Table des matières

RÉSUMÉ

Nom et Prénom : IMINE Abdessamad

Situation actuelle : MCF HdR (Hors Classe)
au Département Informatique, IUT Charlemagne, Université de Lorraine.

Diplômes :

2016 : Habilitation à Diriger des Recherches, Université de Lorraine.

2006 : Docteur en Informatique, Université UHP Nancy 1

Activités d'enseignement :

Université de Lorraine :

Matières : Programmation Web, Bases de Données, Réseaux, Sécurité, Algorithmique et Programmation, Programmation, ...
Volume : équivalent à plus de 3000h TD

Responsabilités :

Membre élu au pôle Automatique, Mathématiques, Informatique et leurs Interactions (AM2I).

Membre élu du Conseil de l'IUT Nancy Charlemagne.

Membre à la CMI (Commission de la Mention Informatique) au LORIA.

Co-Responsable du club étudiants-chercheurs "Economie, Finances, Numérique" (Orion, LUE)

Directeur des études - Filière Réseaux (BUT)

Membre du comité de sélection des ATER

Responsable de plusieurs unités d'enseignement.

Responsable de plusieurs projets de recherche.

Editeur à la revue "Information" (MDPI)

Encadrements : 10 co-encadrements de thèse de doctorat ; 2 encadrements de post-doc ; 5 encadrements de Master recherche.

Prime de recherche : PEDR 2014-2018.

Thèmes de recherche : Protection de la Vie Privée (Privacy) ; Sécurité ; Méthodes Formelles ; Réseaux Sociaux ; Systèmes collaboratifs ; Systèmes Distribués ; Synchronisation de Données ; Big Data ; Cryptomonnaies.

Publications :

19 journaux avec comité de lecture (18 internationaux et 1 national)

72 publications internationales (59 conférences et 13 workshops)

Co-auteur d'un ouvrage

Co-éditeur d'un ouvrage

3 chapitres d'ouvrage

7 publications dans des conférences nationales

3 articles publiés dans des magazines avec comité de lecture.

CURRICULUM VITÆ

2.1 Etat Civil

Nom et prénom	: IMINE Abdessamad
Adresse professionnelle 1	: LORIA Nancy-Grand Est, 615, rue du Jardin Botanique, BP 101, 54602 Villers les Nancy Cedex.
Adresse professionnelle 2	: IUT Charlemagne, Département Informatique, 2 Boulevard Charlemagne, 54052 Nancy Cedex.
Equipe de recherche	: Projet Pesto
Page Web	: https://members.loria.fr/AImine/
	: My Google Scholar
Adresse électronique	: Abdessamad.Imine@loria.fr
Téléphone	: 07 67 74 15 82
Fax	: 03 83 27 83 19

2.2 Activités Professionnelles

2007- : Maître de Conférences HdR (Hors Classe), Université de Lorraine, Nancy ;
2005-2007 : ATER au Département Informatique, Faculté des Sciences, UHP Nancy 1 ;
2003-2005 : ATER à l'UFR Maths-Info, Université Nancy 2 ;
2002-2003 : Chercheur visiteur dans le projet CASSIS du LORIA ;
2001-2002 : Chargé de Cours au Département Informatique, Faculté des Sciences, Université des Sciences et de la Technologie d'Oran (Algérie) ;
1999-2001 : Maître Assistant au Département Informatique, Faculté des Sciences, Université des Sciences et de la Technologie d'Oran (Algérie) ;
1997-1999 : Service Militaire ;
1995-1997 : Maître Assistant au Département Informatique, Faculté des Sciences, Université des Sciences et de la Technologie d'Oran (Algérie) ;

De 2015-2016 à 2017-2018, j'ai bénéficié **d'une demi-délégation INRIA** au sein de mon équipe Pesto. J'ai également bénéficié d'une PEDR en 2014.

2.3 Cursus d'Etudes

2016 : Habilitation à Diriger des Recherches.

- **Thème :** Partage de Données dans les Systèmes Collaboratifs. De la synchronisation à la protection de données.
- **Université :** Université de Lorraine, Nancy
- **Date :** 9 décembre 2016

- **Composition du jury :**
  - ⋆ Angela Bonifati, Professeur à l'Université Claude Bernard, Lyon 1 (**Rapporteur**)
  - ⋆ Frédéric Cuppens, Professeur à l'Ecole Télécom Bretagne (**Rapporteur**)
  - ⋆ Mohamed Mosbah, Professeur à l'Institut de Polytechnique de Bordeaux (**Rapporteur**)
  - ⋆ Sihem Amer-Yahia, Directrice de Recherche CNRS au LIG, Grenoble (**Examinateur**)
  - ⋆ Achour Mostefaoui, Professeur à l'Université de Nantes (**Examinateur**)
  - ⋆ Dominique Méry, Professeur à l'Université de Lorraine, Nancy (**Président**)
  - ⋆ Michaël Rusinowitch, Directeur de Recherche INRIA, Nancy (**Parrain**)

2003-2006 : Etudes Doctorales.

- **Thème :** Conception Formelle d'Algorithmes de Réplication Optimiste.Vers l'Edition Collaborative dans les Réseaux Pair-à-Pair (P2P).
- **Diplôme :** Docteur en Informatique
- **Mention :** Très Honorable
- **Université :** Université Henri Poincaré (UHP), Nancy 1
- **Date :** 11 décembre 2006
- **Composition du jury :**
  - ⋆ Jacques Julliand, Professeur à l'Université de Franche-Comté (**Président**)
  - ⋆ Jean Ferrié, Professeur à l'Université Montpellier II (**Rapporteur**)
  - ⋆ Jan-François Monin, Professeur à l'Université Joseph Fourrier Grenoble I (**Rapporteur**)
  - ⋆ Dominique Méry, Professeur à l'Université Henri Poincaré, Nancy 1 (**Examinateur**)
  - ⋆ Pascal Molli, Maître de Conférences à l'Université Henri Poincaré, Nancy 1 (**Examinateur**)
  - ⋆ Michaël Rusinowitch, Directeur de Recherche au LORIA (**Directeur de thèse**)

1992-1995 : Etudes en Post-Graduation.

- **Diplôme :** Magister en Informatique (équivalent 3ème cycle).
- **Mention :** Très Honorable.
- **Spécialité :** Génie Logiciel.
- **Thème :** Spécification et Analyse de Programmes Parallèles.
- **Directeur de thèse :** Yahya Slimani, Professeur à la Faculté des Sciences de Tunis.
- **Université :** Université des Sciences et de la Technologie d'Oran (Algérie).
- **Date :** 25 novembre 1995.

2.4 Domaines de Compétences

— Protection de la Vie Privée (Privacy)
— Contrôle d'Accès
— Sécurité
— Méthodes Formelles
— Réseaux Sociaux
— Systèmes collaboratifs
— Systèmes Distribués
— Synchronisation de Données
— Big Data
— Cryptomonnaies

ACTIVITÉS D'ENSEIGNEMENT

Cette partie est consacrée aux différentes responsabilités pédagogiques que j'ai assumées. Elle est principalement composée des sections suivantes :

— Enseignements en tant que Maître de Conférences : j'ai effectué plus de 3000h TD d'enseignements.

— Enseignements dans les universités françaises en tant que ATER : j'ai effectué approximativement 471h de TD (387h pour 1er Cycle et 84h pour 2ème Cycle).

— Enseignements dans l'université algérienne : j'ai effectué approximativement 813h de TD.

— Autres responsabilités.

Enfin, je vais présenter quelques propositions pour mes futurs enseignements.

3.1 Enseignements en tant que Maître de Conférences (2007-2023)

Dans cette section, je vais présenter les différentes unités d'enseignements que j'ai enseignées en tant que Maître de Conférences.

3.1.1 SQL dans un autre langage de programmation

Public : 2ème Année BUT - IUT Charlemagne
Volume : 32h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il propose des notions de manipulation à distance de bases de données via des langages de programmation tels que PLSQL, Java et PHP. Il comporte également les notions de base pour la conception des bases de données. Il est enseigné au 3ème semestre.

3.1.2 Programmation Web

Public : 2ème Année BUT - IUT Charlemagne
Volume : 40h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il comporte les notions de base pour la programmation web en utilisant le langage PHP. Il est enseigné au 3ème semestre.

3.1.3 Programmation Efficace

Public : 2ème Année BUT - IUT Charlemagne
Volume : 22h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il aborde des notions de structures de données (tables et arbres). Il traite également de la récursivité, la recherche avec retour arrière, et la programmation dynamique. Il est enseigné au 3ème semestre.

3.1.4 Qualité au delà du Relationnel - Parcours Ingénierie du Logiciel

Public : 2ème Année BUT - IUT Charlemagne
Volume : 24h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il aborde des notions avancées en bases de données, à savoir : les bases de données orientées objet, les transactions pour des accès concurrentiels, et les optimisations effectuées par les SGBD pour le stockage et l'accès aux tables. Il est enseigné au 4ème semestre.

