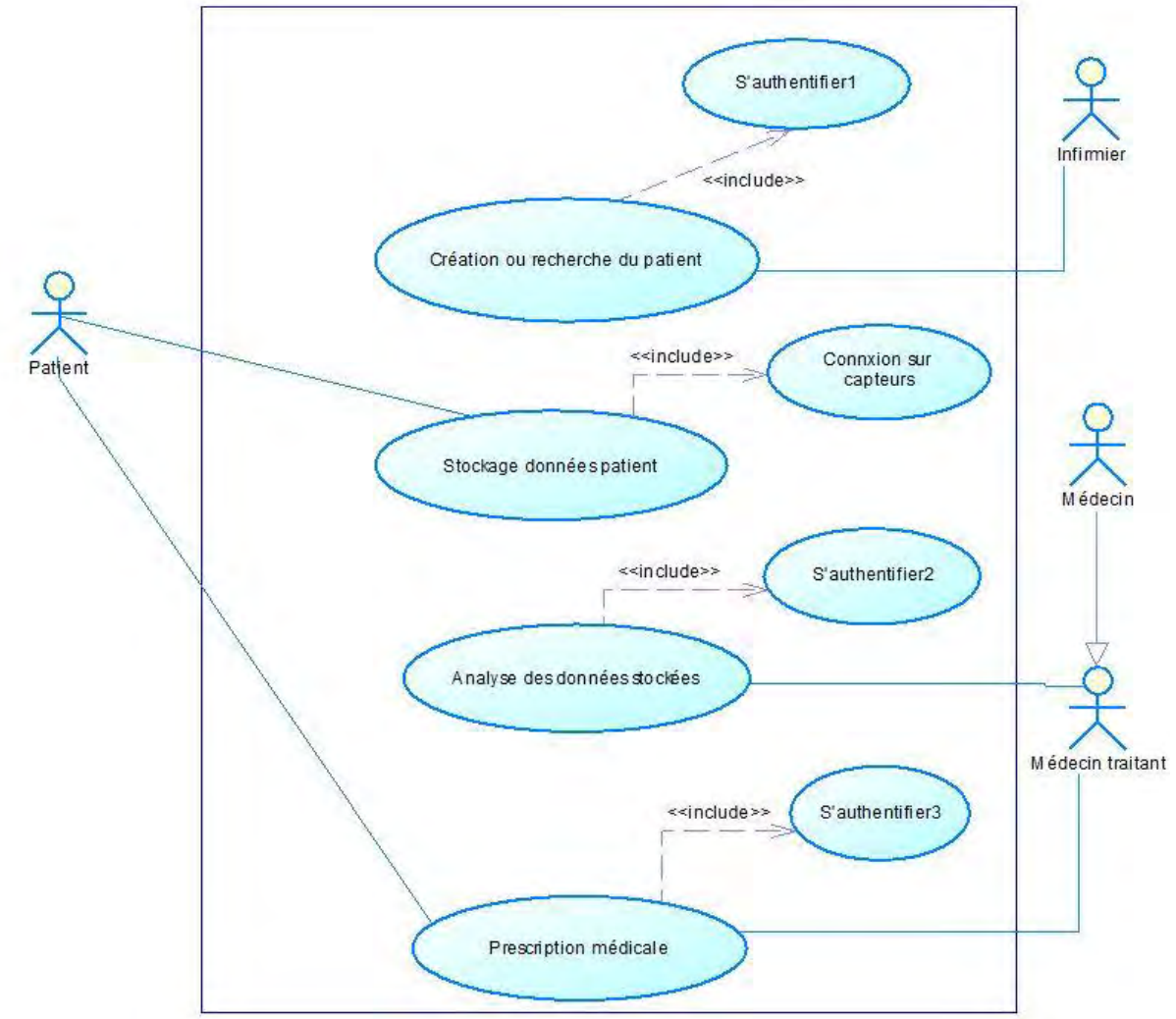

Figure 4.2 : cas d'utilisation consultation à distance

La figure 4.2 présente le cas d'utilisation d'une consultation d'un patient à distance. Le médecin hérite du médecin traitant via le processus de délégation partielle de rôle. Le médecin hérite d'un rôle chaque fois que le médecin traitant le sollicite pour une décision commune sur le cas d'un patient. Les relations « include » indiquent que les cas d'utilisation sources « Création ou recherche de patient », « Analyse des données stockées » et « prescription médicale » contiennent respectivement les cas d'utilisation « S'authentifier1 », « S'authentifier2 » et

« S'authentifier3 ». La relation « include » du cas d'utilisation source « Stockage données patients » a nécessairement besoin du cas d'utilisation « Connexion sur capteurs ». En cas d'échec de d'authentification ou de connexion sur les capteurs, les cas d'utilisation sources ne peuvent être exécutés.

La figure 4.3 montre le diagramme de séquence du scénario nominal « Consultation à distance d'un patient».

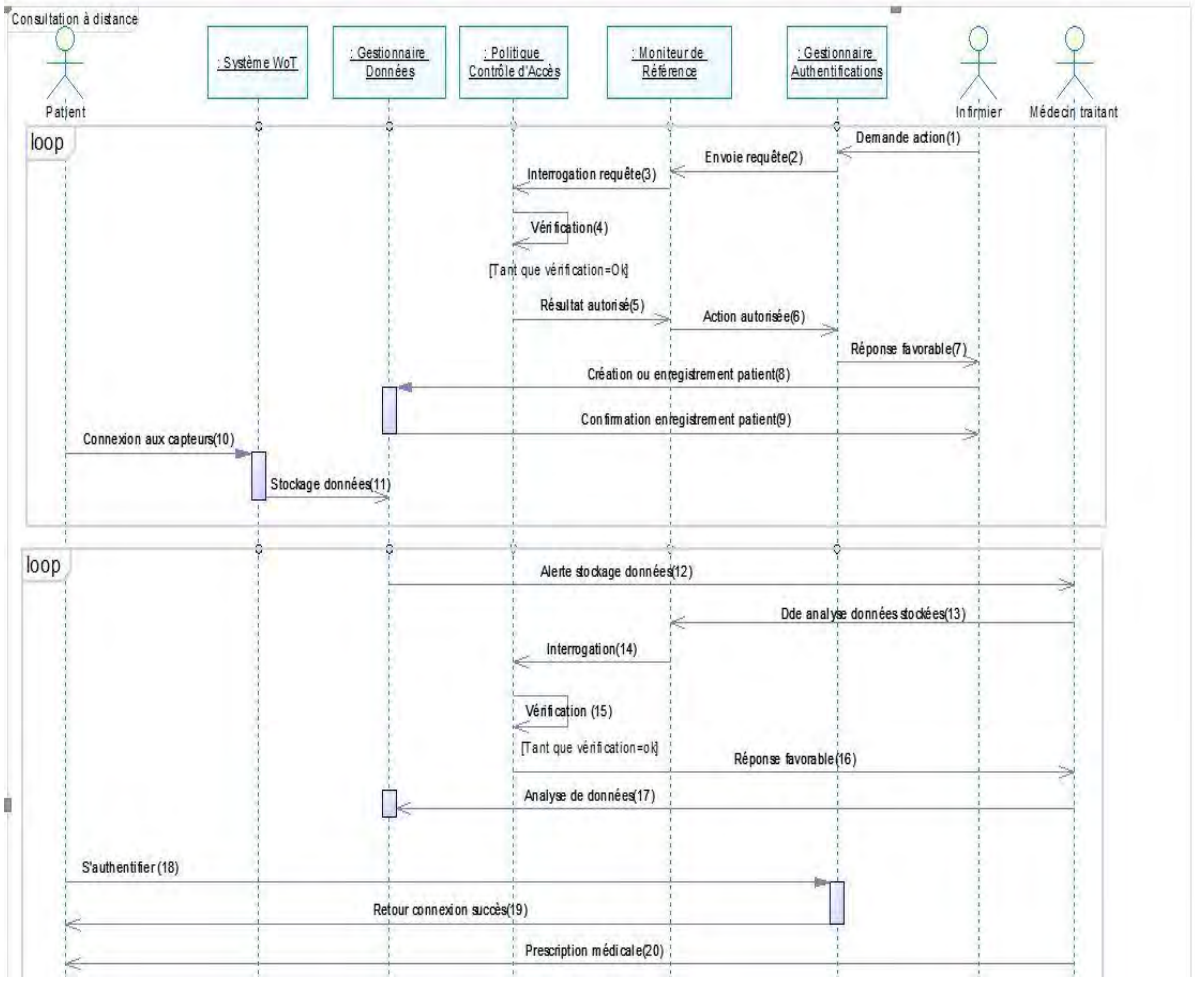

Figure 4.3 : Diagramme de séquence du scénario nominal « consultation à distance »

La figure 4.3 décrit l'ordre chronologique d'exécution du processus d'une consultation d'un patient à distance. Il n'y a pas d'échec pour ce scénario nominal. Tant que le patient se connecte sur les capteurs et que ses données personnelles se stockent dans la base de données, le médecin pourra prendre une décision de prescription sur le patient. Par contre, les phases d'authentification durant le processus doivent être validées avec succès.

4.5.2 Architecture du modèle proposé

La figure 4.4 montre l'architecture du modèle de notre contribution. Elle permet de mettre en place la plateforme K-2I-E-health en utilisant les technologies Node.Js, Kamailio-IMS (IP multimedia subsystem) et KMS (Kurento Media Server). Cette plateforme autorise d'une part une communication multimédia entre deux utilisateurs via l'utilisation de leurs navigateurs ou de leur compte SIP (Session Initiation Protocol) et d'autre part, elle habilite les utilisateurs à accéder aux données des objets connectés prédéfinis.

L'architecture proposée est composée de trois entités distinctes à savoir : Web des objets (WoT), Interface de programmation d'application (API) et application web

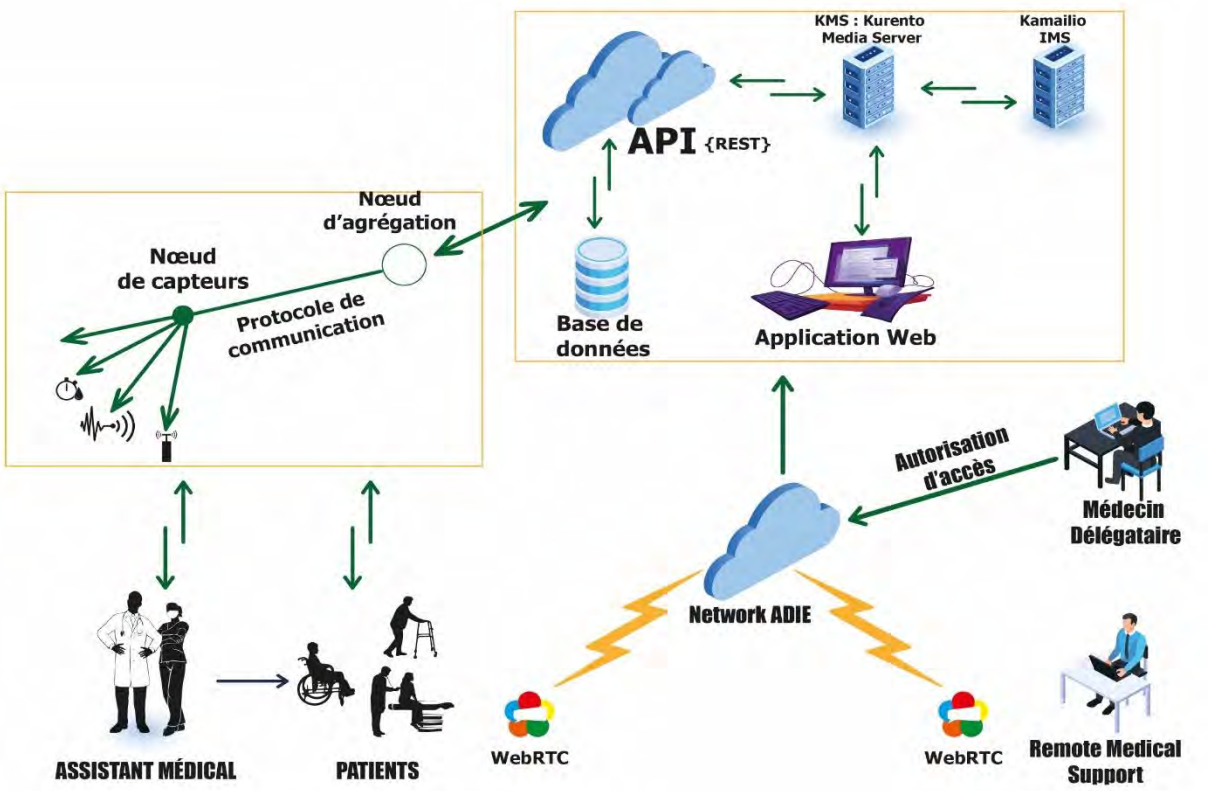

Figure 4.4 : Architecture du modèle DORBAC

4.5.2.1 Description des entités de l'architecture

→ Le web des objets

Le Web des objets désigne l'intégration de tout appareil interrogeable ou contrôlable à distance dans le réseau mondial ou toile (World Wide Web). Il utilise des technologies du web (HTML, JavaScript etc.) pour développer des applications permettant d'intégrer des objets intelligents. Ces objets sont contrôlés par chaque utilisateur qui utilise des mécanismes du web pour interagir avec eux. Le Web des objets regroupe sous forme de réseau de capteurs tous les objets physiques communicants dotés d'une identité numérique unique. Dans ce réseau, nous avons le nœud de capteur et le Nœud d'agrégation NODE MCU ESP8266.

Le nœud de capteur est composé d'un ensemble de capteurs distribués ou localisés. Il est responsable de la collecte d'informations dans les capteurs, de l'exécution des actions des utilisateurs et de l'utilisation des mécanismes de communication pour envoyer les données au nœud d'agrégation.

Le nœud d'agrégation NODE MCU ESP8266 (Raspberry) sert de passerelle entre l'utilisateur et le réseau de capteurs. La passerelle ESP8266 communique avec les capteurs en utilisant un protocole pour la communication (Lora, Zigbee, Bluetooth, WIFI, etc.).

Pour mettre en place notre plateforme, nous avons utilisé un capteur d'humidité et de température DHT11. Ce capteur est connecté à la passerelle NODE MCU (ESP8266) qui se charge d'envoyer les données reçues du capteur via le WIFI (Wireless Fidelity).

→ API

Nous avons développé une API REST capable de récupérer les informations collectées par un dispositif médical connecté et de les stocker dans une base de données MongoDB. MongoDB appartient à la famille NoSQL (document-store, développée en C++). Elle repose sur le concept de couple clé-valeur. Le document est lu ou écrit à l'aide de la clé. MongoDB supporte les requêtes dynamiques faites sur les documents. Comme il s'agit d'une base de données orientée document, les données sont stockées sous la forme de contenu JSON, style BSON Truica et al. [86].

Selon des travaux récents de Cheng et al. [87], les systèmes de bases de données NoSQL contiennent des bases de données non relationnelles conçues pour offrir une grande accessibilité, fiabilité et évolutivité aux données volumineuses. Les bases de données NoSQL peuvent stocker des données non structurées telles que des e-mails et des documents multimédia. MongoDB présente de nombreux risques de sécurité qui peuvent être surpassés par un bon système cryptographique sécurisé Cheng et al.[88]

→ Application web

Pour configurer l'application web, nous utilisons les technologies NodeJs et Kurento Media Server. Cette plateforme permet aux médecins et aux patients de s'enregistrer et de s'authentifier pour accéder aux fonctionnalités de Kurento Media Server. Une fois connecté, le médecin traitant peut visualiser les données du capteur et le flux de données du patient.

4.5.2.2 Description de l'architecture du modèle DORBAC

L'architecture proposée sur la figure 4.4 ci-dessus montre différents acteurs ayant accès aux objets connectés. Les acteurs sont respectivement représentés par le corps médical et les patients. Le corps médical est composé des infirmiers et des médecins. Les infirmiers sont chargés de connecter les capteurs sur les patients. Ils n'ont aucun accès aux informations en rapport avec le dossier médical du patient. Les infirmiers peuvent jouer le rôle de secrétariat pour renseigner sur l'identité du patient dont les informations seront recueillies au niveau des capteurs et stockées directement dans la base de données via la Raspberry. L'architecture proposée permet la mise en œuvre d'un examen clinique à distance. Le médecin traitant peut alors communiquer avec un patient via Kurento Media Server. Il peut traiter les informations du patient recueillies par les capteurs en temps réel, à l'aide de la plateforme K-2I-E-health Bilong et al. [85].

4.5.2.3 Diagramme de communication Médecin – Patient

Les clients (patient et médecin) et le serveur communiquent via un protocole de signalisation basé sur des messages JSON via WebSocket. La figure 4.8 montre la séquence normale entre la logique du client et celle du serveur d'application. Nous décrivons cette séquence comme suit :

→ Le patient, le médecin traitant sont enregistrés sur le serveur d'applications avec les paramètres requis ;
→ L'infirmier émet un appel vers le médecin traitant après avoir rempli les formalités ;
→ Le médecin accepte l'appel entrant ;
→ La communication est établie et le média circule entre le paient et le médecin.

Comme nous pouvons le voir sur la figure 4.5, les candidats SDP (Session Description Protocol) et ICE (Interactive Connectivity Establishment) doivent être échangés entre client (patient et médecin) et serveur, afin d'établir la connexion WebRTC entre le client et le serveur multimédia Kurento. Plus précisément, la négociation SDP connecte WebRtcPeer dans le navigateur avec WebRtcEndpoint sur le serveur.

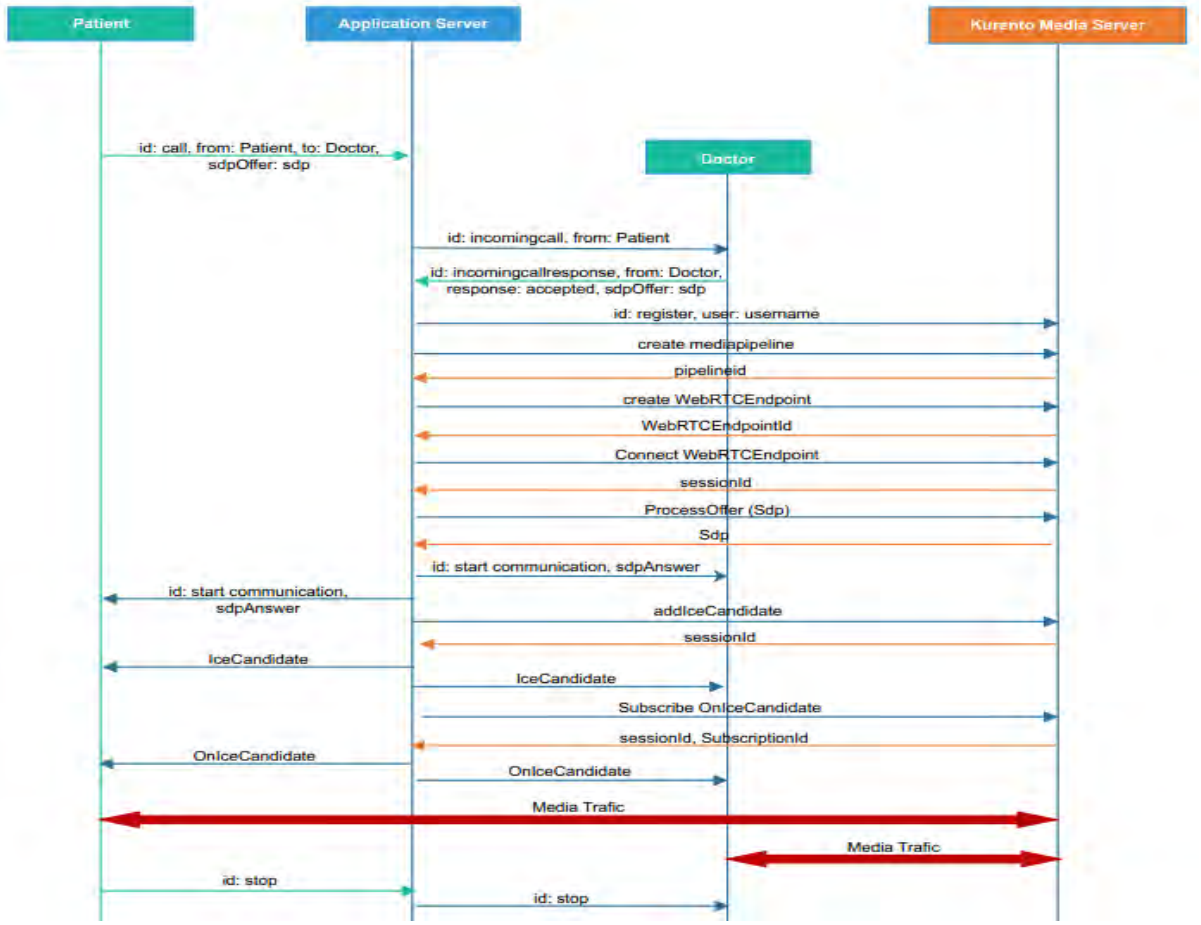

Figure 4.5 : Diagramme de communication entre le patient et le médecin

Pour effectuer un appel, chaque utilisateur (l'appelant et l'appelé) doit être enregistré dans le système. Pour cette raison, il existe une classe nommée UserRegistry qui permet de stocker et de localiser et le patient, et le médecin du côté serveur.

Afin de contrôler les fonctionnalités multimédia fournies par le serveur Kurento, nous avons besoin d'une instance de KurentoClient dans le serveur d'applications. Pour créer cette instance, nous avons spécifié l'emplacement de Kurento Media Server dans la bibliothèque client. Une fois que le client Kurento est instancié, le patient et le médecin sont prêts à communiquer avec Kurento Media Server. Les « Media Pipelines » et les « Media Elements » sont créés et connectés. Dans ce cas de figure, nous avons besoin de deux points WebRtcEnd, à savoir un appelant qui est le patient et un appelé représentant le médecin. Cette logique de média est

implémentée dans la classe CallMediaPipeline. Les points WebRtcEnd doivent être connectés pour chaque direction de support. L'objet est créé dans la fonction incomingCallResponse qui est déclenchée dans son homologue appelé après que l'appelant ait exécuté l'appel de fonction.

A partir de Kurento Media Server 6.0, la négociation WebRTC est réalisée en échangeant des candidats ICE (Interactive Connectivity Establishment) entre les homologues WebRTC. Pour implémenter ce protocole, WebRtcEndpoint reçoit les candidats du client dans la fonction OnIceCandidate. Ces candidats sont stockés dans une file d'attente lorsque le WebRtcEndpoint n'est pas disponible. Ensuite, les candidats sont ajoutés à l'élément multimédia en appelant la méthode addIceCandidate. Une fois que la session est établie, le médecin traitant peut visualiser les données des capteurs et les flux médias du patient sur la plateforme.

4.5.3 Description axiomatique du modèle proposé

Le modèle de contrôle d'accès basé sur la délégation et l'organisation (DORBAC) est une extension du modèle OrBAC. Les éléments centraux de ce modèle sont la délégation et la confidentialité. Nous décrirons nos axiomes en nous référant au contexte décrit dans la section 4.5.1.1. Les principaux acteurs évoqués pour ce modèle sont les médecins, les infirmiers et les patients. Les médecins et les infirmiers sont tous des membres du personnel. Le médecin traitant exerce dans un hôpital en zone urbaine et est parallèlement assigné à un poste de santé en zone rurale dans lequel il exerce à distance grâce au dispositif connecté mis en place. Dans la suite de cette section, nous allons définir axiomatiquement les médecins et les infirmiers. Ensuite, nous ferons une description de leur privilège sur les données et les objets qu'ils manipulent.

L'axiome 4.1 définit le médecin par défaut en tant que membre du personnel comme suit :

$$\text{Doctor} \equiv \text{Staff\_Member} \sqcap \text{Attribute\_Member} \sqcap \text{Licence\_assigment} \sqcap \text{Role\_Assigment} \sqcap \delta\text{Permission} \quad \textbf{(4.1)}$$

Le concept Doctor (médecin) est un membre du personnel (Staff_Member) qui dispose d'attributs(Attribute_Member), d'un rôle(Role_Assigment) qui lui a été attribué et d'une licence (Licence_assigment) qui lui permet de déléguer ses permissions.

L'attribution des rôles peut être considérée comme la première étape du contrôle d'accès. La cession de licence est considérée comme la deuxième étape. Ceci donne le droit à un utilisateur, de déléguer son rôle ou une partie de son rôle à un autre utilisateur qui a les mêmes attributs que lui. L'utilisateur peut aussi déléguer un sous rôle (délégation partielle) à un autre utilisateur

disposant des attributs qui ne donnent accès qu'à l'exécution d'une partie du rôle du cessionnaire. La définition d'un rôle et d'une permission se traduit par les axiomes suivants :

- Role: étant donné U_P l'univers de toutes les permissions, le rôle R est l'ensemble fini de permissions. En d'autres termes,

$$R = \Sigma P_i \,/\, Pi \in U_P \quad \textbf{(4.2)}$$

- Permission: soit U_{OIoT} l'univers de tous les objets de l'Internet des Objets, U_s l'univers des services offerts par les objets connectés et U_{OPS} l'univers de toutes les opérations autorisées d'accès à un sujet, une permission P est représentée par le triplet (O_i, S_i, OPS_i) où $O_i \in U_{OIoT}$, $S_i \in U_s$ and $OPS_i \in U_{OPS}$.

$$P = \Sigma O_i + \Sigma S_i + \Sigma OPS_i \quad \textbf{(4.3)}$$

$$\delta\text{Permission} = \text{ObjectConntedP.permission} \sqcap \text{ServiceP.permission} \sqcap \text{OperationP.permission} \quad \textbf{(4.4)}$$

La définition de l'utilisateur avec le statut de Médecin traitant, lui donne le droit d'accès aux services (ServiceP.permission) de l'environnement des objets connectés. Chaque médecin traitant est assigné à une organisation (Organisation_assigment) et reçoit une licence (Licence_assigment) qui lui permettra de déléguer son rôle (δRole) ou sous-rôle à un autre médecin ayant les mêmes attributs et/ou des attributs supplémentaires. L'axiome 4.5 décrit le concept de médecin traitant comme suit :

$$\text{Medecin\_traitant} \equiv \text{Organisation\_assigment} \sqcap \text{Licence\_assigment} \sqcap \text{Attribute\_Member} \sqcap \delta\text{Role} \sqcap \delta\text{Permission} \quad \textbf{(4.5)}$$

4.5.4 Assignation de licence et de rôle au médecin traitant

L'assignation de licence et de rôle demeure une étape importante dans la définition des politiques de contrôle d'accès. Le processus de délégation passe par l'assignation de la licence et la définition du rôle qui permettra au cessionnaire (Médecin) de déléguer la totalité ou une partie de son rôle. Les axiomes 4.6 et 4.7 décrivent respectivement l'attribution la licence (δLicence_Assigment) et l'assignation de rôle (δRole_Assigment) au médecin. Le médecin contrôle son rôle et la délégation qu'il effectue. Il est le seul à pouvoir faire ou à faire faire (par le système) une révocation.

→ Attribution de licence au médecin traitant

δLicence_Assigment ⊑ OrgL.assigment(Rural_hospital) ⊓ LicenceL.assigment ⊓ AssigneeL.assigment(treating_doctor) ⊓ δPermissionL(O_i, S_i, OPS_i) ⊓ ContextL **(4.6)**

L'axiome 4.6 définit le médecin traitant (AssigneeL.assigment(treating_doctor)) qui est un potentiel cessionnaire affecté dans une organisation en zone rurale (OrgL.assigment (Rural_hospital)). Il lui est assigné la licence (LicenceL.assigment) qui l'autorise à déléguer tout ou une partie de son rôle. Le médecin traitant reçoit des permissions par défaut qui lui donnent accès à l'ensemble des objets connectés liés à l'exercice de son travail (δPermissionL(O_i, S_i, OPS_i)) dans un contexte (ContextL) bien défini.

→ Assignation de rôle au médecin traitant:

δRole_Assigment ⊑ OrgR.Assignee ⊓ AssigneeR.assigment(treating_doctor) ⊓ RoleR.assigment ⊓ δPrivilegesR.Operation ⊓ δPrivilegesR.Service ⊓ δPrivilegesR.ObjectConnected **(4.7)**

Dans l'axiome 4.7, l'assignation de rôle au médecin traitant revient à définir l'organisation(OrgR.Assignee) dans laquelle le médecin traitant devra exercer, définir le médecin (AssigneeR.assigment(treating_doctor)) à qui le rôle sera assigné, assigner le rôle(RoleR.assigment), et donner des permissions (opérations, services et objets connectés) qui permettent de faire un ensemble d'opérations sur des services offerts par les objets connectés pour ce rôle.

4.5.5 Délégation de privilèges et travail collaboratif

En nous référant au contexte décrit dans la section 4.5.1, les médecins traitant ayant les mêmes attributs que leurs pairs peuvent se déléguer leurs rôles ou une partie de leurs rôles à leurs pairs médecins disposant des mêmes attributs. Un médecin peut également déléguer son rôle à un autre médecin ayant plus d'attributs que lui. Les attributs représentent l'ensemble des caractéristiques permettant de déterminer un sujet, un service ou un objet. Afin de préserver la vie privée du patient, la délégation sera partielle si le médecin (délégataire) n'a pas l'autorisation du patient lui permettant d'accéder à son identité et elle sera totale si le délégataire a une autorisation lui permettant d'accéder à toutes les informations concernant le patient. Les axiomes 4.7 et 4.8 définissent respectivement la délégation totale et la délégation partielle de rôles du médecin traitant à son pair.

Empower ⊑ UseRD.Role_Delegation ⊓ AttributeRD.Role_Delegation ⊓ (collaborativ_need)$^{\varepsilon}$ ⊓ patient_permission ⊓ AssigneeRD.Grantor(treating_doctor) ⊓ ServiceRD.Service ⊓ BénéficiaireL.bénéficiaire(doctor) ⊓ OperationRD.Operation ⊓ Object_ConnectedRD.Object ⊓ @(Collaboration_DurationTime)$^{\varepsilon}$ **(4.7)**

L'axiome 4.7 Habilite (Empower) l'utilisation totale des privilèges qu'autorise le rôle (UseRD.Role_Delegation) par le bénéficiaire (BénéficiaireL.bénéficiaire(doctor)) disposant des attributs (AttributeRD.Role_Delegation) définis pour le rôle délégué. La délégation n'est faite que si le cessionnaire sollicite exceptionnellement son collègue médecin pour un besoin de collaboration (collaborativ_need) $^{\varepsilon}$. De plus, le délégataire doit disposer d'une permission du patient (patient_permission) l'autorisant à accéder à ses informations personnelles. Le cessionnaire (AssigneeRD.Grantor(treating_doctor)) autorise le bénéficiaire (docteur) à mener des opérations (OperationRD.Operation) sur des services (ServiceRD.Service) offerts par les objets connectée (Object_ConnectedRD.Object) autorisés par le rôle délégué. La délégation s'effectuera exceptionnellement durant le temps (@(Collaboration_DurationTime)$^{\varepsilon}$) défini pour la collaboration.

Permission ⊑ UseL.Licence_Delegation ⊓ BénéficiaireL.bénéficiaire(doctor) ⊓ OperationRD.Operation ⊓ ServiceRD.Service ⊓ Object_ConnectedRD.Object ⊓ (collaborativ_need)$^{\varepsilon}$ ⊓ @(Collaboration_DurationTime)$^{\varepsilon}$ **(4.8)**

L'axiome 4.8 définit une délégation partielle de rôle encore appelée délégation de sous rôle. La délégation n'a lieu que si le cessionnaire émet exceptionnellement un besoin de décision collaborative (collaborativ_need)$^{\varepsilon}$. Ainsi, la licence de délégation (UseL.Licence_Delegation), permettra au bénéficiaire (BénéficiaireL.bénéficiaire(doctor)) d'accéder à une permission l'autorisant à mener des opérations sur les services offerts par les objets connectés (OperationRD.Operation, ServiceRD.Service, Object_ConnectedRD.Object). Le délégataire n'aura de vue que sur les informations stockées du patient et non sur les informations concernant l'identité de ce dernier.

4.5.6 Révocation de privilège octroyé au médecin délégataire

La révocation de délégation des rôles précédemment faite au docteur par le médecin traitant peut être représentée comme suit :

δPermission $\sqsubseteq$ UseL.License_Delegation $\sqcap$ AssigneeL_Assignee $\sqcap$ AttributeRD.Role_Delegation $\sqcap$ DurationCollaborationEndL.Licence_Delegation $\sqcap$ PermisionD.GD_Revoke **(4.9)**

Dans l'axiome 4.9, la révocation est essentiellement faite par le cessionnaire à cause du type de permission Grant Dependent (PermisionD.GD_Revoke) et a lieu lorsque le temps prévu pour la collaboration arrive à son terme (DurationCollaborationEndL.Licence_Delegation). Le délégataire perd la permission (PermisionD.GD_Revoke) qui lui permettait de mener des opérations sur les services des objets connectés définis pour le rôle au moment de la délégation.

La délégation et la révocation de rôle sont faites autour d'un ensemble d'objectifs composés d'un sujet, d'un objet connecté, d'un service, d'une opération. L'axiome 4.10 décrit la fonction d'affectation d'objectif (Purp_assign) comme suit :

Purp_assign (Subject.ATTR, O_{IOT}.ATTR, Ops.ATTR, service.ATTR) = purp_attr (subject.ATTR) $\subseteq$purp_attr (service.ATTR) $\subseteq$ purp_attr (O_{IOT}.ATTR) $\subseteq$ purp_attr (service.ATTR) $\in$ {0, 1} **(4.10)**

Purp_attr est une fonction qui retourne l'attribut de l'ensemble des objectifs d'un sujet, d'un objet connecté, d'un service ou d'une opération.

4.6 Conclusion

Dans ce chapitre, nous avons proposé le modèle DORBAC qui est une extension du modèle OrBAC. Il permet de prendre en compte la délégation des rôles tout en assurant la protection de la vie privée du patient. Le modèle proposé ne permet de délégation qu'entre des médecins disposant des mêmes attributs. Le modèle implémenté ne permet pas la saisie des informations des patients par un agent de santé (infirmier, assistant etc.). Ainsi, une fois que le patient sollicite une consultation, l'agent de santé enregistre le patient ou met ses informations personnelles en rapport avec son identité à jour. Le patient est ensuite connecté aux capteurs qui vont récupérer les données et les acheminer via le nœud de capteur pour le stockage. Ces données seront ensuite analysées par le réseau de capteurs à l'aide de la passerelle ESP8266 (Raspberry). Cette expérience limite considérablement le risque d'erreurs de saisie et préserve

la confidentialité du patient. Le patient ou le médecin disposant des privilèges peut visualiser les données enregistrées via l'interface de l'application K-2I-E-health. Le médecin peut suivre le patient et prendre une décision sur la base des informations reçues des capteurs. Une séance de vidéoconférence est alors possible entre le patient et le médecin.

La suite de notre travail s'articulera autour de l'implémentation de nos modèles dans des organisations virtuelles du domaine de l'éducation et de la santé.

CHAPITRE 5

Implémentation des modèles proposés

5 Implémentation des modèles proposés

5.1 Introduction

Le développement rapide des technologies d'interconnexion des réseaux informatiques a favorisé le partage des ressources entre plusieurs institutions virtuelles. Depuis ces dernières années, les organisations virtuelles (OV) constituent une problématique de recherche pour laquelle les universités et opérateurs accordent une attention particulière.

Haidar et al. [89] définissent une organisation virtuelle comme un mélange de plusieurs types d'organisations, notamment les établissements universitaires, gouvernementaux, industriels, commerciaux etc. Selon les auteurs, Gueye et al. [90], une organisation virtuelle est un regroupement d'organisations membres dispersées géographiquement et communiquant en réseau via les TIC pour répondre à des besoins spécifiques du marché. L'organisation virtuelle favorise la complémentarité des compétences du fait de sa pluridisciplinarité. Son caractère dynamique s'explique par le fait que durant son cycle de vie, des acteurs peuvent s'ajouter ou se retirer du réseau collaboratif. A cet effet, il devient nécessaire d'assurer la sécurité des données d'un tel réseau.

Moore et al. [91], [89], ont travaillé sur la sécurité des systèmes réseaux maillés (Grid Computing) en utilisant la solution Globus Toolkit. Cette dernière propose un ensemble d'outils permettant de faciliter le développement d'applications utilisant des techniques de grilles. Les auteurs implémentent une couche logicielle supplémentaire qui fait abstraction de l'hétérogénéité de l'environnement. [90].

Dans ce chapitre, nous définirons l'organisation virtuelle en rapport avec les domaines d'e-learning et d'e-santé. Puis, nous y implémenterons les modèles de contrôle d'accès de nos différentes contributions décrites dans les chapitres 2, 3 et 4. Mais avant, nous ferons d'abord une description des outils et des technologies constituant les intrants de l'implémentation. Dans la description desdits outils, nous ferons une contribution portant sur le test de performance de la technologie WebRTC [92], afin de justifier du choix de cette dernière, et par la même occasion de garantir la performance et la fiabilité des plateformes à implémenter.

5.2 Organisation virtuelle dans l'enseignement à distance

L'enseignement à distance s'adresse principalement aux apprenants qui ne peuvent pas ou ne veulent pas utiliser l'enseignement en présentiel [93].

Tout comme en présentiel, la formation à distance est régie par des normes technopédagogiques. La fracture numérique, l'absence physique et l'indisponibilité des enseignants constituent des facteurs bloquants de l'apprentissage pouvant conduire les apprenants à l'abandon. Ce qui pourrait biaiser les résultats escomptés en terme de taux de réussite des apprenants. Il devient alors opportun de proposer des solutions permettant d'éradiquer les décrochages (abandons). La mise en place d'une politique de contrôle d'accès basée sur la délégation de rôle et la confiance pourrait être un début de solution. Ainsi, en cas d'indisponibilité d'un enseignant, ce dernier pourrait déléguer ses privilèges ou rôles à un tuteur digne de confiance.

Dans cette section, nous nous intéresserons particulièrement aux techniques d'apprentissage en rapport avec la conception des environnements orientés vers les encadrements et la disponibilité des principaux acteurs pédagogiques en l'occurrence les enseignants et les tuteurs.

5.2.1 Terminologie de l'enseignement à distance

Les termes utilisés dans l'enseignement à distance par différentes communautés peuvent prêter à confusion. Nous pouvons citer entre autres la formation à distance (FAD), la formation ouverte à distance (FOAD), l'université virtuelle (UV). Nous allons définir ces termes dans la suite du travail afin de comprendre et cerner le contexte d'application de nos modèles.

5.2.1.1 Formation à distance

D'après les travaux de B. Holmerg [93], la formation à distance se caractérise par le fait que l'apprenant est géographiquement séparé de son groupe de pairs et du formateur. C'est pourquoi, pour assurer une communication bidirectionnelle entre les acteurs, la formation à distance s'appuie sur les moyens basés sur les télécommunications.