3.1.5 Qualité au delà du Relationnel - Parcours Web et Mobile

Public : 2ème Année BUT - IUT Charlemagne
Volume : 24h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il aborde des notions avancées en bases de données dans un cadre purement web, à savoir : le mapping objet-relation en PHP, les transactions avec MySQL, et les optimisations de données en MySQL. Il est enseigné au 4ème semestre.

3.1.6 Qualité au delà du Relationnel - Parcours Réseaux

Public : 2ème Année BUT - IUT Charlemagne
Volume : 16h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il aborde des notions avancées en bases de données, à savoir : les transactions pour des accès concurrentiels, et les optimisations effectuées par les SGBD pour le stockage et l'accès aux tables. Il est enseigné au 4ème semestre.

3.1.7 Cryptographie et Sécurité - Parcours Réseaux

Public : 2ème Année BUT - IUT Charlemagne
Volume : 12h TD

C'est un **nouveau cours** dans le cadre du nouveau programme BUT. Il aborde les notions de chiffrement (asymétrique et symétrique), la gestion des certificats ainsi que la signature des documents semi-structurées. Il est enseigné au 4ème semestre.

3.1.8 Python pour les économistes

Public : 2ème Année Master 2 Economie de la régulation des marchés - Faculté de Droit
Volume : 12h TD

Ce cours a pour objectif d'initier des étudiants en économie à la programmation en Python. Il traite essentiellement de la collecte, la manipulation et la visualisation des données. Ce cours est enseigné au département sciences économiques de la Faculté de Droit.

3.1.9 Analyse et Conception des Systèmes d'Information (ACSI)

Public : 2ème Année DUT - IUT Charlemagne
Volume : 56h TD

L'enseignement de ce cours comporte : (i) L'étude des modèles et méthodes utilisés pour l'analyse et la conception des systèmes d'information (e.g. Merise et UML) ; (ii) La pratique d'outils et d'ateliers

permettant la mise en œuvre associée via des réalisations. Il est enseigné au 3ème semestre.

3.1.10 Systèmes de Gestion des Bases de Données (SGBD)

Public : 2ème Année DUT - IUT Charlemagne
Volume : 52h TD

Ce cours a pour but d'approfondir les connaissances en matière de SGBD. Il comporte : (i) La maîtrise des requêtes SQL et la programmation PL-SQL des procédures stockées ; (ii) L'étude des mécanismes de partage de données et de concurrence fournis par un SGBD dans un contexte où il y a plusieurs utilisateurs (e.g. transactions) ; (iii) L'étude des méthodes de stockage des données ainsi que les optimisations utilisées par un SGBD pour accéder rapidement aux données. Ce cours est enseigné au 3ème semestre.

3.1.11 Systèmes de Gestion des Bases de Données Avancées

Public : 2ème Année DUT - IUT Charlemagne
Volume : 20h TD

Ce cours traite des méthodes de sécurité utilisées pour protéger les données dans un SGBD. Il aborde également l'apprentissage du format XML comme un moyen pour stocker, questionner et formatter des bases de données. Ce cours est enseigné au 4ème semestre.

3.1.12 Algorithmique Avancée

Public : 2ème Année DUT - IUT Charlemagne
Volume : 30h TD

Ce cours aborde des notions avancées en algorithmique pour apprendre aux étudiants comment proposer des solutions algorithmiques "optimales" pour des problèmes donnés. Il traite de la récursivité, la recherche avec retour arrière, la programmation dynamique et les structures de données arborescentes. Ce cours est enseigné au 3ème semestre.

3.1.13 Cobol

Public : 1ère Année DUT - IUT Charlemagne
Volume : 40h TD

Ce cours est dédié à l'apprentissage du langage Cobol. Divers problèmes sont abordées, comme le parcours séquentiel ou indexé dans un fichier de données. Il est enseigné au 3ème semestre.

3.1.14 Réseaux

Public : 1ère Année DUT - IUT Charlemagne
Volume : 40h TD

Ce cours a pour objectif de comprendre les concepts de base dans les applications réseaux tels que : le transfert de l'information (support et topologie) et la gestion des communications (routage, adressage, ...). Il est enseigné au 2ème semestre.

3.1.15 Algorithmique

Public : 1ère Année DUT - IUT Charlemagne
Volume : 40h TD

Ce cours est dédié à l'apprentissage d'un langage algorithmique élémentaire de telle façon que l'étudiant puisse comprendre, organiser et concevoir une solution algorithmique d'un problème. Il est enseigné au 1er semestre.

3.1.16 Bases de la programmation

Public : 1ère Année DUT - IUT Charlemagne
Volume : 56h TD

Ce cours a pour objectif d'apprendre le langage orienté objet Java pour servir de support pratique au cours d'algorithmique. En effet, l'étudiant devra comprendre, organiser et concevoir une solution programmée d'un problème. Il est enseigné au 1er semestre.

3.1.17 Algorithmique-Programmation

Public : Année spéciale - IUT Charlemagne
Volume : 56h TD

Ce cours est dispensé pour des étudiants de niveau BAC+2 et pour des bénéficiaires de la formation continue. Il traite des notions fondamentales de l'algorithmique ainsi que la programmation orientée objet. Ce cours est enseigné au 1er semestre.

3.1.18 Programmation

Public : 1ère Année DUT - IUT Charlemagne
Volume : 56h TD

Ce cours aborde des notions avancées en programmation orientée objet telles que l'héritage, les patrons de conception, les API ainsi que les structures de données. Il est enseigné au 2ème semestre.

3.1.19 Bases de données et application

Public : 2ème Année DUT - IUT Charlemagne
Volume : 24h TD

Ce cours traite des techniques pour développer des sites web basés sur un SGBD. Il aborde également l'utilisation du langage PHP ainsi que l'environnement Eloquent pour simuler des bases de données orientées objets. Ce cours est enseigné au 4ème semestre.

3.1.20 Sécurité pour les données semi-structurées

Public : 1ère Année Master Sciences et Technologie (Informatique) - Facultés des Sciences
Volume : 6h Cours - 4h TD - 4h TP

Ce cours a pour objectif d'étudier les méthodes utilisées pour protéger des données semi-structurées dans des SGBD natifs et les web services, tels que le chiffrement et la signature. Ce cours est enseigné au département Informatique de la Faculté des Sciences.

3.2 Tableau récapitulatif des enseignements en tant que Maître de Conférences

Ce tableau donne un aperçu sur les enseignements que j'ai dispensés en tant que Maître de Conférences à l'Université de Lorraine.

Modules	Total		
	CM	TD	TP
SQL dans un autre langage		32h	
Programmation Web		40h	
Programmation Efficace		22h	
Qualité au delà du relationnel - Ingénierie du logiciel		24h	
Qualité au delà du relationnel - Mobile et Web		24h	
Qualité au delà du relationnel - Réseaux		16h	
Python pour les économistes		12h	
Cryptographie et Sécurité - Réseaux		12h	
Analyse et Conception des Systèmes d'Information		112h	
Systèmes de Gestion des Bases de Données		584h	
Systèmes de Gestion des Bases de Données Avancées		160h	
Algorithmique		320h	
Algorithmique avancée		198h	
Bases de la programmation		520h	
Réseaux		40h	
Bases de données et application		72h	
Algorithmique-Programmation		224h	
Programmation		112h	
Sécurité pour les données semi-structurées	38h	30h	32h
Cobol		120	
Projets tuteurés		84h	
Encadrements stages (Fin DUT, Licence professionnelle)		70h	
Encadrements Projet Ingénieur		60h	
Total	**36h**	**2930**	**32h**

En plus de la responsabilité de la gestion des projets tuteurés, j'encadre chaque année au moins deux groupes d'étudiants. Je supervise également des étudiants étrangers (venant principalement des universités tunisiennes) pour la préparation de leurs projets de fin d'études. Enfin, j'encadre régulièrement des étudiants en Master pour des projets d'initiation à la recherche. En général, ces projets sont portés sur mes thématiques de recherche.

Par ailleurs, j'ai également donné des séries de séminaires, entre 2009 et 2011, portant sur les problèmes de synchronisation de données partagées dans les systèmes collaboratifs (**Volume = 36h CM**).

3.3 Enseignements à l'université Henri Poincaré Nancy 1 (2005-2007)

Dans ce qui suit, je vais présenter les différentes unités d'enseignements que j'ai dispensées durant deux années en tant que demi ATER au Département Informatique, Faculté des Sciences, Université Henri Poincaré Nancy 1.

3.3.1 Bases de Données

Public : Etudiants en 1ère Année Master Information Numérique en Entreprise
(Faculté des Sciences - Nancy 1)
Volume : 18h de Cours, 20h de TD, 10h de TP

Ce cours est une introduction aux systèmes de gestion de bases de données. L'accent est mis sur le modèle relationnel. On étudie les langages de requêtes, l'algèbre et le calcul relationnel, et les standards SQL pour le relationnel.