Selon M'hammed Drissi et al. [94], « la formation à distance est l'ensemble des dispositifs et de modèles d'organisation qui ont pour but de fournir un enseignement ou un apprentissage à

des individus qui sont distants de l'organisme prestataire de service. ». Il a résumé la FAD en cinq critères à savoir l'accessibilité, la contextualisation, la flexibilité (temps et espace), la diversification des interactions (notion groupe), la désaffectivation (sort l'apprenant de son isolement sociocognitif et socio-affectif) du savoir.

5.2.1.2 Formation ouverte à distance

La formation ouverte à distance se caractérise par un dispositif de formation fondé sur une prise en compte des besoins des apprenants, articulant les contenus de formation à des services variés tels le tutorat, les forums, les simulations, et libérant ainsi les contraintes de lieu et de temps. Elle peut être faite partiellement ou intégralement à distance.

L'UNESCO caractérise les formations ouvertes par "une liberté d'accès aux ressources pédagogiques mises à disposition de l'apprenant, sans aucune restriction, à savoir : absence de conditions d'admission, itinéraire et rythme de formation choisis par l'apprenant selon sa disponibilité et la conclusion d'un contrat entre l'apprenant et l'institution".

La formation ouverte à distance fait partie de la famille de la FAD mais se positionne sur l'intégration des technologies de l'information et de la communication, de l'adaptation à l'individu et de la modularité de la formation [94].

5.2.1.3 Université virtuelle (UV)

La notion d'Université Virtuelle (UV) est perçue différemment suivant divers contextes. Dans la littérature, une université virtuelle est définie comme une forme particulière de formation à distance qui repose essentiellement sur les technologies du numérique et en particulier sur des techniques liées à la virtualisation et à l'Internet [95].

Selon une étude réalisée par l'UNESCO en 2006, il existe plusieurs approches d'université virtuelle, chaque approche dépend du contexte géographique, social et économique.

La mission d'une université virtuelle ne diffère pas de celle d'une université traditionnelle. Elle offre également un grand choix de programmes de formation, de cours ou des modules assurant à un étudiant des crédits et le menant vers un diplôme attestant de sa spécialisation dans une discipline donnée [96].

Une université virtuelle est une dématérialisation d'une université traditionnelle. Elle se distingue de celle-ci par le fait que les acteurs qui participent à une activité d'apprentissage sont éloignés géographiquement [90].

De notre point de vue, au-delà de la dématérialisation de l'université traditionnelle, l'université virtuelle permet aux différents acteurs d'accéder à l'outil pédagogique à distance dans le but de partager le savoir sans contrainte ni de lieu ni de temps. Cela résout les problèmes liés aux effectifs pléthoriques dans les universités traditionnelles particulièrement en Afrique. La massification des effectifs dans les universités traditionnelles entraine une augmentation des œuvres universitaires.

Dans un contexte où les moyens sont limités, les États africains gagneraient à réduire la prise en charge du service social et l'hébergement des étudiants [1].

5.2.2 Modèles technopédagogiques dans l'enseignement à distance

Un modèle technopédagogique regroupe un ensemble d'outils technologiques mis en place pour faciliter l'enseignement et l'apprentissage. Nous assistons aujourd'hui à une multiplication des modèles technopédagogiques, avec l'accroissement rapide des réseaux de télécommunications haut débit. Ces modèles sont regroupés en six principaux paradigmes parmi lesquels nous citons les deux modèles les plus usités[1] :

→ modèle de classe enrichie : les technologies sont utilisées dans une classe conventionnelle à des fins de présentation et de démonstration. Dans ce modèle, la classe donne accès à des ressources disponibles en réseau. Par exemple, un enseignant peut donner un cours à distance en visioconférence.

→ modèle de classe virtuelle : c'est un environnement d'apprentissage où le système de communication est basé sur un ordinateur. Elle peut utiliser la visioconférence pour supporter les interventions des apprenants ou des personnes ressources distantes. Plusieurs campus universitaires utilisent ce modèle.

5.2.3 Rôle du tutorat dans l'apprentissage

D'un point de vue strictement pédagogique, la recherche a montré l'importance de l'encadrement et du tutorat dans un système de formation à distance : plus le sentiment

d'éloignement et d'isolement est grand plus l'apprenant a besoin d'être soutenu et entouré. La formation à distance prend donc progressivement conscience de l'importance de la coprésence des acteurs de la formation mais en même temps de la nécessité de plus de flexibilité, de décentralisation, de liberté de points de vue tant organisationnel que pédagogique [97].

5.3 Organisation virtuelle liée à la santé

L'hôpital virtuel renvoie à l'hôpital intelligent qui désigne un milieu de travail très interactif dans lequel le personnel de l'hôpital peut accéder à des renseignements médicaux pertinents à travers une variété hétérogène de dispositifs et collaborer avec des collègues, en tenant compte des informations contextuelles. Ce type d'environnement peut également adapter l'information en fonction du contexte (tel que le rôle spécifique, l'emplacement ou l'état), et même de soutenir le périphérique de suivi des patients. Des concepts autour de l'hôpital virtuel ont été développés. Nous citons entre autres la santé numérique (E-santé) et la télésanté (télémédecine et santé mobile).

→ E-santé : elle se définit selon l'Organisation mondiale de la santé (OMS), comme « les services du numérique au service du bien-être de la personne » c'est-à-dire comme l'application des technologies de l'information et de la communication au domaine de la santé et du bien-être [84]. Les équivalents de la e-santé sont la télésanté, la santé numérique, la santé connectée.

→ Télésanté : elle concerne l'utilisation des systèmes de communication pour protéger, promouvoir la santé et regroupe notamment la télémédecine et la m-santé[84].

- Télémédecine :

La télémédecine est une activité professionnelle qui met en œuvre des moyens de télécommunications numériques permettant à des médecins et à d'autres membres du corps médical de réaliser à distance des actes médicaux. Elle se détermine par des actes à savoir la téléconsultation, la télé-expertise, la télésurveillance, téléassistance médicale etc. [84].

- M-santé (Mobile-santé) ou Santé mobile

Il s'agit de la santé disponible en permanence via un appareil mobile connecté à un réseau. Les appareils les plus utilisés pour la santé mobile sont les smartphones (téléphone intelligent disposant d'un système d'exploitation androïde, iOS ou Windows…) et les tablettes.

Selon S. Tachakra et al [98], l'une des utilisations les plus importantes de la télémédecine est le programme spatial qui repose sur les télécommunications pour la gestion des opérations médicales de routine. Ce programme a été conçu pour recueillir des données audio et vidéo médicales du patient dans l'espace.

5.4 Relation de confiance dans l'organisation virtuelle

La problématique de la relation de confiance est d'un intérêt considérable en ce que la mise en œuvre d'une organisation virtuelle nécessite l'implémentation des techniques de sécurité en son sein à travers des modèles de contrôle d'accès.
Le problème qui se pose est que chaque domaine de sécurité est géré par sa propre autorité administrative. De plus, chaque organisation définit ses propres politiques de sécurité. Dans la littérature, Benzekri [99] décrit plusieurs plateformes telles que XACML (eXtensible Acces Control Markup Language), SAML (Security Assertion Markup Language), Permis et Shibboleth afin d'apporter une réponse à la problématique de la relation de confiance.

Les sections 5.3 et 5.4 nous ont permis de décrire et de cerner les enjeux dans les organisations virtuelles liées aux domaines de l'éducation et de la santé. Le problème de confiance demeure tant au niveau organisation qu'au niveau matériel. Dans la suite du travail, nous allons décrire les outils utilisés pour implémenter les modèles que nous avons proposés.

5.5 Outils de mise en place des systèmes implémentés

5.5.1 WebRTC

La technologie WebRTC est un projet open source présenté par Google en 2011 [100]. Elle assure la communication en temps réel via une API JavaScript et s'appuie sur WebSocket pour établir une connexion entre le client et le serveur.

Selon Loreto [101], le WebRTC fournit des applications RTC de haute qualité telles que la téléconférence, l'audio, la vidéo et l'échange de données en mode paire à paire. La figure 5.1 ci-dessous met en évidence deux composants que sont l'API pour les développeurs web et l'API pour les concepteurs de navigateurs.

→ API pour les développeurs web : c'est une couche contenant un ensemble d'APIs JavaScript nécessaires aux réalisations des services RTC (Real Time Communication) tels que MediaStream, PeerConnection et DataChannel.

→ API pour les concepteurs de navigateurs : intègre le WebRTC et offre des solutions permettant d'annuler les échos, de réduire le bruit environnant, de gérer les codecs vidéo VP8 et les codecs audio iSAC (Internet Speech Audio Codec) et iLBC (Internet Low Bitrate Codec). Cette couche offre un algorithme permettant d'annuler les effets aléatoires du réseau pour la mise en cache des données.

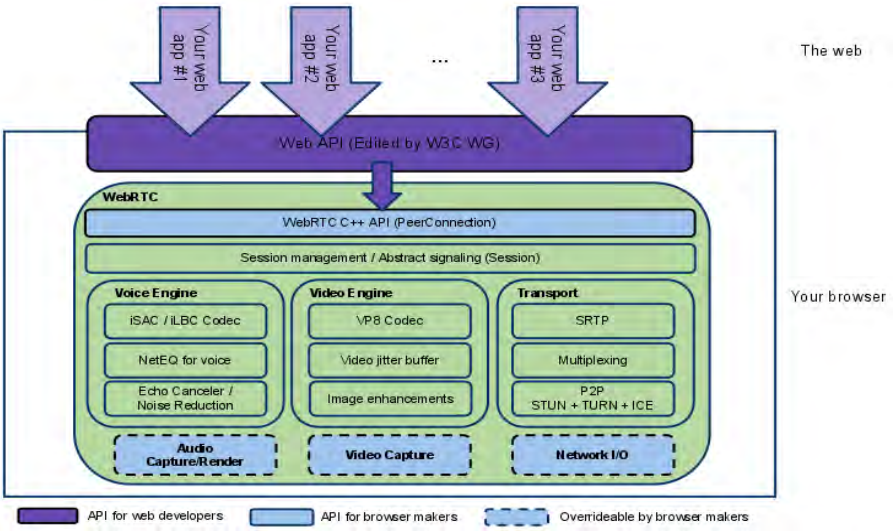

Figure 5.1 : architecture générale de la technologie WebRTC

La technologie WebRTC offre un mode d'échange synchrone entre entités web. Son architecture présente l'avantage de réduire significativement la latence en s'efforçant d'établir des communications directes entre clients en "peer-to-peer" [102].

5.5.1.1 Les composants de la technologie WebRTC

Les groupes de travail W3C (World Wide Web Consortium) et IETF (Internet Engineering Task Force) ont défini trois principaux composants du WebRTC API qui sont PeerConnection, MediaStream et DataChannel [103].

→ PeerConnection : c'est un API qui permet de maintenir un lien de communication direct entre deux paires via les navigateurs web basés sur le protocole UDP (User Datagram Protocol) [101]. Le PeerConnection est sollicité lorsque le lien de communication est établi. Son contenu peut être renégocié selon les besoins en ajoutant ou en modifiant l'API MediaStreams ou des canaux de données. Il a pour objectif de détruire

l'objet MediaStream en cours d'utilisation et ensuite de réinitialiser une requête d'offre qui n'aboutira pas dans le cas où il n'y a plus de flux de données disponibles [104].

→ MediaStream : c'est un API décrivant les flux multimédia (audio ou vidéo). Il permet de prendre des actions en charge sur les flux média tels que l'affichage, l'enregistrement et l'envoi à un pair [105]. L'API MediaStream peut être constitué de plusieurs objets MediaStreamTrack, représentant différentes pistes audio ou vidéos. L'acquisition des flux audio et vidéo par l'API MediaStream passe par l'autorisation de l'utilisateur à l'accès aux ressources telles que la caméra, les haut-parleurs et le microphone. L'utilisateur spécifie le type de média (audio ou vidéo) auquel il souhaite accéder et le navigateur autorise ou refuse l'accès à la ressource demandée. Une fois que le média n'est plus utilisé, l'application peut révoquer son propre accès avec la méthode *stop ()* sur le flux média local [104].

→ DataChannel : il s'agit d'un API offrant un moyen d'échanges de données génériques, bidirectionnelles pair à pair. Cette composante de la technologie WebRTC permet l'échange de données telles que des images ou du texte [105].

5.5.1.2 Test de performance d'une plateforme intégrant la technologie WebRTC

Dans cette section, nous allons faire des tests de montée en charge pour le scénario "authentification", afin d'évaluer la performance de la technologie WebRTC et par la même occasion justifier son choix dans le cadre de nos travaux. Pour cela, nous avons installé l'application à tester sur un serveur doté d'un processeur disposant d'une RAM de 4 MHz. Nous avons aussi installé Apache Jmeter dédié aux tests de montée en charge. Dans la suite de cette section, nous allons d'abord décrire la plateforme à tester ainsi que l'environnement de test Jmeter. Puis, nous ferons les tests à proprement parler.

5.5.1.3 Description de l'environnement de test

L'application de test est une plateforme e-learning qui intègre la technologie WebRTC. Pour sa mise en place, les auteurs S. Ouya et al. [103] ont utilisé la bibliothèque EasyRTC qui dépend principalement du serveur de signalisation mis en place à partir des modules suivants HTTPS (HyperText Transfer Protocol Secure), Websocket et MySQL.

→ HTTPS : permet de créer un serveur web sécurisé du côté signalisation ;

→ Websocket : permet de créer des flux bidirectionnels pour des communications en temps réel [106];

→ MySQL : permet de se connecter et d'interroger la base de données.

5.5.1.4 Description de l'environnement de test Jmeter

Jmeter est une application Java open source conçue pour tester des applications de type client/serveur. Elle permet de tester les performances sur les ressources statiques et dynamiques telles que les fichiers, les objets Java, les bases de données, des serveurs FTP, etc. Elle peut être utilisée pour simuler une lourde charge sur un serveur, un réseau ou un objet, dans le but de tester la performance globale dans différents types de charge [107]. Comme nous pouvons l'observer sur la figure 5.2, le plan de test est le plus haut niveau d'organisation au sein de JMeter. Il décrit une série d'étapes à exécuter lors des tests de montée en charge. Un plan d'essai complet comprendra un ou plusieurs groupes de fils notamment les contrôleurs logiques, les contrôleurs générateurs d'échantillons, les auditeurs, les minuteries, les assertions et les éléments de configuration.

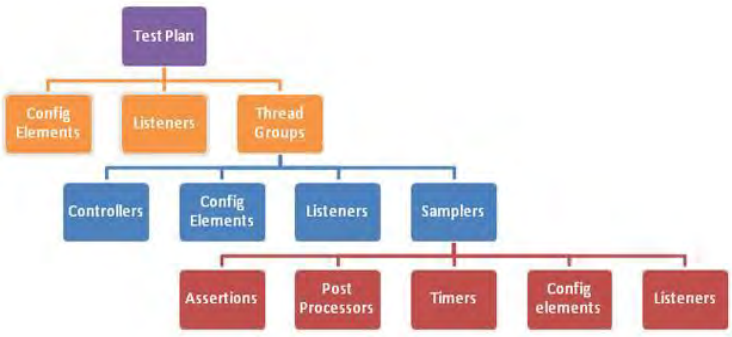

Figure 5.2 : Composants d'un plan de test sous JMeter

→ Description des composants essentiels d'un plan de test

Parmi ces composants, nous nous intéressons à ceux qui correspondent le mieux à nos exigences de test :

- Threads Group : ce sont des composants utilisés pour spécifier le nombre d'unités en cours d'exécution et la période de montée en charge. Chaque unité simule un utilisateur tandis que la période de montée en charge spécifie le temps d'exécution de toutes les unités.

- Samplers : ce sont des requêtes configurables qui prennent les serveurs HTTP, FTP ou LDAP en charge.
- Listeners : ils sont utilisés pour afficher les données de demande de traitement.

→ Architecture de l'environnement de test

L'architecture proposée dans la figure 5.3 représente l'enjeu et l'environnement de test constitué de plusieurs composants qui interagissent entre eux.

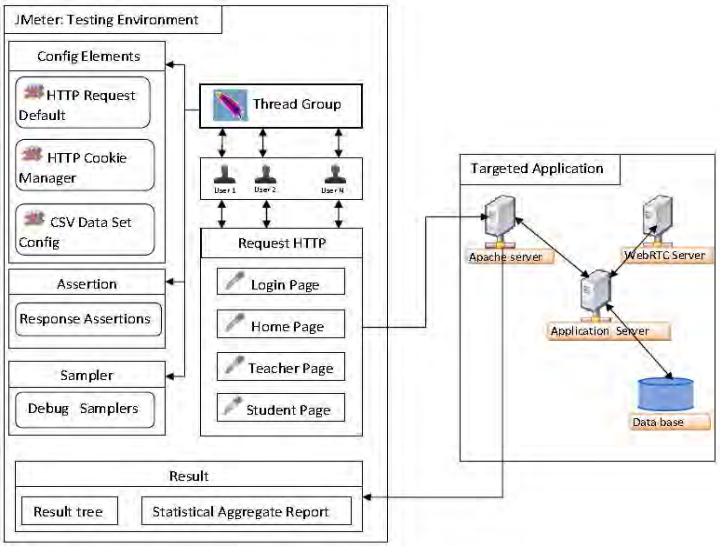

Figure 5.3 : architecture de l'environnement de test

L'architecture de l'environnement de test nous permet de décrire le processus de plan de test. Ce processus montre les interactions entre les différents composants de JMeter et l'application testée. La mise en place d'un plan de test peut être décrite comme suit :

- Lancement de Jmeter avec principalement deux composants qui sont : la section plane de test (espace de travail réservé aux éléments constituant le plan de test à exécuter) et la section Workbench (plan de travail) qui est un espace de travail temporaire non enregistré.
- Définition du nombre d'utilisateurs virtuels, de l'itération et de la durée du Ramp up (durée de montée de charge) via le « Thread Group » préalablement configuré. Ce composant constitue l'élément de base de notre scénario « authentification ». Le Thread group fait appel au HTTP RESQUEST SAMPLERS pour exécuter le scenario de test de performance. Il lance en premier la page de « login » pour l'authentification des utilisateurs. Ces utilisateurs prennent en séquence les informations de connexion stockées dans un fichier CSV (Comma-separated values).

- Lancement de la page de redirection avec les paramètres login et mot de passe par le HTTP REQUEST SAMPLERS, en utilisant les éléments de configuration.
- Chargement du fichier de données des utilisateurs stocké en local sous forme CSV et ouverture de la page d'accueil correspondante par le HTTP REQUEST SAMPLERS selon le type d'utilisateurs connectés (enseignant ou étudiant).

En exécutant le système sous test, l'application reçoit les requêtes, vérifie l'authenticité de l'utilisateur, renvoie le statut (succès ou échec) à JMeter via le composant réponse d'assertion. JMeter génère alors les résultats en utilisant les listeners. Le résultat généré peut être stocké sous forme de fichier XML ou html.

5.5.1.5 Paramétrage et implémentation

Dans cette partie, nous décrivons certaines vues de paramétrage dans notre environnement de test.

→ Groupe d'unité : il permet de définir la charge à appliquer lors du test de la page ainsi que les différents paramètres de test à savoir le nombre d'utilisateurs, la durée de la montée en charge, le nombre d'itérations et la gestion des erreurs.

Les figures 5.4, 5.5 et 5.6 montrent respectivement les vues de paramétrage d'un groupe d'unités, paramétrage HTTP REQUEST par défaut et configuration du fichier source de données csv.

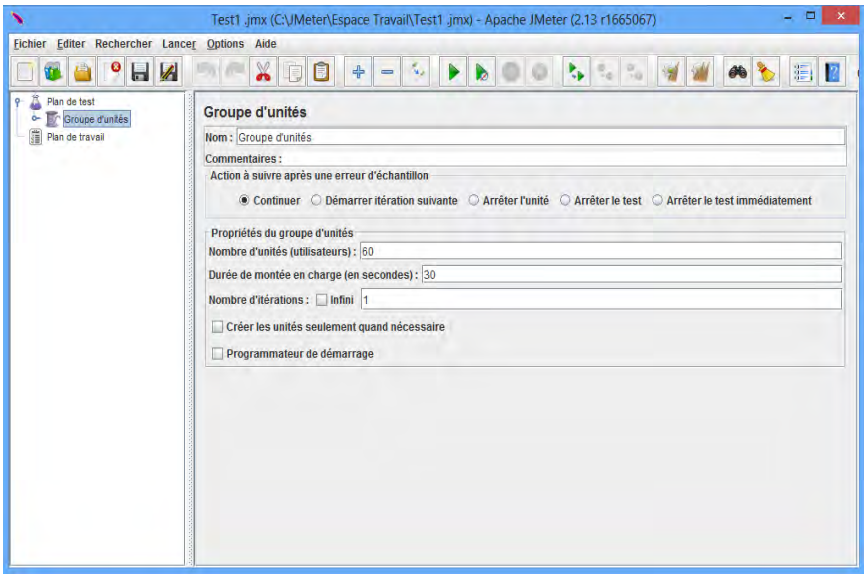

Figure 5.4 : paramétrage d'un groupe d'unités

→ HTTP REQUEST par défaut : il spécifie les paramètres communs à toutes les requêtes HTTP exécutées.

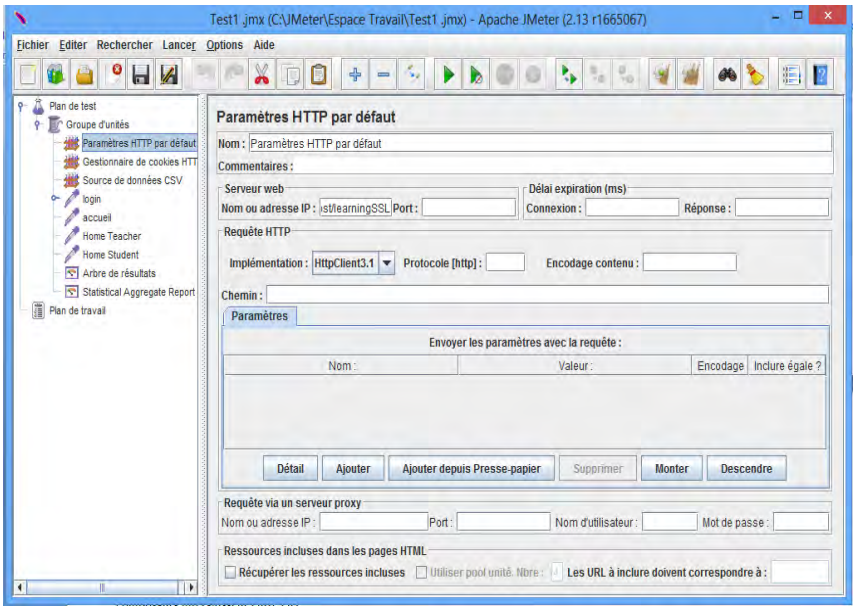

Figure 5.5 : paramétrage HTTP REQUEST par défaut

→ Source de données CSV : elle permet de lire un fichier CSV et de le mettre dans une ou plusieurs variables JMeter. Sur la vue de configuration du fichier source de données CSV de la figure 5.6, nous renseignons les paramètres tels que le chemin absolu, le nom du fichier, l'encodage du fichier, les noms des variables, le délimiteur, le Recycler et l'arrêt de l'unité.

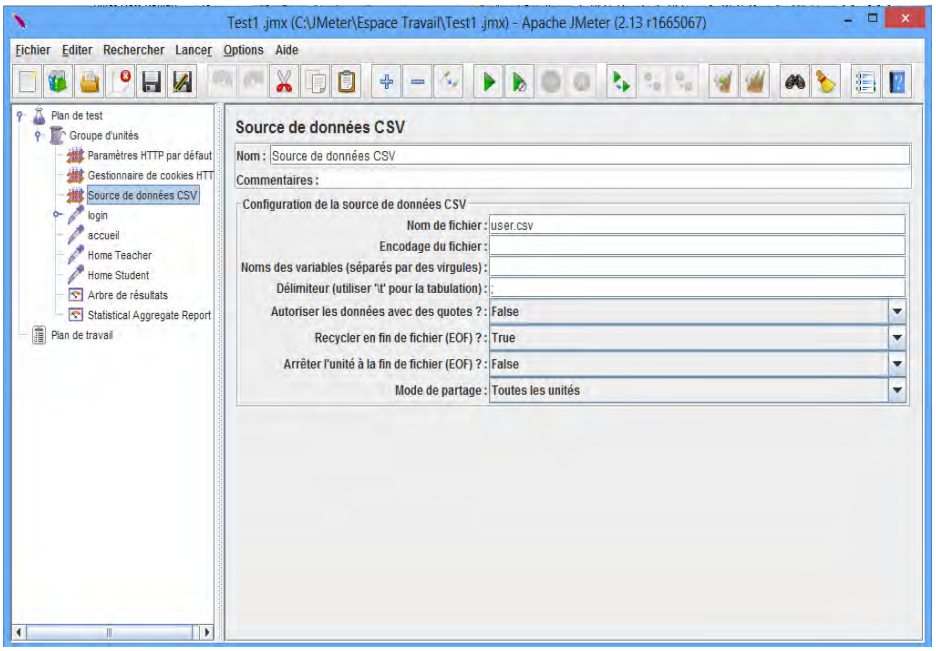

Figure 5.6 : configuration du fichier source de données csv

5.5.1.6 Résultat des tests de notre contribution sur la performance du WebRTC

Dans cette partie, nous présentons les résultats de tests de plusieurs itérations du scénario « authentification » sur la plateforme de test e-learning intégrant la technologie WebRTC. Ces tests ont été faits sur la configuration unique de l'environnement Jmeter.

→ Itération1 : consiste à enrôler 10 utilisateurs virtuels, pour une durée de montée en charge de 30 secondes. L'exécution du test s'est déroulée avec succès tel que le montre la figure 5.7 ci-dessous.

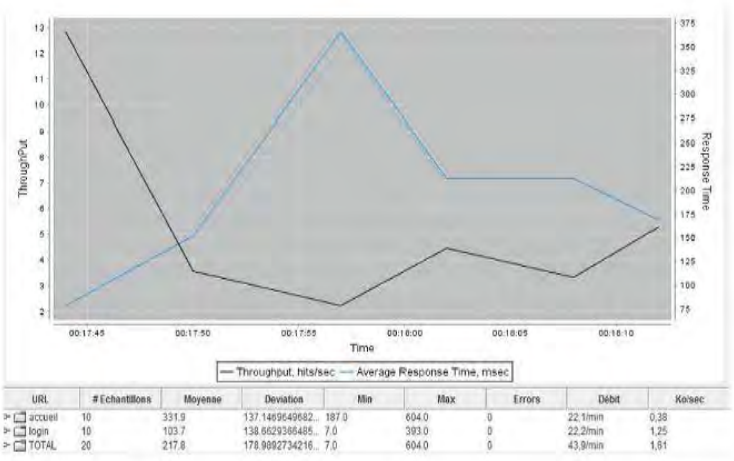

Figure 5.7 : test Plan pour 10 utilisateurs virtuels

→ Itération 2 : elle a été réalisée avec succès pour 50 utilisateurs, tout en conservant les mêmes paramètres définis dans l'itération 1. Voir la figure 5.8.

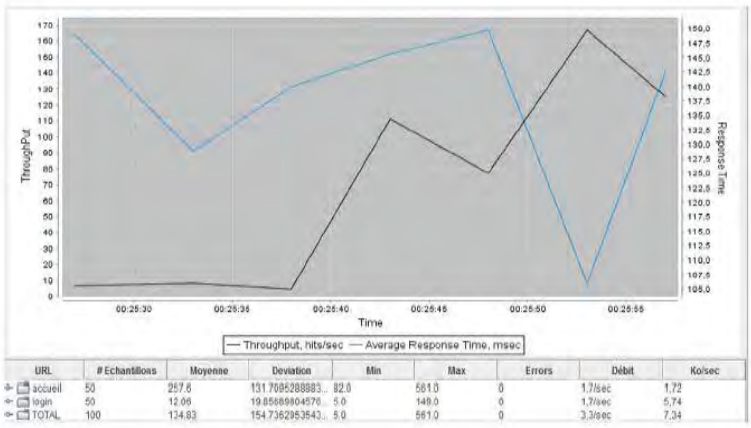

Figure 5.8: test Plan pour 50 utilisateurs virtuels

→ Itération 3 : elle aussi a été effectuée avec succès pour 100 utilisateurs tout en maintenant les mêmes paramètres que ceux définis dans la première itération. Voir la figure 5.9

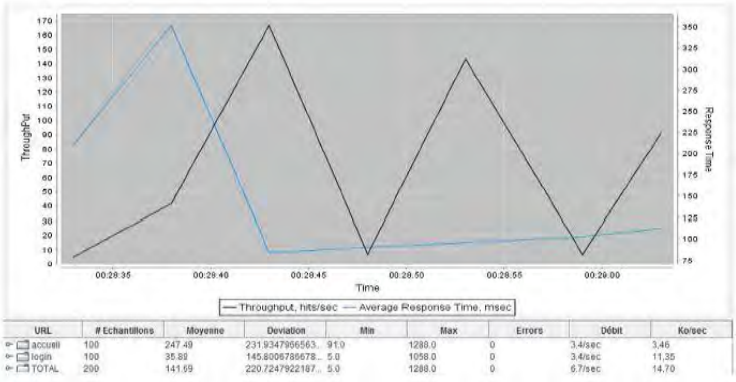

Figure 5.9 : test Plan pour 100 utilisateurs virtuels

→ La plateforme testée permet à un certain nombre d'acteurs (maximum 30 étudiants) de participer à une visioconférence pour un événement concernant un cours. Pour être réaliste, nous avons choisi de charger jusqu'à 200 utilisateurs virtuels pour l'itération 4, avec les mêmes paramètres que ceux des itérations précédentes. La figure 5.10 ci-dessous affiche le résultat du test effectué avec succès.

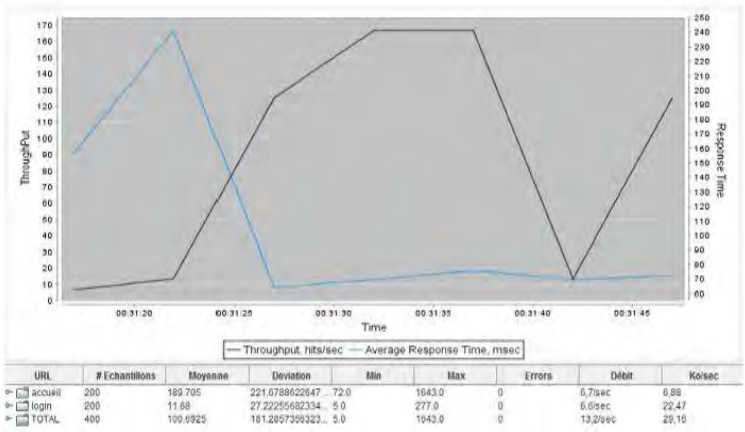

Figure 5.10 : test Plan pour 200 utilisateurs virtuels

→ Analyse des résultats

Le tableau 5.1 affiche les valeurs totales de tous les tests effectués avec un nombre variable d'utilisateurs virtuels.

Tableau 5.1 : Rapport sommaire des tests

	Total Echantillons	Moyenne en ms	Déviation	Min	Max	Erreur	Débit	KO/Sec
Itération 1	10	217.8	178.99	7.0	604.0	0	43.9/s	1.61
Itération 2	50	134.83	154.74	5.0	561.0	0	3.3/s	7.34
Itération 3	100	141.69	220.72	5.0	1288.0	0	6.7/s	14.70
Itération 4	200	100.0	101.21	5.0	1643.0	0	13.2/s	29.70

Les valeurs consignées dans le tableau 5.1 peuvent se décrire comme suit:

→ Le total des échantillons représente le nombre total de requêtes traitées, soit le nombre total d'utilisateurs s'authentifiant à un instant précis sur la plateforme.

→ La moyenne μ représente le temps moyen en milliseconde de réponse à une requête. Elle s'obtient grâce à la formule suivante :

$$\mu = 1/n * \Sigma_{i=1\ldots n} x_i \quad \textbf{(5.1)}$$

Où **n** représente le nombre total de requêtes d'un plan de test, et $\mathbf{x_i}$ représente le temps de réponse du serveur à une requête.

Exemple : considérons l'itération 1 avec les temps de réponse respectifs des requêtes x1 et x2, puis calculons le temps moyen de réponse μ du serveur :

X_1= 331.9 ; X_2= 103.7 ; n=2.

X_1 représente le temps de réponse du serveur à la requête accueil et X_2 le temps de réponse du serveur à la requête de login, et n est le nombre total des requêtes de l'itération 1.

$$\mu = 1/2\ (331.9 + 103.7) = 217.8 \text{ ms}$$

Le résultat obtenu de la moyenne μ pour l'itération 1 peut être observé sur la troisième colonne du tableau 5.

→ La déviation mesure la variabilité ou la dispersion d'un ensemble de données par rapport à la valeur moyenne. Elle s'obtient avec la formule suivante :

$$\sigma = 1 / n * \sqrt{\Sigma i = 1 \ldots n\ (x-\mu)^2} \quad \textbf{(5.2)}$$

n représente le nombre total de requêtes, **x** le temps de réponse à une requête et μ le temps de réponse moyen.

→ Min représente le plus petit temps de réponse à une requête et Max quant à lui, représente le temps de réponse le plus élevé à une requête.

→ Errors à l'état « 0 », signifie que les tests se sont effectués sans erreurs : nous pouvons déduire que le système testé intégrant la technologie WebRTC est fiable.

→ La dernière colonne du tableau 5 montre que le taux (Ko/s) de transfert de l'information ne diminue pas conséquemment, malgré l'augmentation importante du nombre de requêtes.

La figure 5.11 montre que la quantité d'octets transmise est invariable, selon que l'utilisateur accède à la page d'accueil (1967 octets) ou à la page d'authentification (3707 octets). Nous pouvons déduire que le système est stable et performant.

Comparativement à la figure 5.11, la figure 5.12 montre que, le temps de latence est de moins en moins important lorsque le nombre d'utilisateurs ou le nombre de requêtes augmente considérablement.

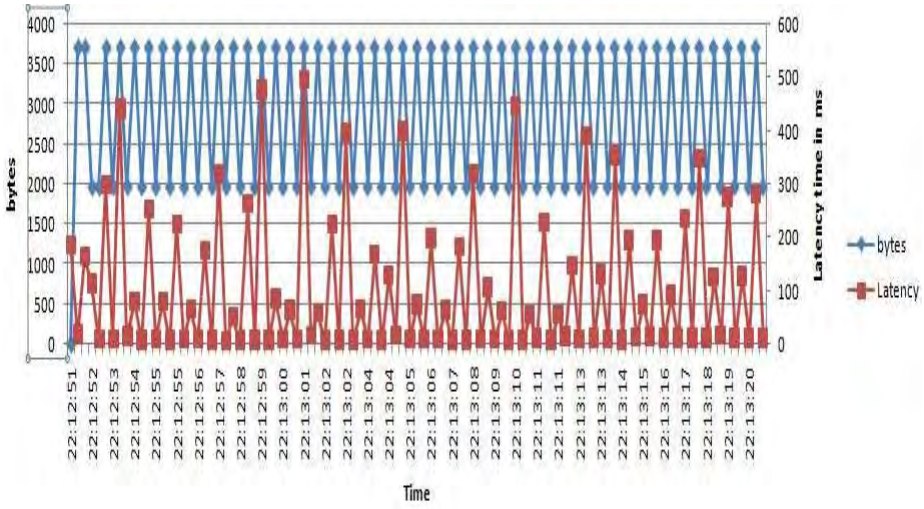

Figure 3 Figure 5.12 : débit et latence par rapport au temps pour 50 Utilisateurs

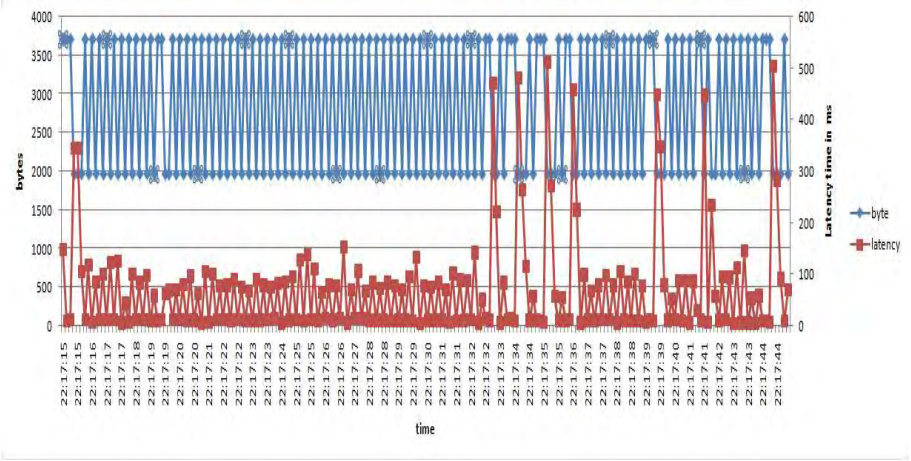

Figure 2 Figure 5.11 : débit et latence par rapport au temps pour 100 Utilisateurs

Le rapport détaillé du fichier.csv d'un plan de test montre que le temps de latence n'augmente pas proportionnellement à l'augmentation du nombre d'utilisateurs, et donc de requêtes. Ceci nous permet de déduire que le système est performant. Voir le tableau 5.3 montre l'extrait du rapport du fichier csv.

Tableau 5.2 : Extrait du rapport du fichier csv

Utilisateurs virtuels total	Temps total écoulé	Etiquette	Code Réponse	Message Réponse	Type de données	Succès	Bits	Temps de latence
5 UV	882	Login/Accueil	200	OK	Texte	True	28362	617
10 UV	3130	Login/Accueil	200	OK	Texte	True	56716	2359
50 UV	13527	Login/Accueil	200	OK	Texte	True	283584	10607
100 UV	20157	Login/Accueil	200	OK	Texte	True	567168	14383
200 UV	27332	Login/Accueil	200	OK	Texte	True	1134344	16325

Dans cette section, nous avons effectué des tests de montée en charge et de performance d'une plateforme e-learning intégrant la technologie webRTC Bilong et al. [92]. Nous avons utilisé plusieurs composants de JMeter dans un environnement unique pour l'exécution des tests. Nous avons fait varier le nombre d'utilisateurs virtuels tout en évitant de stresser le système.
Les résultats obtenus montrent la stabilité, la disponibilité, la fiabilité et la performance du système testé. Ces résultats justifient notre choix de la technologie WebRTC utilisée dans nos travaux de thèse.