3.3.2 Algorithmique-Programmation C

Public : Etudiants en 2ème Année Licence Sciences de la Matière (Faculté des Sciences - Nancy 1)
Volume : 24h de TD, 24h de TP

Cette série de TD et TP avait pour but de permettre aux étudiants de maîtriser les concepts et les méthodes de la programmation structurée, et d'utiliser des méthodes de développement (commentaire et lisibilité du texte source, modularité : interfaces et profils). Le langage de programmation utilisé est le langage C.

3.3.3 Informatique

Public : Etudiants en 2ème Année Licence Sciences de la Matière (**Antenne Bar-le-Duc**)
Volume : 12h de Cours, 12h de TD, 12h de TP

L'objectif de ce cours est de permettre aux étudiants de se familiariser avec le modèle de la programmation fonctionnelle dans lequel la brique de base est la fonction. Le langage utilisé est Ocaml. Cette utilisation est faite à travers des modélisations mathématiques ainsi que des mises en œuvre de structures de données classiques en informatique (listes, arbres, graphes).

3.3.4 Système de Gestion des Bases de Données

Public : Etudiants en 3ème Année Licence Maths-Info
Volume : 18h de TD

Cette série de TD avait pour objectif d'apprendre aux étudiants la conception de requêtes en algèbre relationnelle et leur mise en œuvre en SQL.

3.4 Enseignements à l'université Nancy 2 (2003-2005)

Cette section présente les différentes charges pédagogiques que j'ai eues durant deux années en tant que ATER[1] à l'UFR Maths-Info de l'université Nancy 2.

3.4.1 Informatique

Public : Etudiants en 1ère Année DEUG Sciences du Langage
Volume : 39h de TD

Au premier semestre, 13h sont consacrées pour initier les étudiants à l'utilisation efficace des ordinateurs (système d'exploitation ainsi que des outils de bureautique). Au second semestre, 26h sont destinées

1. ATER à temps plein en 2003-2004 et ATER à mi-temps en 2004-2005.

à l'initiation de l'algorithmique et la programmation. Comme langage de programmation, nous utilisons le langage Pascal.

3.4.2 Certificat Informatique et Internet (C2i)

Public : Etudiants en 1ère Année DEUG Misashs et d'autres DEUG
Volume : 54h de TD

C'est un cours qui vise à développer, renforcer et valider la maitrise des technologies de l'information et de la communication par les étudiants en formation universitaire. Il est scindé en deux niveaux : le premier niveau consiste à initier les étudiants à la maitrise des outils informatiques pour la recherche, la création, la manipulation, et la gestion de l'information. Quant au deuxième niveau, il se base sur la préparation de documents complexes, la création d'un travail collaboratif et la présentation assistée par ordinateur.

3.4.3 Outils de Base

Public : Etudiants en 1ère Année MIAGE-IUP
Volume : 15h de TD
Le but de ces travaux dirigés est de familiariser les nouveaux étudiants avec les ordinateurs. A ce titre il fallait vulgariser le vocabulaire informatique pour comprendre le fonctionnement de base d'un ordinateur, être capable de classer et d'organiser efficacement ses dossiers, apprendre à utiliser les systèmes d'exploitation MS-Windows, et enfin utiliser tous les outils de bureautique (traitement de textes, tableur et bases de données).

3.4.4 Outils Informatique

Public : Etudiants en 1ère Année DEUG MISASH
Volume : 104h de TD

En premier semestre, les étudiants reçoivent des notions de base leur permettant un bon usage des outils informatiques. De nombreuses notions sont abordées de manière plus ou moins approfondie selon leur intérêt pratique, afin de faire acquérir une compréhension générale du fonctionnement d'un ordinateur, ainsi qu'une maîtrise des outils indispensables à leur cursus. En second semestre, les étudiants reçoivent un cours d'algorithmique et de programmation en VBA (Visual Basic Application), intégré à Excel.

3.4.5 Algorithmique et Programmation

Public : Etudiants en Formation Continue
Volume : 12h de cours et 12h de TD
Ce cours est une initiation à l'algorithmique et la programmation en Java. Il est organisé selon les structures de données et les méthodes de programmation utilisées dans différents algorithmes. Ainsi sont considérés successivement les tableaux, les listes, les piles et les files.

3.5 Tableau récapitulatif des enseignements aux universités françaises

Ce tableau donne un aperçu sur les enseignements que j'ai dispensés en tant que ATER dans les universités françaises.

Modules	Total		
	CM	TD	TP
Outils de Base (Nancy 2)		15h	
Outils Informatiques (Nancy 2)		104h	
Informatique (Nancy 2)		78h	
Algorithmique (Nancy 2)	12h	12h	
C2I (Nancy 2)		54h	
Informatique (LSM - UHP Nancy 1)	12h	12h	12h
Algorithmique-Programmation C (UHP Nancy 1)		48h	48h
Système de Gestion des Bases de Données (UHP Nancy 1)		18h	
Bases de Données (Master INE - UHP Nancy1)	18h	20h	10h
Total	**42h**	**361h**	**70h**

3.6 Enseignements donnés durant la période (1995-2002)

J'ai commencé à enseigner au sein du Département Informatique de l'Université des Sciences et de la Technologie d'Oran (USTO) à partir de 1995. Depuis cette date, j'ai assuré des cours, des TD et des TP. Avant de détailler ces enseignements, il faut souligner que le Département Informatique de l'USTO dispose de deux cycles de formation, à savoir :

— Le *cycle court* se fait en trois années et est sanctionné par un Diplôme d'Etudes Universitaires Appliquées (DEUA). Cette formation est similaire à un BTS en France.

— Le *cycle long* dure cinq années et concerne la formation des ingénieurs d'état en informatique.

3.7 Autres responsabilités pédagogiques

J'ai pris d'autres responsabilités pédagogiques qui se déclinent comme suit :

— Membre élu du conseil de l'IUT Nancy Charlemagne.

— Directeur des études (Filière Réseaux) en BUT, département Informatique de l'IUT Nancy Charlemagne (responsabilité nouvellement prise).

— Membre dans le comité de sélection des ATERs.

— Responsable des projets tuteurés au département informatique de l'IUT Charlemagne (2010-2014).

— Responsable du SAÉ "Exploration algorithmique d'un problème" dans le cadre du nouveau programme Bachelor Universitaire de Technologie (BUT).

— Responsable du nouveau cours "SQL dans un autre langage", dispensé en deuxième année BUT au département informatique de l'IUT Charlemagne.

— Responsable du nouveau cours "Qualité au delà du relationnel", dispensé en deuxième année BUT, filière Ingénierie du Logiciel, au département informatique de l'IUT Charlemagne.

— Responsable du nouveau cours "Qualité au delà du relationnel", dispensé en deuxième année BUT, filière Mobile et Web, au département informatique de l'IUT Charlemagne.

— Responsable du nouveau cours "Qualité au delà du relationnel", dispensé en deuxième année BUT, filière Réseaux, au département informatique de l'IUT Charlemagne.

— Responsable du nouveau cours "Cryptographie et Sécurité", dispensé en deuxième année BUT, filière Réseaux, au département informatique de l'IUT Charlemagne.

— Responsable du nouveau cours “Python pour les économistes” dans le cadre du Master M2 Economie et régulation des marchés, de la faculté de droit de l’université de Lorraine.

— Responsable d’un cours intitulé “Sécurité pour les données XML” dans le cadre du Master M1 en Informatique de la faculté des sciences de l’université de Lorraine.

— De 2010 à 2022, j’étais responsable du module “Systèmes de Gestion des Bases de Données” dispensé en deuxième année DUT au département informatique de l’IUT Charlemagne.

— En 2014, j’étais responsable du module “Systèmes de Gestion des Bases de Données Avancées” dispensé en deuxième année DUT au département informatique de l’IUT Charlemagne.

— J’étais responsable du module “Bases de la programmation” dispensé en première année DUT au département informatique de l’IUT Charlemagne.

— J’étais responsable du module “Algorithmique-Programmation” dispensé aux étudiants de l’année spéciale au département informatique de l’IUT Charlemagne.

— 1999-2002 : j’étais membre du conseil scientifique de la Faculté des Sciences à l’Université d’Oran (Algérie).

3.8 Autres activités pédagogiques

— J’ai participé à l’adaptation du contenu de mes cours par rapport aux différentes directives des Programmes Pédagogiques Nationaux (PPN) pour le DUT Informatique et notamment les nouvelles directives du Bachelor Universitaire de Technologie (BUT).

— J’ai monté cinq (05) nouveaux cours dans le cadre du BUT au département Informatique de l’IUT Charlemagne.

— J’ai aussi monté avec mes collègues, Nacer Boudjlida et Lotfi Belalem, un cours portant sur la gestion des données semi-structurées XML et qui est dispensé chaque année au Master M1 en Informatique de la faculté des sciences de l’université de Lorraine.

— Je participe également à la vie du département informatique de l’IUT Charlemagne au travers des réunions du conseil de département, des réunions pédagogiques et des jurys. J’encadre régulièrement des projets tuteurés et des stages en DUT et Licence Professionnelle.