5.5.2 Realm

Realm implémente l'interface Java org.apache.catalina.realm McKinney [108]. C'est un outil du serveur d'application Tomcat qui intègre un mécanisme de sécurité basé sur l'authentification. Il permet de protéger l'accès des ressources au serveur, en appliquant des contraintes de sécurité. Son principe de fonctionnement consiste à gérer une liste d'utilisateurs avec des rôles. Il est un élément particulier de la configuration Tomcat, car il peut être inséré comme threads de différents conteneurs (Moteur, Hôte ou Contexte). Une contrainte de sécurité sera donc de définir quel utilisateur ou rôle a accès à quelle ressource protégée.

5.5.3 Weka

WEKA est un logiciel libre (GNU) développé en JAVA par le département informatique de l'université Wekato (Nouvelle Zélande). Il a été conçu dans le but de constituer une bibliothèque d'algorithmes et d'outils de visualisation qui facilitent la comparaison des jeux de données.

Selon Shapiro [109], l'outil WEKA s'est érigé au fils du temps comme un système de référence dans le domaine du datamining et celui de l'apprentissage machine. Il est constitué des quatre principaux modes suivants :

→ Explorer : mode graphique permettant de réaliser une exploration de l'analyse de données;

→ Experimenter : mode graphique permettant de monter des expériences (construire des schémas) sur de grands jeux de données afin de réaliser des comparaisons de performance ;

→ Knowledge flow : mode graphique alternatif au mode Explorer, permettant de construire un graphe dans lequel les nœuds peuvent être des sources de données, des filtres etc.

→ Simple CLI : mode ligne de commande de WEKA.

La figure 5.14 présente l'écran d'accueil de WEKA avec les quatre modes sous forme d'onglet.

Figure 4 Figure 5.13 : Ecran d'accueil de WEKA

Dans le cadre de nos travaux, nous nous sommes focalisés principalement sur le mode Explorer. Il s'agit de l'interface principale de WEKA composé de 6 modules en l'occurrence Preprocess, Classify, Cluster, Associate, Select attributes et Visualize.

→ Preprocess : permet la saisie des données, l'examen, la sélection et la transformation des attributs.

→ Classify : offre les méthodes de classification.

→ Cluster : permet les méthodes de segmentation (clustering).

→ Associate : gère les règles d'association.

→ Select attributes : permet l'étude et la recherche de corrélations entre attributs.

→ Visualize : permet les représentations graphiques des données.

5.5.4 Kurento Media server (KMS)

Kurento est un serveur multimédia (KMS) WebRTC libre qui permet de créer des applications de traitement de média basées sur le concept de pipelines via un simple protocole réseau basé sur JSON-RPC. Les pipelines médias sont créés par des modules d'interconnexion appelés Media Eléments. Chaque Media Elément fournit une fonctionnalité spécifique. KMS contient

des Media Eléments capables d'enregistrer et de mixer des flux, de faire de la vision par ordinateur, etc.

Cependant, pour simplifier davantage le travail des développeurs, une API client implémentant le protocole JSON-RPC et exploitant directement les Media Eléments et les pipelines est fournie.

Garcia et ses collaborateurs [110] ont mené des tests de montée en charge sur un environnement intégrant KMS. Les résultats obtenus sur la figure 5.14 leur ont permis de déduire que la montée en charge de KMS en termes de latence est éprouvée par le fait que de très gros pipelines média peuvent être exécutés tout en maintenant des fonctionnalités en temps réel pour les applications. De plus, KMS présente des performances linéaires pour les paramètres physiques tels que l'unité centrale de traitement (CPU), la mémoire etc.

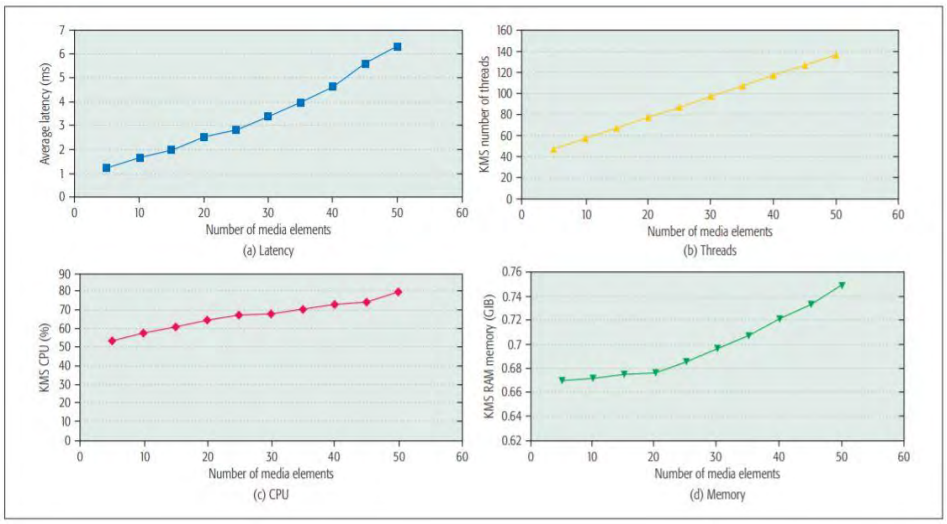

Figure 5.14: Résultats de l'évaluation de la montée en charge de Kurento Media Server

5.6 Implémentation des modèles proposés

Dans les chapitres précédents, nous avons fait la revue de la littérature de plusieurs modèles de contrôle d'accès et y avons extrait les limites. Sur la base de ces limites, nous avons fait des contributions qui permettent respectivement :

→ d'administrer dynamiquement les rôles dans un environnement intégrant Realm

→ d'évaluer et de minimiser les erreurs de confiance

→ de protéger la vie privée des utilisateurs dans un environnement connecté.

Dans cette section, nous allons implémenter ces modèles principalement dans deux domaines sensibles à savoir l'e-learning et l'e-santé

5.6.1 Implémentation dans l'environnement e-learning

Dans cette section, nous allons implémenter nos contributions afin de garantir la stabilité et la disponibilité des plateformes intégrant la technologie WebRTC, de rendre dynamique la délégation de rôle sur les plateformes intégrant Realm de Java security, d'évaluer les critères d'appréciation de la confiance afin de minimiser les erreurs lors d'une délégation de rôle et de préserver la vie privée des sujets via l'internet des objets.

5.6.1.1 Contexte

En référence au contexte décrit dans la section 2.4.1.1 pour la mise en place du modèle, nous réitérons que l'e-learning présente des difficultés tant pour les apprenants que pour les enseignants. A raison du nombre croissant de bacheliers dans plusieurs Etats Africains ces dix dernières années, les gouvernants ont voté le projet qui ratifie la diplomation dans l'enseignement supérieur via l'enseignement à distance.

C'est ainsi qu'au Sénégal, l'Université virtuelle du Sénégal (UVS) a été mise sur pied et à ce jour recrute des milliers d'apprenants. Cette université virtuelle s'organise autour d'un ensemble d'espaces numériques ouverts (ENO), permettant ainsi aux étudiants de rester connectés aux heures de cours ou séances de travail en ligne. Ces ENO permettent d'appliquer le « Blending Learning » (alternance cours en présentiel et à distance) et limitent ainsi la fracture numérique.

Les nouveaux bacheliers ne disposant que d'une expérience d'apprentissage en présentiel rencontrent d'énormes difficultés d'adaptation. Ce qui a entraîné des abandons massifs des étudiants orientés à l'UVS. Ces abandons étaient dus au fait que les apprenants se sentaient seuls, loin de tout contact avec les enseignants. Pour parer à cette situation, plusieurs modèles ont été proposés par des chercheurs, dans le but de faire vivre une meilleure expérience à toutes les parties prenantes de l'enseignement à distance. Les apprenants peuvent alors suivre les cours en mode synchrone via des communications temps réel [103]. Ces plateformes sont sécurisées avec la mise en place des modèles de contrôle d'accès pour la gestion des authentifications, des autorisations et de la protection de la vie privée des utilisateurs.

5.6.1.2 Contribution au mécanisme de « mapping » entre les utilisateurs d'une plateforme e-learning et WebRTC

Malgré les avantages offerts par la technologie WebRTC, cette dernière, une fois intégrée sur la plateforme e-learning proposée dans [103], ne gère pas les identifiants des utilisateurs connectés. Ainsi, lors d'une séance de visioconférence dans une classe virtuelle, l'enseignant qui initie la conférence ne peut pas être capable d'identifier les noms de chaque apprenant. Ceci constitue une faille de sécurité pour une telle plateforme.

L'authentification et l'autorisation étant deux éléments essentiels de notre problématique, nous avons proposé un mécanisme de mapping entre les utilisateurs d'une plateforme e-learning intégrant la technologie WebRTC [111]. Ce mécanisme permettra de fusionner dans une structure logique, un utilisateur de la plateforme e-learning et son correspondant dans celle du WebRTC. L'objectif est de masquer la complexité liée à la signalisation du WebRTC, en offrant un système facile à gérer du point de vue de l'identification des utilisateurs. Nous avons implémenté ce mécanisme sous forme d'un plugin pour un portail e-learning et un portail WebRTC [111] . Il requiert, pour son fonctionnement, une page d'échanges en temps réel afin d'établir la connexion du serveur web avec le serveur WebRTC. L'API Web-Socket sera utilisé, dans ce contexte, pour gérer la communication bidirectionnelle entre le serveur web et le serveur de signalisation.

L'architecture proposée sur la figure 5.16 permet d'intégrer facilement un système de gestion des utilisateurs. Nous pouvons la décrire comme suit :

1. Création de l'utilisateur web de la plateforme à partir d'un panneau d'inscription.
2. Ajout de l'utilisateur dans la base de données.
3. Lancement du serveur de signalisation référencé par son adresse IP et son port grâce au protocole HTTP.
4. Génération d'un nouvel utilisateur Signalling/WebRTC à partir du serveur de signalisation.
5. Insertion de l'utilisateur généré dans la base de données par le serveur de signalisation.
6. Envoi d'un callback au serveur web pour confirmer l'ajout de l'utilisateur de signalisation dans la base de données.
7. Lancement de l'API mapping par le serveur web en lui passant les informations de ces deux utilisateurs créés dans la base de données.

L'utilisateur logique résulte de la transformation de deux utilisateurs du système via l'API « mapping ». Cet utilisateur combine des informations lui permettant d'accéder à l'ensemble des services de la plateforme (services web et services Signalisation). Nous avons intégré ce mécanisme sous forme de plugin dans le but de montrer la faisabilité et l'utilité de notre approche.

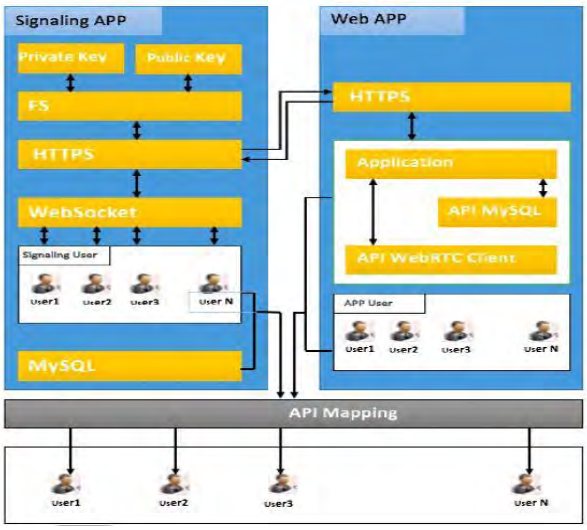

Figure 5.15 : composants de l'environnement étudié

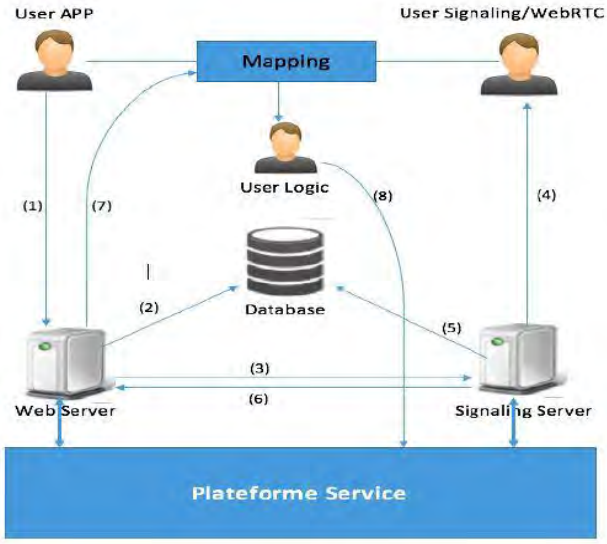

Figure 5.16 : architecture du mécanisme de « mapping »

Comme le montre la Figure 5.15, le système étudié contient deux plateformes (qui s'exécutent sur deux serveurs différents). L'API mapping y intervient pour remplir les tâches suivantes :

→ Récupérer la liste des utilisateurs e-learning de la plateforme web stockée dans la base des données.

→ Attendre qu'un utilisateur choisisse une vue d'échange en temps réel sur la plateforme web (visioconférence, le Tchat, le partage d'écran ou le transfert de fichier … etc.)

→ Lancer la connexion et l'interaction avec le serveur WebRTC (elle utilise le protocole HTTP pour se connecter au serveur de signalisation (WebRTC) et le protocole Web-Socket pour gérer la communisation bidirectionnelle).

→ Récupérer l'utilisateur de signalisation généré par le serveur WebRTC grâce à son identifiant et le fusionner avec l'utilisateur web (en lançant la page vue de la plateforme web) pour en faire un utilisateur logique.

→ Insérer cette combinaison de deux utilisateurs différents dans la base de données.

Le processus se répète pour tout utilisateur e-learning désirant échanger en temps réel avec un autre utilisateur.

La Figure 5.17 montre l'interaction entre les composants des différentes phases (Mapping des utilisateurs et le contrôleur de service). Ces composants sont des interfaces qui s'exécutent dans deux serveurs distincts (le serveur de signalisation implémenté grâce au langage NodeJs et le serveur web implémenté avec le langage PHP). Ces interfaces décrivent le scénario de mapping entre les utilisateurs de la plateforme web et celle du WEBRTC.

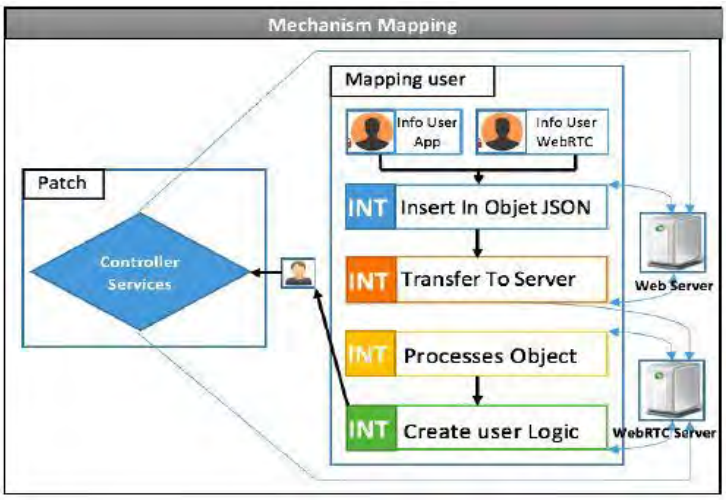

Figure 5.17 : interface du mécanisme de mapping des utilisateurs

Sur la Figure 5.18**,** nous pouvons observer que le serveur WebRTC ne gère pas l'identité des utilisateurs. Ainsi, l'enseignant dont le nom est « Amath Bamba Mbacké » reçoit un appel de l'un de ses étudiants connectés dont l'identifiant est **HsPiGapuczsq47IXAAAB**.

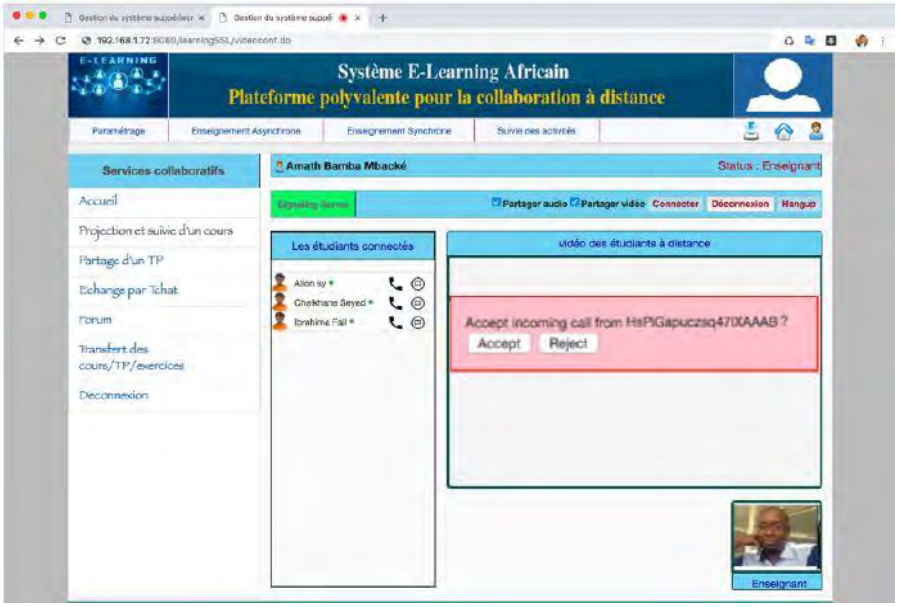

Figure 5.18 : utilisateur non mappé

Suite à l'installation du plugin décrit par le mécanisme de mapping ci-haut implémenté, nous obtenons les traces des résultats au niveau du serveur de signalisation. Ces traces décrivent le

résultat des interfaces implémentées, pour mapper les utilisateurs. La Figure 5.19 montre les traces de mapping sur le serveur de signalisation entre l'utilisateur e-learning connecté en tant qu'enseignant et son profil correspondant WebRTC.

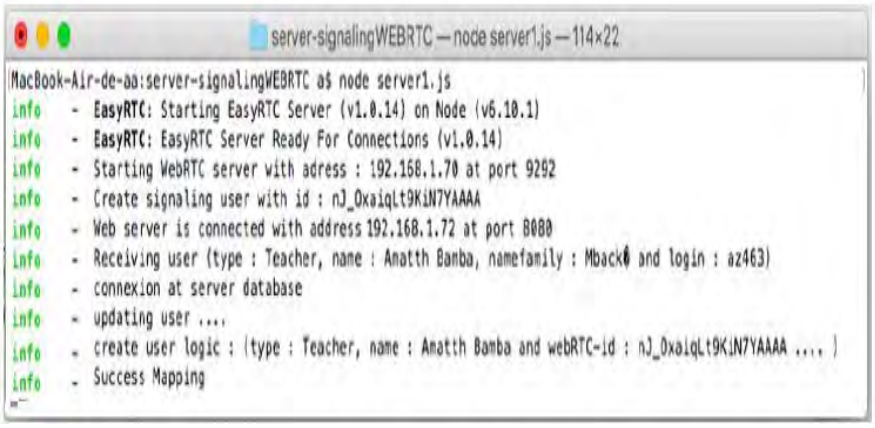

Figure 5.19 : trace de mapping d'un utilisateur de type enseignant avec celui du WebRTC

La Figure 5.20 montre le mapping avec succès des utilisateurs du fait que l'enseignant (Amath Mbacké) reçoit un appel de la part d'un utilisateur authentique dont le nom est : Alion Sy (Le Figure illustre l'étudiant mappé avec son correspondant WebRTC).