— Entre 2009 et 2011, j’ai contribué au montage d’un cours sur la gestion de données répliquées dans les systèmes distribués et ce dans le cadre d’une formation en post graduation à l’Université d’Oran (Algérie).

— Il m’arrive aussi d’intervenir dans les lycées pour participer dans les délibérations des diplômes ainsi que les ateliers de vulgarisation. A titre d’exemple, en juillet 2015, j’étais président du jury de délibération pour le baccalauréat professionnel (session juin 2015) au lycée Paul Louis Cyffle de Nancy. En avril 2018, j’ai animé un atelier sur la protection de données personnelles dans les réseaux sociaux et ce pour les élèves du Lycée Jacques Callot de Vandœuvre-lès-Nancy[2].

3.9 Projet pédagogique

Les enseignements que j’ai pu dispenser m’ont permis d’acquérir une expérience tant au niveau de la préparation des cours que des responsabilités associées (préparation des sujets d’examen, corrections,

2. https://www.estrepublicain.fr/edition-de-nancy-agglomeration/2018/04/21/si-c-est-gratuit-c-est-toi-le-produit

jurys). Venant de l'IUT Charlemagne de Nancy, je peux sans le moindre problème enseigner les matières en Informatique à PolyTech de Nancy. Par ailleurs, je reste ouvert bien entendu pour enseigner dans la filière "Cybersécurité" ainsi que dispenser des enseignements proches de mes compétences en recherche, à savoir :

- Sécurité et Privacy : j'ai traité des problèmes de la sécurité et privacy (plus particulièrement la notion de vie privée dans les média sociaux et les bases de données classiques/multidimentionnelles) allant du contrôle d'accès dans les systèmes collaboratifs et les bases de données semi-structurées à la détection des attaques portant sur la divulgation des informations sensibles dans les réseaux sociaux, en passant par les protocoles de sécurité pour le partage et la synchronisation des données répliquées.
- Big Data et Data Science : Mes projets de recherche (financés par la fondation MAIF et Cisco), sur les problèmes liés à la vie privée dans les médias sociaux, m'ont permis de manipuler des outils concernant la fouille de données sur des graphes de taille massive, l'utilisation des bases de données NoSQL et graphiques, et les techniques d'intelligence artificielle.
- Systèmes distribués : j'ai travaillé sur ce thème dans mes travaux de recherche et j'ai même donné une série de séminaires sur les problèmes de synchronisation dans les systèmes collaboratifs (une classe particulière des systèmes distribués).
- Cloud : j'ai co-dirigé une thèse portant sur la conception d'applications appropriées pour le Cloud où la migration optimale des traitements ainsi que la virtualisation sont d'une importance majeure.

En parallèle des enseignements, je souhaite participer à l'encadrement des étudiants lors des projets individuels ou de stage, aussi bien en entreprise qu'en recherche. D'autre part, j'espère également remplir des responsabilités liées à la fonction de Professeur des universités, telles que les responsabilités administratives inhérentes au bon déroulement d'une formation.

ACTIVITÉS SCIENTIFIQUES

Cette partie est consacrée à mes activités scientifiques. Elle est principalement composée des sections suivantes :

— Un projet de recherche pour ma candidature à un poste de professeur.

— Mes activités de recherche depuis mon recrutement en tant que MdC.

— Encadrements et animation de la recherche.

— Rayonnement scientifique.

4.1 Projet de Recherche : Un pour tous et tous pour un. Protection collaborative de la vie privée

Mots clés : Vie privée collaborative, attaques, analyse des risques liés à la vie privée, contre-mesures, partage d'information.

Dans cette section, je vais présenter un projet de recherche pour l'intégration dans l'équipe PESTO du laboratoire LORIA.

4.1.1 Contexte

Les systèmes de partage d'informations (SPI) sont destinés à stocker, manipuler et partager des informations sur des entités (par exemple, des entreprises ou/et des individus) dispersées géographiquement. Avec l'émergence de nouvelles technologies telles que les plateformes de réseautage social et le "cloud computing", les dimensions sociales et collaboratives sont intégrées dans tels systèmes. Au-delà de la réalisation de tâches communes, les SPI permettent désormais aux individus et aux organisations de former des groupes afin de coopérer autour d'intérêts communs et, surtout, de partager un large éventail de types de données (par exemple, des données multimédias et sociales). Des médias sociaux à l'intelligence collective, de nombreux environnements ont vu le jour tels que le microblogage, le partage de fichiers via le cloud, les pages wiki, les systèmes de recommandation et les sites de questions-réponses [6, 23].

Malgré leur popularité, la protection de la vie privée liée aux informations partagées devient une préoccupation croissante dans ces systèmes. En effet, les utilisateurs sont de plus en plus conscients des conséquences néfastes des fuites sur la vie privée. Comme le promeut le RGPD (Règlement Général sur la Protection des Données dans l'Union européenne), la vie privée est le droit pour toute entité de contrôler quelles informations la concernant sont collectées et stockées et avec qui elles sont partagées. En conséquence, plusieurs travaux de recherche ont proposé des modèles et des mécanismes capables de protéger la vie privée des individus. Cependant, la vie privée individuelle n'est pas seulement tributaire de la manière dont nous manipulons nos propres données, mais également de la manière dont les autres divulguent des informations qui nous concernent (voir nos travaux [3, 14, 15, 16, 17, 19] sur les réseaux sociaux). L'individu s'assimile tout le temps aux membres de sa communauté avec lesquels il partage, par exemple, des convictions, des idées et des choix sociétaux. Aussi, la vie privée individuelle peut être mise à mal car la communauté facilite amplement l'identification du caractère et la personnalité de l'individu.

Par conséquent, la protection de la vie privée individuelle va nécessiter un effort collectif de la part de la communauté où chaque individu cache ses liens (cette action est en général asymétrique dans les réseaux sociaux) avec les autres membres. C'est ce qu'on appelle communément la *vie privée collaborative*.

Nous donnons deux exemples sur les problèmes liés à la vie privée collaborative. Le premier exemple est le fameux scandale de Cambridge Analytica (avec la complicité de Facebook). Cette société a recueilli des informations d'utilisateurs consentants de Facebook via une application tierce mais aussi collecté des informations personnelles de tous leurs amis qui n'avaient jamais donné leur consentement quant à l'exploitation de leurs propres données [10]. Le deuxième exemple concerne les sites de questions-réponses (par exemple Quora) qui permettent aux utilisateurs de poser, répondre et suivre des questions sur une variété de sujets structurés autour de groupes d'utilisateurs. Chaque membre du groupe peut choisir de suivre/répondre à une question de manière anonyme pour éviter les conséquences fâcheuses que son action peut entraîner, ou de manière non anonyme pour promouvoir sa visibilité et son engagement. Néanmoins, il est possible de détecter avec une forte probabilité lorsque certains utilisateurs ont agi de manière anonyme sur certaines questions, en raison de leur appartenance explicite à d'autres groupes où des sujets sensibles (par exemple, des expériences émotionnelles et personnelles) sont abordés [6].

Une autre et meilleure possibilité consiste à utiliser la collaboration pour éviter les situations où les comportements de certains mettent en danger la vie privée des autres [11]. Pour cette raison, un certain nombre de systèmes de gestion collaborative de la vie privée ont été proposés dans la littérature. Nous présentons dans ce qui suit quelques travaux. Dans [8], les auteurs ont abordé le problème de la gestion collaborative de la confidentialité des photos partagées sur les réseaux sociaux en ligne. Dans [5], les auteurs ont manipulé des données, tels que les dossiers médicaux, les appels téléphoniques et les localisations géographiques, pour proposer des mécanismes de protection des données personnelles liées à plusieurs utilisateurs où chacun décide de la manière dont les données sont partagées. Dans [7], les auteurs ont étudié la vie privée collaborative pour le problème de partage de données de localisation et ont proposé des protocoles basés sur la théorie des jeux. Dans [1], les auteurs ont traité des problèmes liés à la vie privée lorsque des données génomiques et des photos sont partagées sans le consentement de leurs propriétaires. Dans [9], les auteurs proposent un mécanisme basé sur des enchères pour gérer la vie privée des utilisateurs lorsque des informations liées à plusieurs individus sont en jeu.

La plupart des solutions existantes sont adaptées à des environnements spécifiques (par exemple, les réseaux sociaux), utilisent des terminologies différentes pour décrire en quelque sorte les mêmes problèmes de confidentialité et s'appuient sur des méthodes dédiées entièrement à l'apprentissage machine sur des données spécifiques pour quantifier les risques sur la vie privée.