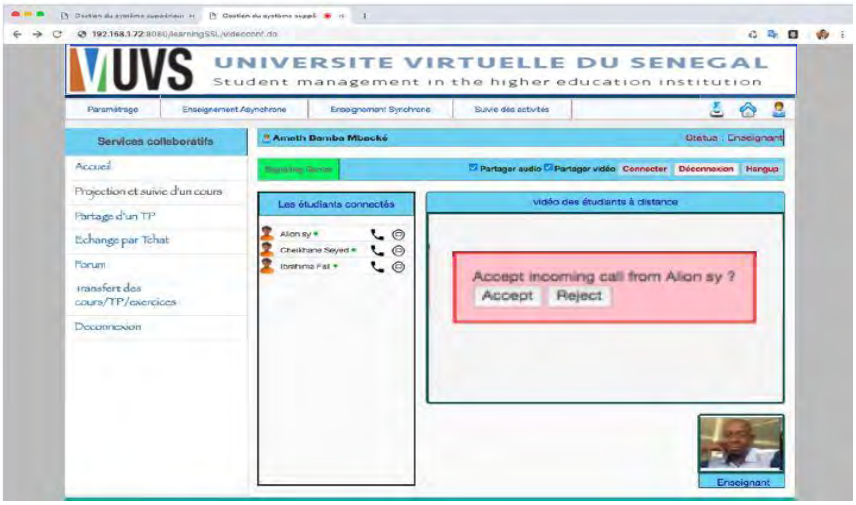

Figure 5.20 : appel authentifié

La Figure 5.21 décrit les traces de mapping pour un utilisateur e-learning dont le statut est étudiant avec son correspondant WebRTC.

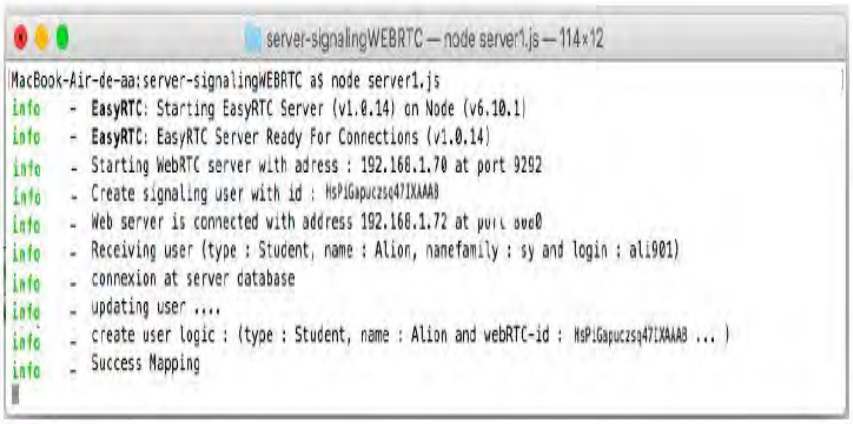

Figure 5.21 : trace de mapping d'un utilisateur de type étudiant avec celui du WebRTC

Cette section de notre thèse propose une solution qui permet de gérer l'authenticité de l'identité des utilisateurs connectés sur la plateforme e-learning. La solution est effective grâce au mécanisme de mapping entre les profils physique et logique d'un utilisateur. Nous avons implémenté ce mécanise sous forme d'un plugin qui a été intégré avec succès dans un environnement comprenant une plateforme e-learning et plateforme WebRTC. Cette solution nous amène à gérer les contrôles d'accès des utilisateurs ainsi authentifiés et stockés dans la base de données de notre application web.

5.6.1.3 Sécurisation des données via Realm

Comme défini précédemment, Realm est un outil du serveur d'application Tomcat de JEE qui intègre un mécanisme de sécurité basé sur l'authentification. Il permet de protéger l'accès des ressources au serveur, en appliquant des contraintes de sécurité. Seulement, ce mécanisme est statique et fonctionne selon le standard du modèle de contrôle d'accès basé sur les rôles. Ce mode de contrôle d'accès est complexe pour la mise à jour de par son caractère statique. Ainsi, pour des besoins de mise à jour de politique de contrôle d'accès dans des applications développée sous JEE, l'intervention d'un programmeur est nécessaire. Selon McKinney [108], les applications web Java disposent de deux zones de contrôle d'accès à savoir Java EE et Spring Role Contrôles déclaratifs et Permission RBAC Vérifications programmatiques. La figure 5.22 montre un code de contrôle d'accès basé sur le modèle RBAC.

```
1 < Context  reloadable = " true " >
2
3    < Realm  className = " org.apache.directory.fortress.realm.tomcat.Tc7AccessMgrProxy "
4          defaultRoles = " ROLE_DEMO2_SUPER_USER, DEMO2_ALL_PAGES, ROLE_PAGE1, ROLE_PAGE2, ROLE_PAGE3 "
5          containerType = " TomcatContext "
6          contextId = " HOME "
7          realmClasspath = " "
8           />
9 </ Contexte >
```

Figure 5.22 : activation du domaine de sécurité (Realm) Java EE

Nous pouvons observer sur la figure 5.24 qu'il n'est pas aisé de modifier la politique de contrôle d'accès ainsi définie. La ligne 3 montre l'activation de Realm de Tomcat. La ligne 4 active les rôles ROLE_DEMO2_SUPER_USER, DEMO2_ALL_PAGES, ROLE_PAGE1, ROLE_PAGE2, ROLE_PAGE3 sur une session RBAC.

Pour parer à cette difficulté, nous avons fait une contribution qui permettra de gérer dynamiquement le contrôle d'accès dans une application web Java EE. Nous avons proposé une architecture qui permettra d'implémenter une plateforme interfacée par un middleware.

La figure 5.23 montre la vue d'authentification des utilisateurs. Ces derniers pourront s'identifier afin d'accéder à l'ensemble des ressources qui leur ont été assignées.

Figure 5.23 : vue d'authentification

La figure 5.24 montre la page accueil de notre plateforme. Cette vue est réservée à l'administrateur chargé d'administrer l'ensemble de l'application, y compris la configuration et la gestion du contrôle d'accès. A cet effet, il crée les différents acteurs qui peuvent être des enseignants ou des tuteurs. Il attribue dynamiquement des rôles des tuteurs à différents utilisateurs en fonction de leurs profils.

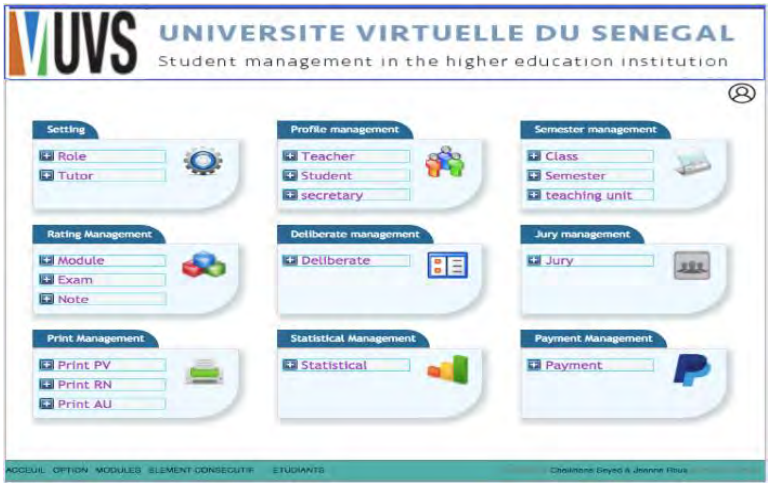

Figure 5.24 : Vue de paramétrage de l'application réservée à l'administrateur

La Figure 5.25 permet de gérer les deux principales fonctions de gestion du contrôle d'accès, telles que l'attribution des rôles et des tuteurs aux enseignants. Sur cette figure précisément, l'administrateur sélectionne l'enseignant Jeanne roux BILONG et lui donne l'autorisation sur les tâches qui lui sont assignées.

Figure 5.25 : vue d'assignation de rôle et de tuteur à l'enseignant

La Figure 5.26 présente la liste des différents tuteurs enregistrés dans la base de données. Seuls les tuteurs ayant un niveau de confiance avec le statut 'valider' sont assignés à l'enseignant. L'enseignant peut alors leur déléguer des tâches pour une durée déterminée.

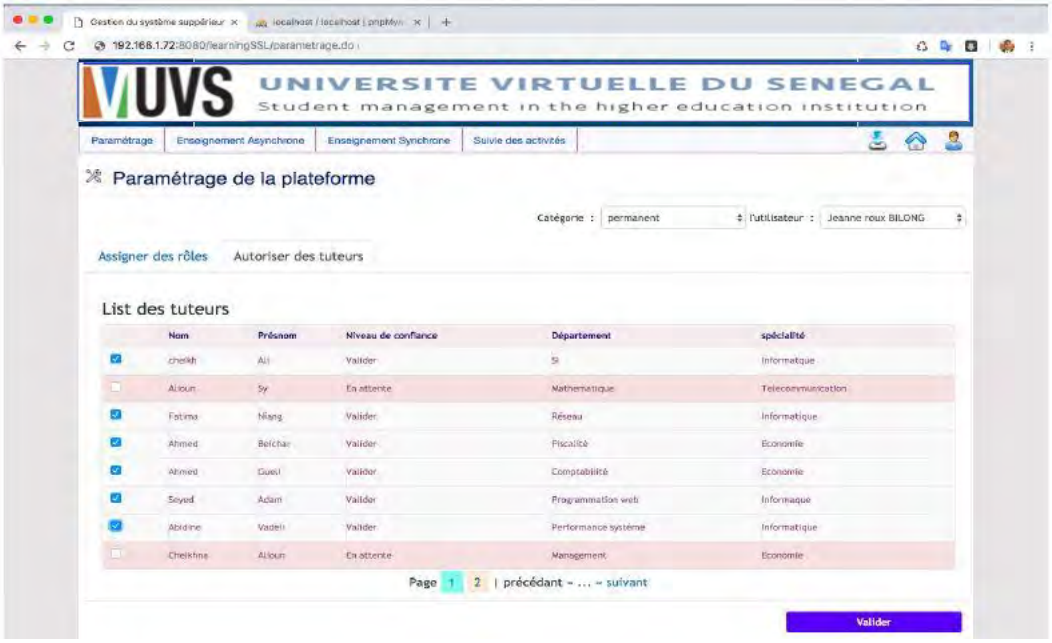

Figure 5.26 : liste de tuteurs et leur niveau de confiance

La Figure 5.27 est dédiée à l'enseignant. Ce dernier doit s'authentifier au préalable pour accéder à cette page. Comme le montre la figure suivante, l'enseignant Jeanne roux BILONG a la possibilité d'une part de faire les tâches qui lui ont été assignées par l'administrateur et d'autre part de déléguer ou de révoquer ses tâches.

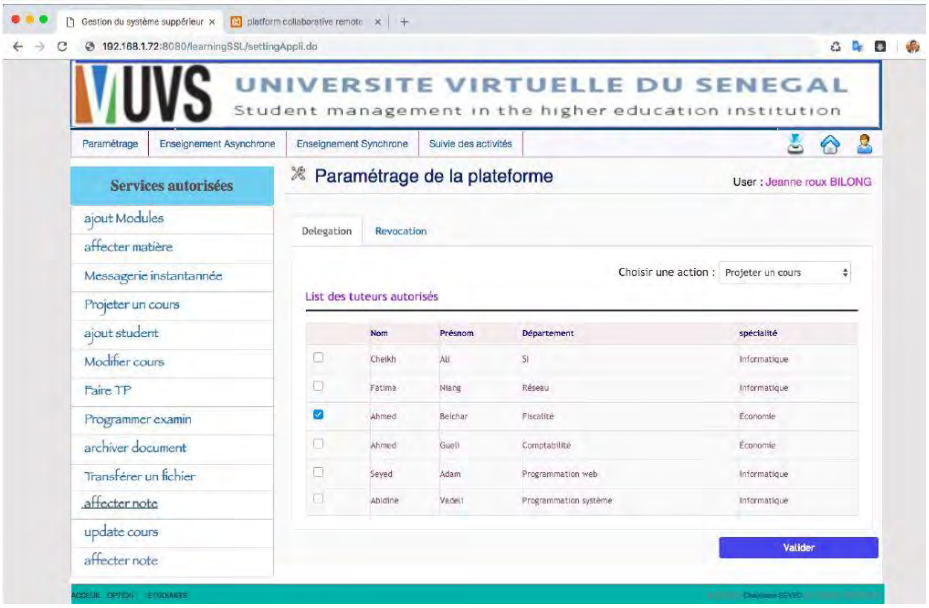

Figure 5.27 : vue de l'enseignant jeanne Roux BILONG

Sur la figure 5.28 ci-dessous, nous pouvons observer le statut du niveau de confiance de chaque tuteur. Seulement, ce niveau de confiance est défini de façon arbitraire. Pour corriger cette limite, nous avons proposé un modèle qui évalue les critères de confiance. Nous avons produit un algorithme de « scoring » (Score) après avoir défini les coefficients de chaque critère. Cet algorithme permet d'afficher les statuts « délégable » ou non « délégable » selon que le niveau de confiance est supérieur ou inférieur au seuil de confiance. La figure 5.30 affiche les statuts des tuteurs délégables et celui des tuteurs non délégables.

5.6.2 Implémentation du modèle proposé DORBAC dans l'environnement e-santé

A l'heure où les échanges d'informations deviennent nombreux et importants, l'accès aux informations d'ordre médical est de plus en plus complexe. En effet, la confidentialité est une notion importante dans la gestion des informations stockées des patients. Afin de résoudre les problèmes liés à la protection de la vie privée des sujets, nous allons implémenter le modèle en se référant au contexte décrit dans le chapitre 4.

5.6.2.1 Consultation à distante et stockage privé de l'information collectée

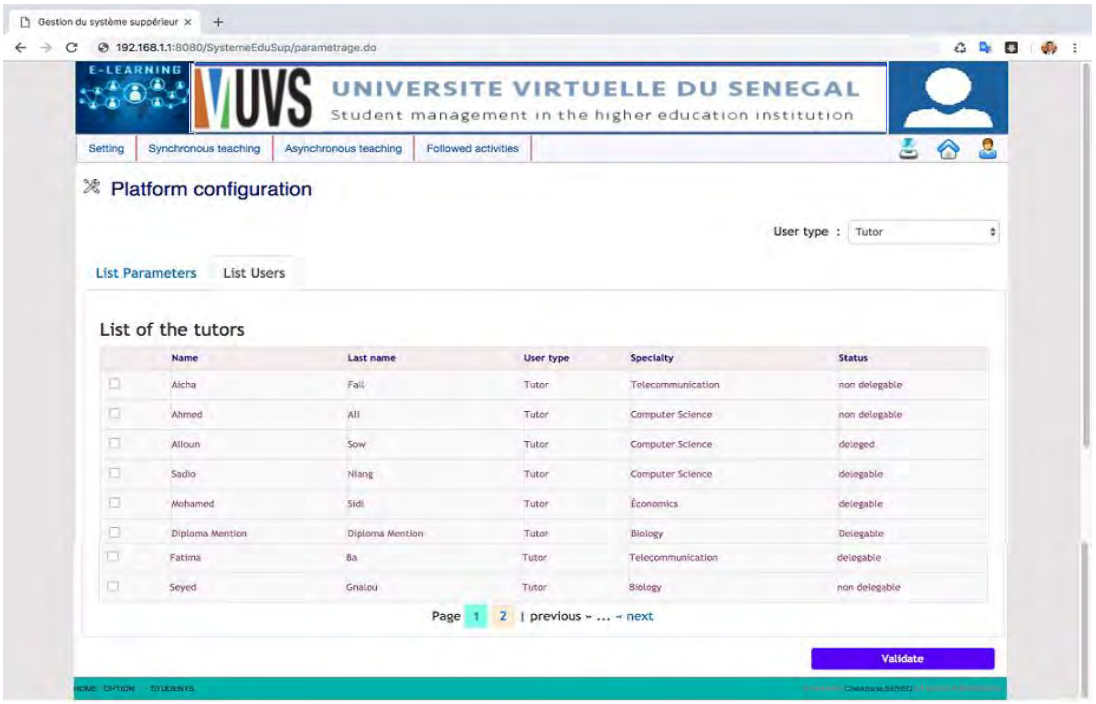

Figure 5.28 : vue de configuration d'un tuteur

La plateforme mise en place permet d'une part à l'agent de santé (infirmier, secrétaire médical etc.) de se connecter sur la plateforme afin d'enregistrer les informations liées à l'identité du patient et d'autre part aux médecins et aux patients de s'enregistrer et de s'authentifier pour accéder aux fonctionnalités.

Lorsque le patient se présente pour une consultation, l'agent de santé lui crée un dossier électronique s'il arrive pour la première fois ou alors, il le recherche dans la base de données des patients afin de procéder à la récupération des informations de consultation via les capteurs médicaux.

L'architecture que nous avons proposée dans le chapitre 4 nous permet d'implémenter l'examen clinique à distance. La figure 29 ci-dessous montre le câblage de la passerelle Node MCU Gateway avec le capteur de température et d'humidité DHT11 qui sera connecté au patient afin de recueillir l'information.

Figure 5.29: Câblage de l'ESP8266 avec le DHT11

Une fois que l'information du patient est stockée via les capteurs dans la base de données, le médecin peut alors communiquer avec un patient à l'aide du serveur Kurento Media. Le médecin traitant dispose d'un ensemble de capteurs. Il peut traiter les informations recueillies par ces capteurs en temps réel, à l'aide de la plate-forme K-2I-E-health que nous avons mise en place. Ces données peuvent être analysées et commentées par d'autres médecins pour une décision collaborative. Seulement, ces derniers doivent bénéficier d'une autorisation du patient d'accéder à ses informations privées et d'une délégation de rôle lui donnant accès aux données du patient.

Figure 5.30: authentication sur K-2I-E-health

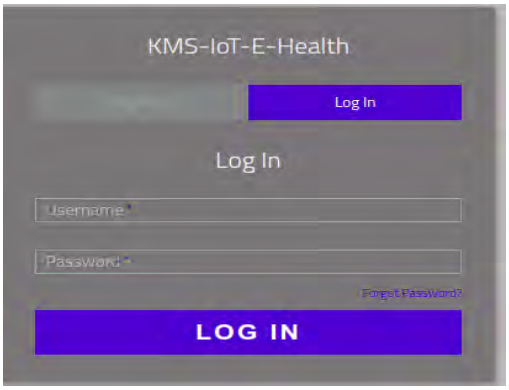

Figure 5.31: Login sur K-2I-E-health

Les figures 5.30 et 5.31 affichent respectivement les vues d'authentification (création de session) et de connexion (ouverture de session) de notre plateforme. Les utilisateurs connectés peuvent alors visualiser les données qui ont été collectées via les capteurs.

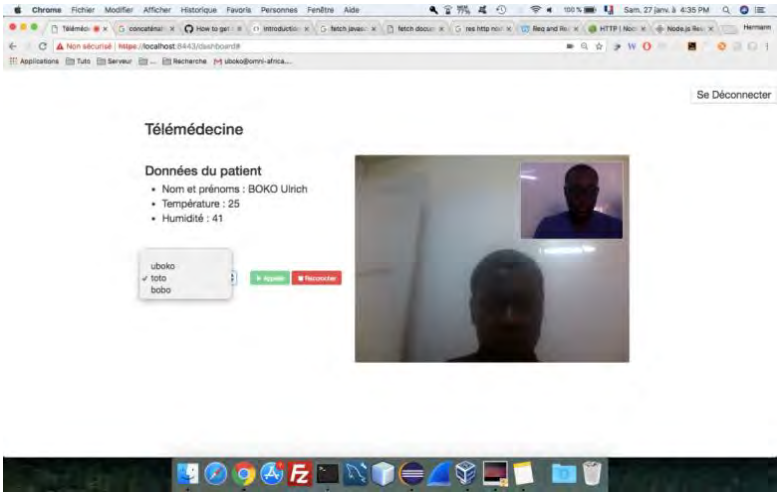

Figure 5.32 : Communication entre le médecin traitant toto et le patient BOKO

La figure 5.32 montre les acteurs médecins traitant et patients en pleine communication temps réel. Ils accèdent par la même occasion aux informations du capteur de température et d'humidité. Le même mécanisme est applicable à tous les autres capteurs.

5.7 Conclusion

Dans ce chapitre, nous avons défini le concept d'organisation virtuelle ainsi que la terminologie des organisations virtuelles du domaine de l'éducation et de la santé. Nous avons ensuite

implémenté les modèles de contrôle d'accès de nos différentes contributions en l'occurrence RDBDAC, DORBAC. Le modèle RDBDAC consiste à dynamiser le contrôle d'accès dans les applications web Java où la définition des autorisations se fait au niveau du domaine de sécurité (Realm) « Java EE Security » et « RBAC Policy decision point » via un fichier XML. Le modèle RDBDAC gère le contrôle d'accès basé sur les délégations et les rôles de façon dynamique sans avoir à modifier le code. Seulement, l'appréciation partiale de la confiance observée dans le modèle RDBDAC nous a amené à évaluer les critères de confiance afin de minimiser les erreurs de choix porté sur un délégataire. Le modèle DORBAC propose une architecture qui met le sujet (patient) en contact direct avec les capteurs via lesquels l'information sera récupérée et stockée directement dans la base de données. La vie privée du sujet est ainsi préservée car, seul le médecin traitant peut accéder aux informations du patient. En cas de besoin d'une décision collaborative sur le cas du patient, le modèle DORBAC donne la possibilité au médecin traitant de déléguer des privilèges ou rôles à un autre médecin disposant de l'autorisation du patient à accéder à ses informations personnelles.

Conclusion générale

Les travaux présentés dans cette thèse traitent de la stratégie des politiques de contrôle d'accès dans le but d'améliorer les délégations dynamiques de rôles et de protéger la vie privée des sujets. Suite aux limites observées dans l'état de l'art des modèles de contrôle d'accès, nous avons fait des contributions dont le but était de rendre objectifs et fiables (contributions qui ont permis d'intégrer des paramètres afin de prendre en compte les variations sensibles au contexte ainsi que les faits d'exception), les contrôles d'accès dynamiques basés sur les rôles et l'organisation. Nous avons introduit à la fois la notion de contexte (temporel et géographique) et celle de la confiance.

Nous avons entamé ces travaux par la définition de la terminologie autour de la politique de sécurité. Puis, nous avons fait l'état de l'art sur les modèles de contrôle d'accès. Cette revue de la littérature nous a permis de déceler les limites des contrôles d'accès basés sur les rôles qui sont caractérisés par leur aspect statique. De plus, les délégations de rôles basées sur la confiance restent partiales.

Nous avons par la suite proposé un modèle de contrôle d'accès dynamique nommé RDBDAC. Ce dernier améliore le modèle RBAC préconisé sur les plateformes intégrant Realm de Java security. Le modèle proposé a été implémenté en interfaçant un middleware afin de rendre dynamiques les délégations de rôle ainsi que leur mise à jour. Le modèle RDBDAC prend en compte les paramètres de confiance et de contexte temporel.

Par ailleurs, le modèle RDBDAC présente une limite car la valeur de la confiance ne peut prendre que deux états que sont 0 et 1. A cet effet, le cessionnaire peut déléguer son rôle lorsque la valeur du niveau de confiance assignée au délégataire équivaut à 1. La délégation ne dure que pendant une période bien définie. Passée cette durée, la délégation est révoquée.

Pour résoudre la question de subjectivité de la confiance qui pourrait être observée dans le modèle RDBDAC, nous avons proposé un modèle qui permet d'évaluer la confiance sur la base d'un ensemble de critères. Dans un premier temps, nous avons évalué les critères utilisés dans le recrutement d'un tuteur, en les pondérant grâce à l'algorithme du modèle SVR. La prédiction obtenue nous a permis de proposer une fonction qui minimise les erreurs de recrutement. Les tuteurs recrutés avec le meilleur score sont de potentiels délégataires. De plus, nous avons proposé un algorithme de confiance qui fait le scoring (score) afin de déterminer le

tuteur le plus digne de confiance. Cette évaluation a permis de minimiser les erreurs confiance lors d'une délégation de rôle.

La question de la protection de la vie privée n'ayant pas été prise en compte dans nos précédentes contributions, nous avons proposé un autre modèle dans le but de contribuer à la stabilité, fiabilité, et intégrité des modèles de contrôle d'accès. La contribution portant sur la protection de la vie privée intègre l'usage de l'IoD disposant en son sein d'un système de contrôle d'accès qui garantit l'intégrité de l'information. Le modèle DORBAC ainsi proposé est conçu autour du contexte géo-temporel en plus de la confiance.

L'ensemble des modèles a été implémenté dans des environnements intégrant la technologie WebRTC. Cette dernière a fait l'objet d'une de nos contributions, afin de justifier de son choix. Nous avons utilisé la logique T-JClassic pour la description axiomatique des modèles et le langage UML pour la représentation des diagrammes permettant de décrire des processus.

Malgré son résultat exceptionnel, le modèle SVR présente une faible tolérance au bruit, notamment pour la sélection des vecteurs de support. En perspectives, nous voudrions travailler sur la prédiction de la marge d'erreur de confiance. Nous nous pencherons également sur les questions de disponibilité et de suspension de l'objet de la délégation. Nous travaillerons aussi sur la notion de véracité de l'information fournie pour évaluer la confiance.

Annexes

Analyse des contributions produites dans le cadre de cette thèse

Les résultats obtenus dans cette thèse ont fait l'objet de 5 publications dont :

Une publication dblp & Springer

1. Seyed C., Ouya S., Ngo Bilong J.R. (2018) Proposal for a Mapping Mechanism Between an E-Learning Platform Users and WebRTC. In: Auer M., Tsiatsos T. (eds) Interactive Mobile Communication Technologies and Learning. IMCL 2017. Advances in Intelligent Systems and Computing, vol 725.

https://link.springer.com/chapter/10.1007/978-3-319-75175-7_91
https://doi.org/10.1007/978-3-319-75175-7_91

Quatre publications Springer Verlag

2. Seyed C., Bilong J.R.N., Ouya S., Nanne M.F., Niang I. (2019) Scalability and Performance Testing of an E-Learning Platform Integrating the WebRTC Technology: Scenario "Authentication". In: Auer M., Tsiatsos T. (eds) The Challenges of the Digital Transformation in Education. ICL 2018. Advances in Intelligent Systems and Computing, vol 916.

https://link.springer.com/chapter/10.1007/978-3-030-11932-4_19
https://doi.org/10.1007/978-3-030-11932-4_19

3. Bilong J.R.N., Seyed C., Mendy G., Ouya S., Gaye I. (2019) Proposal of a Dynamic Access Control Model Based on Roles and Delegation for Intelligent Systems Using Realm. In: Auer M., Tsiatsos T. (eds) The Challenges of the Digital Transformation in Education. ICL 2018. Advances in Intelligent Systems and Computing, vol 916.

https://link.springer.com/chapter/10.1007/978-3-030-11932-4_38
https://doi.org/10.1007/978-3-030-11932-4_38

4. Ngo Bilong J.R., Gueye K., Mendy G., Ouya S. (2019) Access Control Model Based on Dynamic Delegations and Privacy in a Health System of Connected Objects. In: Mendy G., Ouya S., Dioum I., Thiaré O. (eds) e-Infrastructure and e-Services for Developing

Countries. AFRICOMM 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 275.

https://link.springer.com/chapter/10.1007/978-3-030-16042-5_11
https://doi.org/10.1007/978-3-030-16042-5_11

5. Bilong, J. R. N., Paco Sie, A. I., Mendy, G., Seyed, C., Ouya, S., Diop, P. S., & Sow, D. (2019, September). Proposal of the objective function of trust for the dynamic delegation and automatic revocation of roles

Acceptée et présentée (Best paper award à l'Intercontinental Bangkok ICL2019 Thaïlande)

https://www.conftool.com/iclconference/index.php?page=browseSessions&print=head&doprint=yes&form_session=242&presentations=show

1. Tests de montée en charge et de performance d'une plate-forme e-learning intégrant la technologie WebRTC grâce à JMeter (Cheikhane et al 2018)

Dans le cadre de nos travaux de recherche, nous avons procédé à une contribution en amont des tests de performance des outils utilisés pour implémenter les plateformes aidant à la collaboration et à la communication en temps réel. A cet effet, nous avons fait des tests de montée en charge et de performance d'une plateforme intégrant la technologie. Ladite plateforme est dédiée à l'e-learning et disposant des classes virtuelles dans lesquelles un nombre limité de cinquante étudiants peut se connecter simultanément. L'enjeu des tests revient à garantir de la disponibilité du serveur d'application de telles plateformes. Pour cela, nous avons procédé à une simulation avec des utilisateurs virtuels respectivement par groupe de 10, 50, 100 et 200. Malgré le stress qu'a subit ladite plateforme avec une montée en charge de jusqu'à 200 utilisateurs virtuels, le serveur est resté disponible et a réagi aux requêtes des utilisateurs. De plus, le temps de latence s'est réduit au fur et à mesure que le nombre d'utilisateurs virtuels a drastiquement augmenté. Seulement, la gestion du contrôle d'accès dans une telle application reste biaisée car, la complexité de l'authentification des profils côté signalisation WebRTC et coté application web (plateforme e-learning) ne permet pas d'identifier les sujets connectés. Pour y remédier, nous avons envisagé la contribution portant sur le mapping des utilisateurs des plateformes intégrant la technologie WebRTC.

2. Proposition d'un mécanisme mapping des utilisateurs de plateforme e-learning et WEBRTC (Seyed C. et al. 2018) :

Le système d'enseignement supérieur utilise des extensions ou des portails avec des tâches précises dans le processus pédagogique. Cette matérialisation du système d'enseignement supérieur en ligne pose un problème d'adaptation au processus pédagogique du fait qu'il requiert des configurations supplémentaires et souvent compliquées dans certains cas pour les utilisateurs.

Le challenge de cette contribution consiste en la gestion des profils utilisateurs d'un système complexe intégrant les applications WebRTC dans une plateforme e-learning. Ce système intègre deux profils pour un utilisateur à savoir un profil signalisation WebRTC et un profil e-learning web. De ce fait, nous avons proposé un mécanisme automatique de gestion de mapping de ces profils afin de faciliter l'authentification des utilisateurs.

Pour ce faire, nous avons proposé un algorithme permettant de fusionner un utilisateur de la plateforme e-learning et son correspondant du côté signalisation (WebRTC) dans une structure logique combinant les informations qui offrant la possibilité de réagir sur l'ensemble des services du processus pédagogique.

Pour montrer la faisabilité et l'utilité de notre approche, nous avons implémenté ce mécanisme sous forme d'un plugin masquant les complexités liées aux configurations des profils dans un système d'enseignement supérieur en ligne. Nous y avons intégré également un contrôleur de service qui permet à l'utilisateur logique de gérer parallèlement la sécurité ainsi que les services offerts par la technologie WebRTC.

Les résultats de cette contribution ont abouti à l'authentification des utilisateurs connectés sur cette plateforme. L'authentification étant un élément important dans la gestion des autorisations, cette contribution nous a permis d'évoluer vers la proposition des modèles de contrôle d'accès dynamiques de telles plateformes.

3. Proposition d'un modèle de contrôle d'accès dynamique basé sur les rôles et la délégation pour les systèmes intelligents utilisant Realm (Bilong J. et al. 2019) :

La revue de la littérature sur les modèles de contrôle d'accès révèle que le modèle RBAC est un modèle de contrôle d'accès statique à partir du quel plusieurs modèles dérivés (modèles dynamiques) ont été conçus. JEE Security repose sur le modèle de contrôle d'accès RBAC. A cet effet, la gestion des mises à jour des politiques de contrôle d'accès des applications web développées sous JEE s'avère difficile. Ainsi, la redéfinition ou modification des privilèges d'accès nécessite l'intervention du programmeur qui devra modifier le code source. En cas d'omission de mise à jour des politiques d'accès, un sujet démissionnaire ou licencié dans l'entreprise pourrait continuer d'agir illégitimement sur les données. De plus, l'aspect statique alourdit les procédures de contrôle d'accès. Pour parer à cette limite, nous avons proposé le modèle RDBDAC pour la gestion dynamique du contrôle d'accès basé sur les rôles. Ce dernier permet de corriger le côté statique du modèle RBAC dans « Java EE Security Realm » et permet d'implémenter une interface conviviale permettant de gérer les rôles de manière dynamique, sans avoir recours à la modification du code.

Le modèle RDBDAC met l'accent sur les paramètres tels que le niveau de confiance, la délégation et le contexte temporel. Une vue « administrateur » permet d'attribuer aisément des rôles aux tuteurs et aux enseignants.

La protection de la vie privée et l'appréciation de la confiance ne sont pas mises en exergue dans cette contribution. Compte tenu de l'importance qu'il y a à protéger les informations personnelles d'un sujet et à garantir une délégation fiable de rôle, nous avons proposé dans les contributions 4 et 5 ci-dessous des modèles qui gèrent respectivement la protection de la vie privée et la prédiction des erreurs de confiance en vue d'une délégation de rôle.

4. Modèle de contrôle d'accès basé sur les délégations dynamiques et la confidentialité dans un système de santé d'objets connectés (Bilong J. et al. 2019) :

Le besoin de contrôle d'accès dynamique dans les systèmes de plus en plus complexes et connectés requiert la prise en compte de la protection de la vie privée des sujets. La contribution porte sur la protection de la vie privée des sujets dans un environnement connecté e-santé. L'architecture que nous avons proposée permet de stocker les informations personnelles du patient sans une intervention manuelle.

Le modèle proposé DORBAC (Delegation and Organisation Based Access Control) autorise le médecin traitant à accéder aux informations stockées du patient. Ces informations sont recueillies par les capteurs et acheminées via la Raspberry pour stockage dans le serveur de base de données. La Raspberry fonctionne avec le système d'exploitation Raspbian de Debian GNU/linux. Ce système intègre les modèles de contrôle d'accès MAC et RBAC pour assurer la sécurité des données transmises. Le médecin traitant est assigné à un contexte géographique précis (poste de santé rural) et ne peut avoir accès qu'aux informations des patients de cette localité.

Pour des besoins de travail collaboratif, le médecin traitant peut déléguer son rôle ou une partie de son rôle à un autre médecin pour obtenir son avis sur le cas du patient. Le médecin en question doit avoir au préalable l'autorisation du patient lui donnant le droit d'accès à toutes ses informations durant une période déterminée. Au cas contraire, le médecin n'aura accès qu'aux données du patient, sans connaître son identité.

La contribution ainsi décrite limite les risques d'erreurs de saisie lors du stockage de l'information par l'agent de santé (infirmier, assistant médical…). De plus, la vie privée du sujet est préservée.

Seulement, toutes les contributions présentées jusqu'ici n'ont pas traité de l'évaluation de la confiance. Cette dernière est une notion très significative dans la gestion des délégations de

rôle. D'où l'intérêt de mettre en place un modèle de contrôle d'accès intégrant l'évaluation de la confiance.

5. Proposition de la fonction objectif de confiance pour la délégation dynamique et la révocation automatique des rôles (Bilong J. et al. 2019) :

L'ensemble de nos contributions précédentes portent sur les modèles de contrôle d'accès basés sur la délégation. A cet effet, nous avons trouvé opportun de développer une notion essentielle qu'est la confiance.

Ce papier porte sur l'amélioration du modèle RDBDAC. Le modèle proposé permet de gérer la délégation dynamique des rôles tout en évaluant les critères de définition et d'appréciation de la confiance. De plus, il améliore le système de révocation automatique de la délégation des rôles en fonction des cas d'exceptions.

Dans ce papier, l'approche consiste à modéliser le processus de sélection des candidats. Pour y arriver, nous avons travaillé sur deux modèles d'apprentissage automatique à savoir le modèle de régression linéaire et le modèle SVR. Ce dernier, propose des coefficients qui permettent de prédire les erreurs de recrutement d'un tuteur. Selon le recueil de l'existant, ce recrutement est basé sur l'évaluation d'un ensemble de critères non pondérés. Les résultats de la prédiction permettent à partir d'un algorithme que nous avons proposé, de réaliser un score, afin de déterminer le tuteur (délégataire) le plus digne de confiance.

La contribution de cette méthode limite la pratique de la délégation basée sur un sentiment personnel au profit de la délégation basée sur une appréciation neutre et impartiale.

Contribution connexe

6. Diop P.S., Mbacké A.B., Mendy G., Gaye I., Bilong J.R.N. (2019) Optimisation of Energy Consumption in Traffic Video Monitoring Systems Using a Learning-Based Path Prediction Algorithm. In: Palattella M., Scanzio S., Coleri Ergen S. (eds) Ad-Hoc, Mobile, and Wireless Networks. ADHOC-NOW 2019. Lecture Notes in Computer Science, vol 11803.

https://link.springer.com/chapter/10.1007/978-3-030-31831-4_26

https://doi.org/10.1007/978-3-030-31831-4_26

Références

[1] M. D. Edgard, « Titre : Contribution Aux Stratégies De Partage Et D'accès Dans Les Organisations Virtuelles : Application À La Mutualisation De Ressources Pédagogiques Universitaires En Ligne », p. 177.

[2] S. Sene *et al.* , « Comité de lecture et de correction », p. 325, 2015.

[3] « Présentation ENO », *Université virtuelle du Sénégal*. https://www.uvs.sn/eno-de-luvs/presentation-eno/ (consulté le nov. 04, 2019).

[4] A. Ndiaye, « Tableau de bord au 30 septembre 2018 », p. 17, 2018.

[5] C. P. Pfleeger et S. L. Pfleeger, *Security in Computing*, 3rd éd. Prentice Hall Professional Technical Reference, 2002.

[6] M. Ennahbaoui, « Contributions aux contrôles d'accès dans la sécurité des systèmes d'information », 2016.

[7] K. Laudon et J. Laudon, *Les systèmes d'information de gestion: organisations et réseaux stratégiques, éditions*. Pearson Education (Canada), 2001.

[8] G. Goncalves et F. Hémery, « Des cas d'utilisation en UML à la gestion de rôles dans un système d'information. », in *INFORSID*, 2000, p. 367–379.

[9] F. Large, « Navigation autonome d'un robot mobile en environnement dynamique et incertain », PhD Thesis, 2003.

[10] R. S. Sandhu et P. Samarati, « Access Control: Principles and Practice », p. 21.

[11] L. Bloch, « Les systèmes d'exploitation des ordinateurs », p. 485.

[12] C. D. Jensen, « Un modèle de contrôle d'accès générique et sa réalisation dans la mémoire virtuelle répartie unique Arias », oct. 1999, Consulté le: sept. 25, 2019. [En ligne]. Disponible sur: https://tel.archives-ouvertes.fr/tel-00004841.

[13] K. Rihaczek, « The harmonized ITSEC evaluation criteria », *Computers & Security*, vol. 10, nº 2, p. 101-110, avr. 1991, doi: 10.1016/0167-4048(91)90003-V.

[14] J. Briffaut, « Formalisation et garantie de propriétés de sécurité système: application à la détection d'intrusions », p. 204.