En conséquence, il est nécessaire de définir un modèle unifié de la vie privée collaborative qui se base sur la formation dynamique des groupes autour d'un ou plusieurs intérêts communs. S'inspirant de notre expérience sur les systèmes distribués, et plus particulièrement les problèmes de convergence dans les systèmes collaboratifs (voir nos travaux récents [20, 21, 22, 2]), la vie privée collaborative peut être perçue comme une propriété de sûreté qui doit être préservée durant toutes les interactions intra et inter groupes. De plus, un système collaboratif de gestion de la vie privée repose sur des aspects sociaux (par exemple, améliorer le "moi algorithmique") et techniques (par exemple, utiliser un contrôle d'accès simple) dont la combinaison doit être claire et simple afin d'augmenter l'utilisabilité des systèmes de partage d'informations. Il y a également un manque d'outils logiciels pour aider les utilisateurs à auditer et expliquer les risques sur la vie privée et aussi à détecter et résoudre les conflits au sein du groupe quant à la protection collaborative de la vie privée.

4.1.2 Description du projet

La mission principale du projet est de fournir à des SPI un modèle unifié de la vie privée collaborative et des mécanismes efficaces pour la protection des groupes où l'analyse des risques liés à la vie privée [4] et les aspects techniques/sociaux sont conjointement intégrés. Nous prévoyons donc de concevoir des protocoles distribués pour des réseaux overlay (ou réseaux de recouvrement) bâtis au-dessus des SPI. Ces protocoles ont pour objectifs de contrôler (c.-à-d. détecter de potentielles attaques) et renforcer (c.-à-d. réparer les "mauvais" comportements des utilisateurs) la vie privée collaborative. Contrairement aux travaux existants qui sont ad hoc et spécifiques (ou complètement orientés) aux données, nos protocoles envisagés doivent trouver un équilibre entre les données et les aspects de contrôle.

Pour ce faire, nous allons explorer les attaques contre la vie privée collaborative, quantifions leurs risques et expliquons leurs conséquences. Une fois les origines des menaces détectées, nous concevons des contre-mesures efficaces et optimales pour empêcher la divulgation involontaire d'informations sensibles de la part des membres du groupe. A ce titre, nous explorerons des solutions techniques telles que le contrôle d'accès optimiste [2], l'anonymisation et les techniques d'obscurcissement.

Nous prévoyons donc d'aborder les points suivants :

1. Comprendre la vie privée collaborative

Étant donné un groupe où chacun de ses membres possède plusieurs données personnelles, entretient plusieurs relations (par exemple, des amis, des partenaires et/ou des collègues) et exécute un ensemble d'actions (par exemple, commenter sur des publications et partager des photos). La question qui se pose est : quels sont les membres qui mettent en danger la vie privée du groupe ? La réponse à une telle question nécessite une définition claire de la vie privée collaborative et une analyse approfondie des informations et comportements qui affectent la vie privée du groupe.

La formation des groupes est d'une importance majeure qui peut se faire soit de manière automatique, soit de manière interactive. D'une part, nous pourrons adapter des techniques de détection de communautés (comme notre travail [13]) pour construire des groupes ayant les mêmes attentes en matière de vie privée. D'autre part, nous pourrons concevoir un protocole de négociation entre plusieurs utilisateurs pour converger vers un groupe ayant une vie privée consensuelle.

Il convient de noter que la construction des groupes peut entraîner des conflits sous forme de résidus de vie privée qui peuvent différer d'un membre à un autre dans le même groupe ou proviennent du même individu appartenant à des groupes différents. Il est nécessaire de détecter et résoudre ces conflits afin de converger vers la vie privée collaborative escomptée. Par ailleurs, le groupe peut être dynamique où les membres peuvent joindre ou quitter à tout moment. Il faut donc évaluer comment la variation du groupe pourrait affaiblir ou consolider la vie privée collaborative.

2. Concevoir un protocole collaboratif pour détecter les vulnérabilités.

Les risques sur la vie privée peuvent apparaître soit directement après les comportements en ligne (par exemple, trouver le numéro de téléphone d'un utilisateur dans un commentaire publié par un autre utilisateur), soit indirectement par le biais d'une inférence d'informations privées (par exemple, en déduisant les traits de personnalité et la localisation géographique à partir du groupe) sur une ou plusieurs plateformes [12]. Dans cette partie, nous projetons de concevoir un protocole collaboratif qui s'appuie sur la communication (moyennant des réseaux overlay) entre les utilisateurs impliqués dans le groupe. Notre protocole sera basé sur des approches algorithmique et statistique afin de détecter et de quantifier les risques sur la vie privée.

Un équilibre entre les données et les fonctions de contrôle doit être atteint dans un tel protocole [4,3]. En effet, il doit être capable (i) d'analyser un volume important de données différentes (par exemple,

données multimédia et sociales) et (ii) mettre en évidence les causes réelles – au-delà des corrélations – des vulnérabilités (par exemple, quels comportements mettent en péril la vie privée du groupe) en utilisant des outils d'interprétabilité et d'explicabilité. L'utilisation des techniques d'Intelligence Artificielle (IA) se prête bien au contrôle de la vie privée. Cependant, ces techniques sont généralement utilisées comme des boîtes noires. Pour détecter les sources de vulnérabilité, il est important d'injecter un peu de contrôle dans les outils IA afin de pouvoir tracer l'influence de chaque membre du groupe (via ses données, ses relations et ses actions) et expliquer comment il impactera la vie privée collaborative. Cette traçabilité est importante pour délimiter les zones à risques dans le groupe et introduire des contre-mesures adéquates.

Par ailleurs, des expérimentations extensives et approfondies sur des systèmes réels (par exemple, des sites de microblogage et de questions-réponses) seront nécessaires pour démontrer l'efficacité et le passage à l'échelle (telle que la taille du groupe) de notre protocole.

3. Concevoir un protocole collaboratif pour renforcer la vie privée

Lorsqu'une vulnérabilité de la vie privée est détectée, elle peut provenir d'un ou plusieurs utilisateurs à l'intérieur du groupe. Toute contre-mesure doit être équitable (c'est-à-dire qu'elle n'affecte pas la vie privée des autres utilisateurs) et optimale (c'est-à-dire qu'elle n'isole pas complètement l'utilisateur du groupe). Pour éliminer ou minimiser les vulnérabilités de la vie privée, nous prévoyons de développer un protocole collaboratif pour aider les utilisateurs à appliquer des contre-mesures optimales et équitables en leur fournissant des explications claires sur les impacts de ces contre-mesures sur le groupe.

Deux techniques de compromis seront explorées. La première technique s'appuie sur des politiques de contrôle d'accès pour masquer ou publier des données personnelles inter et intra-groupes. Pour traiter les groupes dynamiques ainsi que leur abondant contenu généré par les utilisateurs, nous pouvons utiliser une technique de contrôle d'accès optimiste de telle sorte que l'application des autorisations soit rétroactive (voir notre travail [2]). Basée sur des schémas d'anonymisation et d'obscurcissement, la seconde technique nous permet de changer la sémantique des informations publiées de manière à ce qu'elles deviennent moins précises (ou bruitées). Pour ce faire, l'utilisation coordonnée de plusieurs réseaux adverses génératifs (en anglais Generative Adverserial Networks) pour générer un bruit avec un fort degré de réalisme peut être une piste très prometteuse.

Par ailleurs, l'application des contre-mesures relève d'un problème d'optimisation : minimiser les risques et maximiser les profits pour un groupe (voir notre travail [18]). La définition d'une telle optimisation se heurte au problème de passage à l'échelle. En effet, d'une part, le nombre de variables à considérer est important (par exemple, combiner les données multimédia avec les données sociales). Et d'autre part, le nombre et la nature des contraintes à satisfaire pourraient varier d'un utilisateur à un autre. Pour contourner ce problème de passage à l'échelle, il serait donc judicieux de définir le problème d'optimisation avec des abstractions (ou des classes d'équivalences) qu'il faudra déterminer sur la base de la vie privée collaborative et des profits du groupe.

4.1.3 Références

1. D. BOYD. "Networked Privacy". *Surveillance & Society*, Vol 10 No 3/4, 2012.
2. A. CHERIF, A. IMINE and M. RUSINOWITCH. "Practical access control management for distributed collaborative editors". *Journal Pervasive and Mobile Computing Journal*, 15 : 62-86, Elsevier, 2014.
3. S. J. DE and A. IMINE. "Privacy Risk Analysis of Online Social Networks". *Synthesis Lectures on Information Security, Privacy, & Trust*, pp. 1-110, Morgan & Claypool Publishers, 2021.
4. S. J. DE and D. LE MÉTAYER. "Privacy Risk Analysis". *Synthesis Lectures on Information Security, Privacy, & Trust*, pp. 1-133, Morgan & Claypool Publishers, 2016.

5. S. GNESI, C. MOISO, M. PETROCCHI and M. VESCOVI. "My Data, Your Data, Our Data : Managing Privacy Preferences in Multiple Subjects Personal Data". *APF*, pp. 154-171, 2014.
6. S. T. PEDDINTI, A. KOROLOVA, E. BURSZTEIN and G. SAMPEMANE. "Cloak and Swagger : Understanding Data Sensitivity through the Lens of User Anonymity". *IEEE Symposium on Security and Privacy*, pp. 493-508, 2014.
7. F. SANTOS, M. HUMBERT, R. SHOKRI and J-P. HUBAUX. "Collaborative Location Privacy with Rational Users". *GameSec*, pp. 163-181, 2011.
8. A. SQUICCIARINI, M. SHEHAB and F. PACI. "Collective privacy management in social networks". *WWW* pp. 521-530, 2009.
9. O. ULUSOY and P. YOLUM. "Agents for Preserving Privacy : Learning and Decision Making Collaboratively". *EUMAS/AT*, pp. 116-131, 2020.
10. "Cambridge Ananlytica". Wikipédia. https ://fr.wikipedia.org/wiki/Cambridge_Analytica
11. G. MENG, Y. LIU, J. ZHANG, A. POKLUDA and R. BOUTABA. "Collaborative Security : A Survey and Taxonomy". *ACM Computing Surveys*, 48(1 :1), July 2015.
12. A. ANDREOU, O. GOGA and P. LOISEAU. "Identity vs. Attribute Disclosure Risks for Users with Multiple Social Profiles". *IEEE/ACM ASONAM*, pp. 163–170, 2017.
13. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Detecting Communities under Differential Privacy". *Workshop on Privacy in the Electronic Society, WPES@CCS 2016*, pp. 83–93, 2016.
14. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Inferring attributes with picture metadata embeddings'. *Journal of ACM SIGAPP Applied Computing Review*, 20(2) :36-45, 2020.
15. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Online Attacks on Picture Owner Privacy". *The 31th International Conference of Database and Expert Systems Applications (DEXA)*, (LNCS 12392), pp. 33-47, Bratislava, Slovakia, September 14-17, 2020.
16. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "You are what Emojis say about your Pictures : Language-independent Gender Inference Attack on Facebook". *The 35th ACM Symposium on Applied Computing (SAC), Social Network and Media Analysis Track*, Brno, Czech Republic, March 30-April 3, 2020.
17. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Gender Inference for Facebook Picture Owners". *The 16th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, Linz, Vienna, August 26-29, 2019.
18. S. J. DE and A. IMINE. "To Reveal or Not To Reveal : Balancing User-Centric Social Benefit and Privacy in Online Social Networks". *The 33th ACM Symposium on Applied Computing (SAC), Privacy by Design Track*, Pau, France, April, 2018.
19. Y. ABID, A. IMINE, A. DI NAPOLI, C. RAISSI and M. RUSINOWITCH. "Two-Phase Preference Disclosure in Attributed Social Networks". *The 28th International Conference of Database and Expert Systems Applications (DEXA)*, (LNCS 10438), Lyon, France, August, 2017.
20. M. ALGHAMDI, A. CHERIF and A. IMINE. "EdgeDoc : An edge-based distributed collaborative editing system". *Journal Pervasive and Mobile Computing Journal*, 79 : 101-121, Elsevier, 2021.
21. M. D. MECHAOUI and A. IMINE. "Lightweight Coordination Model for Mobile Collaborative Mapping". *International Journal of Communication Networks and Distributed Systems*, 26(3) : 334-366, Inderscience, 2021.

22. M. D. MECHAOUI, N. GUETMI and A. IMINE. “MiCa : Lightweight and mobile collaboration across a collaborative editing service in the cloud”. *Journal Peer-to-Peer Networking and Applications*, 9(6) : 1242-1269, Springer, 2016.
23. F. JOUANOT, O. PALOMBI and M-C. ROUSSET. “Ontology-based Learning Analytics in Medicine”. *Ercim News*, vol. 120, 2020.

4.2 Activités de recherche

Dans ce quit suit, je décris les principaux thèmes de recherche sur lesquels j'ai travaillé et/ou travaille encore.

4.2.1 Analyse des risques sur la vie privée

L'anonymat sur les réseaux sociaux ne supprime pas les risques sur la vie privée des utilisateurs découlant du recoupement des informations personnelles publiées par ceux-ci ou par leurs relations en ligne. Dans cette optique, nous avons mené une enquête par questionnaire pour mesurer la sensibilité des données personnelles publiées sur les medias sociaux et analysé les pratiques des utilisateurs. Nous avons montré ainsi que plus de 76% des internautes sondés sont vulnérables aux attaques de révélation d'identité et d'inférence d'informations sensibles. L'étude est complétée par la description d'une procédure automatique qui montre que ces vulnérabilités sont simples à exploiter en pratique et doivent donc être prises en compte dans un système de protection. Ensuite, nous avons classé les utilisateurs de réseaux sociaux selon le risque encouru par leur vie privée. Ce risque est identifié par trois vecteurs qui prennent en compte les informations rendues publiques par les utilisateurs eux-mêmes, leurs communautés (groupes, pages, événements) et leur réseau de contact. Enfin, pour inférer des liens potentiels entre profils ainsi que des attributs cachés (par exemple, genre, pages aimées, etc.), nous avons analysé les interactions entre les utilisateurs et leurs agrégations au sein de groupes. Pour ce faire, nous avons implémenté une stratégie permettant, pour un utilisateur donné, de divulguer ses liens d'amitiés et groupes ainsi que ses attributs même s'il les a explicitement cachés. Ce travail a été réalisé dans le cadre d'un projet financé par la Fondation MAIF[1].

Étant données des images publiées en ligne par les utilisateurs sur Facebook, nous avons exploré comment lancer des attaques d'inférence de genre (féminin ou masculin) contre leurs propriétaires à partir de métadonnées d'images composées de : (i) tags générés par Facebook pour décrire le contenu des images (par exemple, le nombre de personnes présentes dans l'image), et (ii) des commentaires publiés par des amis, des amis d'amis ou d'autres utilisateurs. Nous nous sommes concentrés sur Facebook, car il s'agit du plus grand réseau social au monde. Nous avons montré la possibilité d'inférence des attributs, tels que le genre et l'âge, sur des données qui sont a priori innocentes et non sensibles. Nous avons déterminé comment ces données conduisent à la conception d'ensembles de caractéristiques qui peuvent être analysés par un attaquant pour déduire les attributs des propriétaires d'images.

Nous avons également étudié la protection de la vie privée des médias sociaux contre les attaques par inférence d'attribut en utilisant l'explicabilité de l'apprentissage automatique et des stratégies de défense antagonistes (en anglais, adversarial). Plus précisément, nous avons proposé FOX (FOoling with eXplanations), un cadre d'attaque antagoniste pour expliquer et tromper les modèles d'inférence d'attributs sensibles en générant des réactions contradictoires efficaces. Nous avons évalué les performances de FOX, dans un cadre de boîte noire, en attaquant cinq classificateurs d'attributs de genre formés sur les réactions aux images Facebook. Nos expériences ont montré que FOX trompe avec succès (environ 99,7% et 93,2% du temps) les classificateurs et donne une bonne transférabilité des caractéristiques contradictoires.

Dans un autre travail, financé par CISCO (San Jose, Etats Unis d'Amérique), nous avons conçu une méthode efficace pour évaluer l'exposition de la vie privée à des attaques (modélisées sous forme d'arbres) communément connues dans les réseaux sociaux. Cette méthode permet de mieux guider les internautes dans la compréhension des différents risques sur leur vie privée. De plus, nous avons formulé la configuration des paramètres de confidentialité comme un problème d'optimisation linéaire pour qu'un utilisateur puisse tirer

1. https://www.fondation-maif.fr/pageArticle.php?rub=1&id=258

le maximum de profit de sa présence sur les réseaux sociaux tout en se protégeant de tous ou au moins de certains risques importants sur la vie privée. Ces risques ont été également évalués pour des mécanismes de consentement issus des exigences du RGPD (Règlement Général sur la Protection de Données) de l'Union Européenne.

Récemment, je me suis intéressé aux problèmes de la vie privée dans les plateformes sociales de codage (par exemple, GitHub) grâce à une collaboration avec l'université de Hambourg (Allemagne). En effet, les utilisateurs de telles plateformes sont soumis à des attaques sur leur vie privée compte tenu des grandes quantités de données personnelles et celles liées aux projets disponibles dans leurs profils et leurs référentiels de logiciels. Nous avons mené une enquête en ligne portant sur les préoccupations et les perceptions des développeurs concernant les menaces à la vie privée. Nos résultats montrent que, bien que les utilisateurs se disent préoccupés par les menaces sur la vie privée, ils se sentent souvent en sécurité en partageant des informations sur ces plateformes. Ce constat nous encourage à concevoir des outils de veille pour la protection de la vie privée dans les plateformes sociales de codage.

Voir Publications dans la section 5 : 5, 6 (Revues internationales) - 1, 7, 8, 10, 11, 15, 16, 17, 18, 19 (Conférences internationales) - 1, 2, 3 (Workshops internationaux) - 2, 3 (Conférences nationales).