[15] R. L. Rivest, A. Shamir, et L. Adleman, « A Method for Obtaining Digital Signatures and Public-key Cryptosystems », *Commun. ACM*, vol. 21, nº 2, p. 120–126, févr. 1978, doi: 10.1145/359340.359342.

[16] C. P. Schnorr, « Efficient signature generation by smart cards », *J. Cryptology*, vol. 4, nº 3, p. 161-174, janv. 1991, doi: 10.1007/BF00196725.

[17] K. Kawabata, T. Nakamura, et E. Fukuda, « Estimating velocity using diversity reception », in *Proceedings of IEEE Vehicular Technology Conference (VTC)*, juin 1994, p. 371-374 vol.1, doi: 10.1109/VETEC.1994.345101.

[18] V. Nicomette, « La protection dans les systèmes à objets répartis », déc. 1996, Consulté le: sept. 25, 2019. [En ligne]. Disponible sur: https://tel.archives-ouvertes.fr/tel-00175252.

[19] A. A. E. Kalam *et al.*, « ORBAC : un modèle de contrôle d'accès basé sur les organisations », p. 12.

[20] M. Zerkouk, « Modèles de contrôle d'accès dynamiques », Thesis, University of sciences and technology in Oran, 2015.

[21] R. Thion, « structuration relationnelle des politiques de contrôle d'accès représentation, raisonnement et vérification logiques », PhD Thesis, Université Paul Sabatier Toulouse, 2008.

[22] B. Lampson, « A Note on the Confinement Problem », janv. 1973, Consulté le: sept. 25, 2019. [En ligne]. Disponible sur: https://www.microsoft.com/en-us/research/publication/a-note-on-the-confinement-problem/.

[23] M. A. Abakar, « Etude et mise en oeuvre d'une architecture pour l'authentification et la gestion de documents numériques certifiés : application dans le contexte des services en ligne pour le grand public », thesis, Saint-Etienne, 2012.

[24] A. A. E. Kalam, Y. Deswarte, et G. Trouessin, « Une d´emarche m´ethodologique pour l'anonymisation de donn´ees personnelles sensibles », p. 27.

[25] I. Ray et M. Toahchoodee, « A Spatio-temporal Role-Based Access Control Model », in *Data and Applications Security XXI*, vol. 4602, S. Barker et G.-J. Ahn, Éd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, p. 211-226.
[26] « BiblioComaCeline2005 (2).pdf ». .
[27] F. Autrel, F. Cuppens, et N. Cuppens, « MotOrBAC 2 : a security policy tool », 2008.
[28] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, et C. E. Youman, « Role-based access control models », *IEEE Computer*, 1996.
[29] R. K. Thomas et R. S. Sandhu, « Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management », in *Database Security XI: Status and Prospects*, T. Y. Lin et S. Qian, Éd. Boston, MA: Springer US, 1998, p. 166-181.
[30] E. Bertino, B. Catania, M. L. Damiani, et P. Perlasca, « GEO-RBAC: A Spatially Aware RBAC », p. 9.
[31] K. Jayaraman, V. Ganesh, M. Tripunitara, M. C. Rinard, et S. J. Chapin, « ARBAC Policy for a Large Multi-National Bank », *arXiv:1110.2849 [cs]*, oct. 2011, Consulté le: août 06, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1110.2849.
[32] R. Sandhu et Q. Munawer, « The ARBAC99 model for administration of roles », in *Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99)*, déc. 1999, p. 229-238, doi: 10.1109/CSAC.1999.816032.
[33] S. Hotomski et M. Glinz, « GuideGen: A Tool for Keeping Requirements and Acceptance Tests Aligned », in *Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings*, New York, NY, USA, 2018, p. 49–52, doi: 10.1145/3183440.3183484.
[34] E. Bertino, S. Castano, E. Ferrari, et M. Mesiti, « Specifying and enforcing access control policies for XML document sources », *World Wide Web*, vol. 3, nº 3, p. 139-151, nov. 2000, doi: 10.1023/A:1019289831564.
[35] S.-H. Park, Y.-J. Han, et T.-M. Chung, « Context-Role Based Access Control for Context-Aware Application », in *High Performance Computing and Communications*, 2006, p. 572-580.
[36] « Managing Delegation in Access Control Models - IEEE Conference Publication ». https://ieeexplore.ieee.org/abstract/document/4426056 (consulté le sept. 25, 2019).
[37] T. Sans et F. Cuppens, « Nouvelles Problématiques de Contrôle d'Usage dans les Systèmes d'Information », p. 13.
[38] A. A. E. Kalam, « Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales », déc. 2003, Consulté le: sept. 25, 2019. [En ligne]. Disponible sur: https://tel.archives-ouvertes.fr/tel-00012162.
[39] A. BAINA, « approche pour le controle d'accès collaboratif dans les infrastructures critiques ».
[40] J. Goepel, « Upholding public trust: an examination of teacher professionalism and the use of Teachers' Standards in England », *Teacher Development*, vol. 16, nº 4, p. 489-505, nov. 2012, doi: 10.1080/13664530.2012.729784.
[41] D. Gambetta, « Can We Trust Trust? », p. 17.
[42] T. Grandison et M. Sloman, « A survey of trust in internet applications », *IEEE Communications Surveys Tutorials*, vol. 3, nº 4, p. 2-16, Fourth 2000, doi: 10.1109/COMST.2000.5340804.
[43] S. Chakraborty et I. Ray, « TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems », in *Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies*, New York, NY, USA, 2006, p. 49–58, doi: 10.1145/1133058.1133067.
[44] M. Toahchoodee, R. Abdunabi, I. Ray, et I. Ray, « A Trust-Based Access Control Model for Pervasive Computing Applications », in *Data and Applications Security XXIII*, 2009, p. 307-314.
[45] I. Ray, I. Ray, et S. Chakraborty, « An interoperable context sensitive model of trust », *J Intell Inf Syst*, vol. 32, nº 1, p. 75-104, févr. 2009, doi: 10.1007/s10844-007-0049-9.
[46] « Framework for role-based delegation models - IEEE Conference Publication ». https://ieeexplore.ieee.org/abstract/document/898870 (consulté le sept. 25, 2019).
[47] M. Li, X. Sun, H. Wang, et Y. Zhang, « Multi-level delegations with trust management in access control systems », *J Intell Inf Syst*, vol. 39, nº 3, p. 611-626, déc. 2012, doi: 10.1007/s10844-012-0205-8.

[48] J. R. N. Bilong, C. Seyed, G. Mendy, S. Ouya, et I. Gaye, « Proposal of a Dynamic Access Control Model Based on Roles and Delegation for Intelligent Systems Using Realm », in *The Challenges of the Digital Transformation in Education*, 2020, p. 398-409.
[49] A. F. A. Dafa-Alla, G. Sohn, et K. H. Ryu, « Employing PRBAC for Privacy Preserving Data Publishing », in *Proceedings of the 2Nd International Conference on Interaction Sciences: Information Technology, Culture and Human*, New York, NY, USA, 2009, p. 1416–1421, doi: 10.1145/1655925.1656186.
[50] F. Baader, I. Horrocks, et U. Sattler, « Chapter 3 Description Logics », in *Foundations of Artificial Intelligence*, vol. 3, F. van Harmelen, V. Lifschitz, et B. Porter, Éd. Elsevier, 2008, p. 135-179.
[51] B. Nebel et C. Rich, *Principles of Knowledge Representation and Reasoning: Proceedings of the Third International Conference (KR '92)*. M. Kaufmann, 1992.
[52] L. Padgham et B. Nebel, « Combining classification and nonmonotonic inheritance reasoning: A first step », in *Methodologies for Intelligent Systems*, 1993, p. 132-141.
[53] « Extending Conceptual Definitions with Default Knowledge - Coupey - 1997 - Computational Intelligence - Wiley Online Library ». https://onlinelibrary.wiley.com/doi/abs/10.1111/0824-7935.00040 (consulté le sept. 25, 2019).
[54] N. Boustia et A. Mokhtari, « JClassic δε+ A Description Logic Reasoning Tool: Application to Dynamic Access Control », in *Proc. The Second International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking, Computation Tools*, 2011, vol. 11, p. 25–30.
[55] N. Chleq, « Contribution à l'étude du raisonnement temporel. Résolution avec contraintes et application à l'abduction en raisonnement temporel », p. 202.
[56] P. D. Loor, « Raisonnement Temporel La logique de ALLEN », p. 58.
[57] A. Artale, R. Kontchakov, V. Ryzhikov, et M. Zakharyaschev, « Past and Future of DL-Lite », présenté à Twenty-Fourth AAAI Conference on Artificial Intelligence, juill. 2010, Consulté le: sept. 25, 2019. [En ligne]. Disponible sur: https://www.aaai.org/ocs/index.php/AAAI/AAAI10/paper/view/1608.
[58] O. Bettaz, N. Boustia, et A. Mokhtari, « Extending nonmonotonic description logic with temporal aspects », in *2013 IEEE INISTA*, juin 2013, p. 1-5, doi: 10.1109/INISTA.2013.6577615.
[59] O. Bettaz, N. Boustia, et A. Mokhtari, « Dynamic Delegation Based on Temporal Context », *Procedia Computer Science*, vol. 96, p. 245-254, janv. 2016, doi: 10.1016/j.procs.2016.08.137.
[60] A. Ahadipour et M. Schanzenbach, « A Survey on Authorization in Distributed Systems: Information Storage, Data Retrieval and Trust Evaluation », in *2017 IEEE Trustcom/BigDataSE/ICESS*, août 2017, p. 1016-1023, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.346.
[61] Z. Wang, M. Ritou, C. M. Da Cunha, et B. FURET, « Classification contextuelle pour système d'aide à la décision pour machines-outils », Les Karellis, France, avr. 2019, Consulté le: sept. 28, 2019. [En ligne]. Disponible sur: https://hal.archives-ouvertes.fr/hal-02100713.
[62] S. Giguère, « Algorithmes d'apprentissage automatique pour la conception de composés pharmaceutiques et de vaccins », 2015.
[63] J. Jacques, « Fouille de données », p. 93.
[64] A. Léon, « Apprentissage séquentiel budgétisé pour la classification extrême et la découverte de hiérarchie en apprentissage par renforcement. », p. 127.
[65] « These Zaidenberg.pdf ». .
[66] D. Basak, S. Pal, et D. C. Patranabis, « Support vector regression », *Neural Information Processing-Letters and Reviews*, vol. 11, nº 10, p. 203–224, 2007.
[67] A. Makiou, « Sécurité des application Web: analyse, modélisation et détection des attaques par apprentissage automatique », p. 112.
[68] « demain internet des objets ». Consulté le: oct. 04, 2019. [En ligne]. Disponible sur: https://s3.eu-west-1.amazonaws.com/expopolis-4instance/magazines/MagazineN5-a3.pdf.
[69] I. Saleh, « Les enjeux et les défis de l'Internet des Objets (IdO) », *IdO*, vol. 17, nº 1, avr. 2017, doi: 10.21494/ISTE.OP.2017.0133.
[70] L. Touati, « Internet of things security: towards a robust interaction of systems of systems », p. 148.

[71] S. C. B. Intelligence, « Disruptive civil technologies », *Six technologies with potential impacts on US interests out to*, vol. 2025, 2008.
[72] Wenyuan Xu, Ke Ma, W. Trappe, et Yanyong Zhang, « Jamming sensor networks: attack and defense strategies », *IEEE Network*, vol. 20, nº 3, p. 41-47, mai 2006, doi: 10.1109/MNET.2006.1637931.
[73] « The-Internet-of-Things-2005.pdf ». Consulté le: nov. 27, 2019. [En ligne]. Disponible sur: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf.
[74] « Security Challenge for IoT_Turner.pdf ». .
[75] S. Gusmeroli, S. Piccione, et D. Rotondi, « A capability-based security approach to manage access control in the internet of things », *Mathematical and Computer Modelling*, vol. 58, nº 5-6, p. 1189–1205, 2013.
[76] G. Bianchi, A. T. Capossele, C. Petrioli, et D. Spenza, « AGREE: exploiting energy harvesting to support data-centric access control in WSNs », *Ad Hoc Networks*, vol. 11, nº 8, p. 2625-2636, nov. 2013, doi: 10.1016/j.adhoc.2013.03.013.
[77] J. Bethencourt, A. Sahai, et B. Waters, « Ciphertext-Policy Attribute-Based Encryption », in *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, mai 2007, p. 321-334, doi: 10.1109/SP.2007.11.
[78] P. N. Mahalle, B. Anggorojati, N. R. Prasad, et R. Prasad, « Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things », p. 41.
[79] B. Anggorojati, P. N. Mahalle, N. R. Prasad, et R. Prasad, « Capability-based Access Control Delegation Model on the Federated IoT Network », p. 6.
[80] P. N. Mahalle, P. A. Thakre, N. R. Prasad, et R. Prasad, « A fuzzy approach to trust based access control in internet of things », in *Wireless VITAE 2013*, 2013, p. 1–5.
[81] D. Ma, A. K. Prasad, N. Saxena, et T. Xiang, « Location-aware and safer cards: Enhancing RFID security and privacy via location sensing », p. 11.
[82] N. Saxena et J. Voris, « Still and silent: motion detection for enhanced RFID security and privacy without changing the usage model », in *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, 2010, p. 2–21.
[83] S. Brands et D. Chaum, « Distance-bounding protocols », in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1993, p. 344–359.
[84] « 2019 - La e-santé télésanté, santé numérique ou santé c.pdf ». .
[85] J. R. Ngo Bilong, K. Gueye, G. Mendy, et S. Ouya, « Access Control Model Based on Dynamic Delegations and Privacy in a Health System of Connected Objects », in *e-Infrastructure and e-Services for Developing Countries*, 2019, p. 108-119.
[86] C.-O. Truica, A. Boicea, et I. Trifan, « CRUD operations in MongoDB », 2013.
[87] Y. Cheng, J. Ren, Z. Wang, S. Mei, et J. Zhou, « Attributes union in cp-abe algorithm for large universe cryptographic access control », in *2012 Second International Conference on Cloud and Green Computing*, 2012, p. 180–186.
[88] Y. Cheng, Z. Wang, J. Ma, J. Wu, S. Mei, et J. Ren, « Efficient revocation in ciphertext-policy attribute-based encryption based cryptographic cloud storage », *Journal of Zhejiang University SCIENCE C*, vol. 14, nº 2, p. 85–97, 2013.
[89] A. N. Haidar et A. E. Abdallah, « Comparison and Evaluation of Identity Management in Three Architectures for Virtual Organizations », in *2008 The Fourth International Conference on Information Assurance and Security*, Naples, Italy, sept. 2008, p. 21-26, doi: 10.1109/IAS.2008.67.
[90] A. D. Gueye, D. E. Moussavou, S. Ouya, et C. Lishou, « Proposal of a standard mutual authentication system in a virtual organization », p. 9, 2013.
[91] P. C. Moore, W. R. Johnson, et R. J. Detry, « Adapting globus and kerberos for a secure ASCI grid », in *Proceedings of the 2001 ACM/IEEE conference on Supercomputing (CDROM) - Supercomputing '01*, Denver, Colorado, 2001, p. 21-21, doi: 10.1145/582034.582055.
[92] C. Seyed, J. R. N. Bilong, S. Ouya, M. F. Nanne, et I. Niang, « Scalability and Performance Testing of an E-Learning Platform Integrating the WebRTC Technology: Scenario "Authentication" », in *The Challenges of the Digital Transformation in Education*, vol. 916, M. E. Auer et T. Tsiatsos, Éd. Cham: Springer International Publishing, 2020, p. 186-193.

[93] M. G. Moore, W. G. Anderson, M. G. Moore, et W. G. Anderson, *Handbook of distance education*. 2003.
[94] « La formation à distance, un système complexe et compliqué ». https://edutice.archives-ouvertes.fr/edutice-00277820/file/a0609b.htm (consulté le oct. 29, 2019).
[95] M. Mirzakhani, H. Ashrafzadeh, et A. Ashrafzadeh, « The virtual university: Advantages and disadvantages », in *2010 4th International Conference on Distance Learning and Education*, oct. 2010, p. 32-36, doi: 10.1109/ICDLE.2010.5606048.
[96] H. Dridi et R. Chouinard, « La transformation de l'université : vers une université virtuelle », *RSE*, vol. 29, nº 2, p. 439-458, juill. 2005, doi: 10.7202/011041ar.
[97] D. Peraya, « De la correspondance au campus virtuel. Formation à distance et dispositifs médiatiques. », p. 20.
[98] S. Tachakra, X. H. Wang, R. S. H. Istepanian, et Y. H. Song, « Mobile e-health: the unwired evolution of telemedicine. », *Telemedicine journal and e-health : the official journal of the American Telemedicine Association*, vol. 9, nº 3, p. 247-257, 2003, doi: 10.1089/153056203322502632.
[99] O. Salem et A. Benzekri, « Towards End-to-End QoS in Ad Hoc Networks », p. 10.
[100] « Web APIs | WebRTC ». https://webrtc.org/web-apis/ (consulté le oct. 09, 2019).
[101] S. Loreto et S. P. Romano, « Real-Time Communications in the Web: Issues, Achievements, and Ongoing Standardization Efforts », *IEEE Internet Comput.*, vol. 16, nº 5, p. 68-73, sept. 2012, doi: 10.1109/MIC.2012.115.
[102] M. Phankokkruad et P. Jaturawat, « An evaluation of technical study and performance for real-time face detection using web real-time communication », in *2015 International Conference on Computer, Communications, and Control Technology (I4CT)*, 2015, p. 162–166.
[103] S. Ouya, C. Seyed, A. B. Mbacke, G. Mendy, et I. Niang, « WebRTC platform proposition as a support to the educational system of universities in a limited Internet connection context », in *2015 5th World Congress on Information and Communication Technologies (WICT)*, déc. 2015, p. 47-52, doi: 10.1109/WICT.2015.7489643.
[104] C. Jennings, T. Hardie, et M. Westerlund, « Real-time communications for the web », *IEEE Communications Magazine*, vol. 51, nº 4, p. 20-26, avr. 2013, doi: 10.1109/MCOM.2013.6495756.
[105] S. Holmer, M. Shemer, et M. Paniconi, « Handling packet loss in WebRTC », in *2013 IEEE International Conference on Image Processing*, Melbourne, Australia, sept. 2013, p. 1860-1864, doi: 10.1109/ICIP.2013.6738383.
[106] « Citeseer - Full Text PDF ». Consulté le: oct. 31, 2019. [En ligne]. Disponible sur: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.830.3793&rep=rep1&type=pdf.
[107] D. Nevedrov, « Using JMeter to Performance Test Web Services », p. 11.
[108] S. McKinney, « The Anatomy of a Secure Web App Using JavaEE, Spring Security and Apache Directory Fortress », p. 74, 2015.
[109] G. Piatetsky-Shapiro, « KDnuggets news on SIGKDD service award », *Avaible: http://www. kdnuggets. com/news*, nº 13, 2005.
[110] B. Garcia, L. Lopez-Fernandez, M. Gallego, et F. Gortazar, « Kurento: The Swiss Army Knife of WebRTC Media Servers », *IEEE Comm. Stand. Mag.*, vol. 1, nº 2, p. 44-51, 2017, doi: 10.1109/MCOMSTD.2017.1700006.
[111] C. Seyed, S. Ouya, et J. R. N. Bilong, « Proposal for a Mapping Mechanism Between an E-Learning Platform Users and WebRTC », in *Interactive Mobile Communication Technologies and Learning - Proceedings of the 11th IMCL Conference, 30 November - 1 December 2017, Mediterranean Palace Hotel, Thessaloniki, Greece*, 2017, vol. 725, p. 936–943, doi: 10.1007/978-3-319-75175-7_91.