4.2.2 Gestion et analyse des Big Data préservant la confidentialité dans les environnements distribués

De nos jours, l'exploitation des Big Data, souvent basées sur des environnements distribués, gagnent du terrain au sein de la communauté de la recherche. Dans ce contexte, la question de la prise en charge de la gestion et de l'analyse des Big Data préservant la confidentialité joue un rôle de premier ordre, en particulier en ce qui concerne la vaste classe d'applications, qui vont des réseaux sociaux à la bio-informatique, des réseaux de capteurs aux outils de recommandation, etc.

Nous avons exploré le problème de la vie privée des individus dans la publication de cubes de données intérrogées par des requêtes SUM, où un utilisateur malveillant est censé avoir une connaissance agrégée (par exemple, des moyennes) sur les plages de données. Nous avons proposé une solution qui maximise l'utilité des requêtes SUM tout en atténuant les attaques par inférence à partir de connaissances agrégées. Notre solution combine la compression de cube (c'est-à-dire la suppression des cellules de données) et la perturbation des données. Grâce à une évaluation empirique sur des cubes de données de référence, nous avons montré que notre solution donne une meilleure performance en termes d'utilité et de confidentialité. Ce travail rentre dans le cadre de la préparation de thèse de l'étudiant Ala Eddine Laouir.

Voir Publications dans la section 5 : 2 (Conférences internationales).

4.2.3 Fraudes et sécurisation dans les Crypto-Actifs

Les crypto-actifs se basent sur un réseau informatique pair-à-pair pour réaliser des transactions financières. Ces transactions sont stockées dans un grand livre partagé, appelé la chaine de blocs (Blockchain, en anglais). De par leur caractère décentralisé, ils ne sont contrôlés par aucune institution financière mais régulés par tout le monde dans le réseau. Bien que les crypto-actifs apportent un certain nombre d'avantages, l'infrastructure de la chaine de blocs sur laquelle ils sont construits est sensible à plusieurs types de cyberattaques qui se caractérisent par des fraudes. Ces fraudes prennent leur origine pour une part dans la nouveauté de ces contrats et l'absence de standardisation réglementaire, pour une autre part des spécificités informatiques propres à ces contrats et à leur distribution. Il semble crucial pour appréhender les fraudes de considérer non seulement la nature innovante des contrats liés aux crypto-actifs dans un espace financier

non stabilisé (intermédiaires sans réputation et sans agrément ; transparence réduite) mais aussi les failles informatiques propres aux dispositifs de la chaîne de blocs (réseau distribué, clés publique/privé).

Dans le cadre d'une collaboration avec l'économiste Pr Tadjeddine Yamina (et plus précisément dans le cadre de sa chaire EFNUM – Économie, Finance et Numérique), nous menons actuellement une réflexion pour concevoir des stratégies basées sur les techniques de Machine Learning et ce pour identifier des situations de fraude liées à l'absence d'une régulation équitable et à des failles des infrastructures informatiques. De cette collaboration est né le club étudiants-chercheurs "Économie, Finances, Numérique" dans le cadre du projet Orion (Oser la Recherche durant la formatION) de Lorraine Université d'Excellence (LUE). Nous avons actuellement deux stagiaires en Master 2 qui travaillent sur cette problématique. Par ailleurs, LUE a accepté notre soumission pour un projet de recherche d'aide à la dynamique interdisciplinaire pour un budget de 150 000 euros.

4.2.4 Anonymisation des graphes sociaux

La publication de données sociales (sous forme de graphes) à une partie tierce (à des fins commerciales ou académiques) impose la protection de certaines informations personnelles, telle que l'identité des utilisateurs. Néanmoins, les méthodes classiques d'anonymisation généralisant (ou ajoutant/supprimant) les nœuds/arêtes d'un graphe social, s'avèrent inefficaces. Par contre, des méthodes récentes, exploitant la sémantique des graphes incertains, permettent de mieux préserver la vie privée des utilisateurs ainsi que leurs relations. Ces techniques anonymisent (ou obscurcissent) un graphe déterministe en le convertissant en un graphe incertain (en étiquetant les arêtes avec des probabilités). Dans ce travail, nous avons proposé un modèle général d'obscurcissement basé sur des matrices d'adjacence incertaines qui maintiennent les degrés des nœuds égaux à ceux attendus dans le graphe sans anonymisation. Nous avons également utilisé la technique de vie privée différentielle (en anglais Differential Privacy) pour proposer un cadre formel quant à la publication anonyme des graphes sociaux. Nous avons donc proposé une méthode d'anonymisation qui permet un bon compromis entre l'utilité du graphe social et la protection de la vie privée. Avec un budget logarithmique de la vie privée, nous avons montré qu'il existe un algorithme capable de publier un graphe obscurcis avec une distance d'édition égale à $O(1)$. Pour faire des comparaisons équitables, nous avons proposé un environnement pour quantifier le compromis entre la vie privée et l'utilité des graphes. Les expérimentations faites sur des graphes sociaux réels (de grande taille) ont montré l'efficacité de notre proposition. Nous avons également proposé un algorithme de détection de communautés privées qui procède en deux étapes : la perturbation du graphe social et la construction approximative de modules à partir du graphe bruité. Enfin, nous avons introduit le problème d'échange (utilisant les filtres de Bloom) de liens privés comme une alternative à l'exploration de graphe social et l'anonymisation centralisée des données.

Dans un autre travail, financé par le projet DigiTrust (Lorraine Université d'Excellence), nous avons adapté la technique de vie privée différentielle pour traiter du problème de l'inférence d'attributs lors de publication des graphes sociaux pour des systèmes de recommandation.

Voir Publications dans la section 5 : 8 (Revues internationales) - 3,4, 24, 25, 30, 31 (Conférences internationales) - 4 (Workshops internationaux) - 1 (Conférences nationales).

4.2.5 Conception des systèmes collaboratifs

Dans ce travail, nous nous sommes intéressés à la conception des éditeurs collaboratifs en temps réel, déployés sur des plateformes basées sur le Cloud et Edge Computing, qui permettent la manipulation de divers objets partagés, tels que les pages wiki ou les articles scientifiques, par plusieurs personnes

réparties dans le temps et dans l'espace. Nous avons proposé un modèle de contrôle d'accès générique basé sur l'approche de réplication optimiste du document partagé ainsi que sa politique de contrôle d'accès. Pour cela, nous avons proposé une approche optimiste de contrôle d'accès dans la mesure où un utilisateur peut violer temporairement la politique de sécurité. Pour assurer la convergence, nous avons fait recours à l'annulation sélective pour éliminer l'effet des mises à jour illégales. Quant à la validation de notre approche, tous nos algorithmes ont été implémentés en java et testés sur la plateforme distribuée Grid'5000. Un dépôt APP a été fait pour les algorithmes développés durant ce travail (réf. APP : $IDDN.FR$.001.150007.000.$S.P$.2010.000.10000).

En outre, en employant une technique symbolique de model-checking borné, nous avons spécifié formellement l'empilement de notre contrôle d'accès à un système collaboratif. L'analyse a permis de conclure que le contrôle d'accès est uniformément appliqué sur toutes les copies de l'objet partagé et préserve la cohérence. Cette analyse nous a également permis de valider certains choix conceptuels de notre modèle.

Voir Publications dans la section 5 : 2, 3, 4, 9, 13 (Revues internationales) - 1 (Revues nationales) - 2 (Chapitres d'ouvrage) - 7, 31, 39 (Conférences internationales) - 7, 12 (Workshops internationaux).

4.2.6 Problème de sondage dans les réseaux sociaux

Dans ce travail, nous avons abordé le problème de sondage dans les réseaux sociaux où le caractère secret des informations échangées et la réputation de l'utilisateur sont très critiques. En effet, les utilisateurs désirent préserver la confidentialité de leur choix et dissimuler, le cas échéant, leurs mauvais comportements (par exemple, biaiser un vote). Nous avons proposé trois protocoles décentralisés de sondage basés sur le partage de secret et ne nécessitant aucune infrastructure cryptographique. Les deux premiers protocoles utilisent respectivement des modèles de communication synchrone et asynchrone, et manipulent des procédures de vérification pour détecter les utilisateurs malhonnêtes. Quant au troisième protocole, il est asynchrone et ne nécessite pas de procédures de vérification. Pour que ce protocole permette une diffusion efficace de messages, nous avons défini une propriété basée sur le tri topologique des graphes sociaux. Dans la deuxième partie de ce travail, nous avons formalisé le problème de "l'ajout des amis" qui consiste à trouver une transformation optimale des graphes sociaux pour les adapter au partage de secret. Pour résoudre ce problème, nous avons présenté deux algorithmes selon deux configurations différentes : centralisée et décentralisée.

Voir Publications dans la section 5 : 23, 33, 35 (Conférences internationales).

4.2.7 Contrôle d'accès pour des données XML

Dans ce travail, nous avons étudié le problème d'accès à des informations confidentielles contenues dans des documents XML partagés par un nombre important d'utilisateurs ayant des rôles variés et divers. Nous avons considéré les langages XPath et XQuery Update Facility pour la formalisation des requêtes, respectivement, d'accès et de mise à jour. Nous avons donné des descriptions formelles de nos modèles de contrôle d'accès et nous avons présenté des algorithmes efficaces pour le renforcement des politiques de sécurité spécifiées sur la base de ces modèles. L'autre partie de ce travail est consacrée à l'étude pratique de nos propositions. Pour ce faire, nous avons implémenté un système, appelé SVMAX, qui met en œuvre nos solutions. Pour mesurer le passage à l'échelle de SVMAX, nous avons conduit une étude expérimentale basée sur des schémas réels (par exemple, des DTDs). Même si XML connaît actuellement une perte de vitesse, notre travail a abouti à un résultat notable, à savoir la proposition d'algorithmes efficaces pour

contrôler et répondre, de manière sécurisée, aux requêtes des utilisateurs en utilisant uniquement la puissance expressive du XPath standard.

Voir Publications dans la section 5 : 10 (Revues internationales) - 32, 34, 36 (Conférences internationales) - 8 (Workshops internationaux) - 4 (Conférences nationales).

4.2.8 Vérification et synthèse d'algorithmes de réplication optimiste

L'approche des transformées opérationnelles est utilisée pour assurer la convergence des données dans les éditeurs collaboratifs basés sur la réplication. Elle possède deux composants : (i) l'algorithme d'intégration qui est responsable de la génération, la réception et la diffusion des opérations ; (ii) l'algorithme de transformation (spécifique à la sémantique de l'objet partagé) assure l'exécution des opérations concurrentes dans n'importe quel ordre. La convergence des données est acquise si, et seulement si, l'algorithme de transformation satisfait deux propriétés de base, communément appelées TP1 et TP2.

Il s'agit, à ce niveau, de développer un environnement qui permet de tester et vérifier les algorithmes de transformation en prenant en compte l'algorithme d'intégration. Pour ce faire, nous avons utilisé la technique de model-checking. Le comportement de chaque site (à savoir, génération aléatoire d'opérations, réception, intégration et transformation d'opérations) est décrit au moyen d'un automate étendu aux variables et canaux de synchronisation. La vérification de la convergence des données, à chaque fois que le système est dans un état stable, est réalisée par l'outil UPPAAL[2]. Cette approche, cependant, impose de fixer le nombre de sites, le nombre d'opérations générées sur chaque site, et la taille et l'alphabet du document partagé. Nous avons pu montrer que pour un nombre de sites plus grand que 2 et un nombre d'opérations plus grand que 3 (dont 3 sont au moins concurrentes), un scénario complet de divergence est généré pour chaque algorithme de transformation existant dans la littérature.

Par ailleurs, nous avons étudié l'existence de fonctions de transformation satisfaisant les propriétés TP1 et TP2 pour assurer la convergence. En utilisant une méthode de synthèse de contrôleur basée sur les automates de jeu, nous avons montré l'impossibilité de trouver une fonction de transformation assurant la cohérence des objets linéaires (tels que le texte, l'arbre ordonné XML, etc.) altérés par de simples opérations d'insertion et de suppression. L'extension de l'opération d'insertion par une méta-donnée nous a permis de proposer une nouvelle fonction de transformation dont la propriété de convergence a été vérifiée par une technique de model-checking.

Voir Publications dans la section 5 : 11 (Revues internationales) - 41, 44 (Conférences internationales) - 9 (Workshops internationaux).

4.2.9 Réalisation logicielles

Mes travaux de recherche ont donné lieu à des réalisations logicielles, à savoir[3] :

- **PROP (Privacy Risk analysis tool for OSN Profiles).** Un environnement pour évaluer l'exposition de la vie privée à des attaques communément connues dans les réseaux sociaux. Cet outil permet d'assister les internautes pour mieux comprendre les différents risques sur leur vie privée (voir Publications section 5 : 18 (Conférences internationales)).
- **SONSAI (SOcial Network Sensitive Attribute Inference).** Un environnement pour inférer des informations sensibles dans les réseaux sociaux. Cet outil permet de construire des attaques en ligne

2. http://www.uppaal.com/
3. Les outils PROP et SONSAI ne sont pas encore disponibles en ligne car nous attendons l'aval de la CNIL.

en utilisant des techniques d'apprentissage machine (voir Publications section 5 : 1, 2 (Workshops internationaux)).

- **Environnements collaboratifs avec un contrôle d'accès optimiste.**[4] Basé sur notre modèle de contrôle d'accès optimiste (voir Publications section 5 : 13 (Revues internationales)), deux applications ont été implémentées : (i) **P2PEdit** est un éditeur collaboratif complètement décentralisé ; (ii) **DeSCal** est un environnement collaboratif déployé sur un réseau de mobiles IPhone pour le partage d'agenda sécurisé. Un APP (réf : $IDDN.FR$.001.150007.000.$S.P$.2010.000.10000) a été déposé.

4. https://members.loria.fr/AImine/tools/home.htm

4.3 Encadrements et animation de la recherche

4.3.1 Encadrements Post-Doc

1. **Evaluation des Risques sur la Vie Privée dans les Réseaux Sociaux**
   - **Post-doc :** Sourya Joyee De
   - **Années :** 2017-2019
   - **Financement :** Cisco San Jose (Etats Unis d'Amérique), Région Grand Est.
   - **Publications, section 5 :** 5 (Revues internationales) - 1 (Ouvrages) - 15, 16, 17, 18 (Conférences internationales).
2. **Préserver la confidentialité des utilisateurs lors de la publication du graphe social ayant des attribues**
   - **Post-doc :** Kamalkumar R. Macwan
   - **Années :** 2022-2023
   - **Financement :** Lorraine Université d'Excellence (LUE).
   - **Publications, section 5 :** 3, 4 (Conférences internationales).

4.3.2 Encadrement de thèses de doctorat

J'ai co-encadré sept (10) thèses (sept soutenues et trois en cours).

1. **Modèles de Contrôle d'Accès optimiste pour les Applications Collaboratives**[5]
   - **Doctorante :** Asma Cherif
   - **Années :** 2008-2012
   - **Lieu :** Université de Lorraine
   - **Co-Directeur :** Michaël Rusinowitch (DR, INRIA)
   - **Financement :** Bourse du Ministère de la Recherche Scientifique en France
   - **Situation actuelle du thésarde :** Professeur Associé, Faculty of Computing and Information Technology, King Abdulaziz University, Djeddah, Arabie Saoudite.
   - **Publications, section 5 :** 13 (Revues internationales) - 2 (Chapitres d'ouvrage) - 37, 42, 45 (Conférences internationales) - 12 (Workshops internationaux).
2. **Contrôle d'Accès Efficace pour des Données XML : problèmes d'interrogation et de mise-à-jour**[6]
   - **Doctorant :** Houari Mahfoud
   - **Années :** 2010-2014
   - **Lieu :** Université de Lorraine
   - **Co-Directeur :** Michaël Rusinowitch (DR, INRIA)
   - **Financement :** Bourse du Ministère de la Recherche Scientifique en Algérie

5. https://tel.archives-ouvertes.fr/tel-01093684
6. https://tel.archives-ouvertes.fr/tel-01093661

- **Situation actuelle du thésard :** Maître des Conférences à l'Université Abou-Bekr Belkaïd, Tlemcen, Algérie.
- **Publications, section 5 :** 10 (Revues internationales) - 32, 34, 36 (Conférences internationales) - 8 (Workshops internationaux).

3. **Problème de Sondage dans les Réseaux Sociaux Décentralisés**[7]
   - **Doctorant :** Bao-Thien Hoang
   - **Années :** 2011-2015
   - **Lieu :** Université de Lorraine
   - **Co-Directeur :** Christophe Ringeissen (CR HdR, INRIA)
   - **Financement :** Bourse financée par le projet ANR Streams
   - **Situation actuelle du thésard :** Professeur Associé à l'Université de Ho Chi Minh, Vietnam.
   - **Publications, section 5 :** 23, 33, 35 (Conférences internationales).
4. **Problème d'Anonymisation dans les Réseaux Sociaux**[8]
   - **Doctorant :** Huu-Hiep Nguyen
   - **Années :** 2013-2016
   - **Lieu :** Université de Lorraine
   - **Co-Directeur :** Michaël Rusinowitch (DR, INRIA)
   - **Financement :** Bourse de contrat de recherche doctoral (CORDI INRIA)
   - **Situation actuelle du thésard :** Chercheur à Duty Tan University, Institute of Research Development (Vietnam).
   - **Publications, section 5 :** 8 (Revues internationales) - 24, 25, 30, 31 (Conférences internationales) - 4 (Workshops internationaux) - 1 (Conférences nationales).
5. **Modèles de Conception pour des Applications Collaboratives Mobiles dans le Cloud**[9]
   - **Doctorant :** Nadir Guetmi
   - **Années :** 2013-2016
   - **Lieu :** École Nationale Supérieure de Mécanique et d'Aérotechnique (ENSMA), Poitiers
   - **Co-Directeur :** Ladjel Bellatreche (Pr, ENSMA, Poitiers)
   - **Financement :** Bourse du Ministère de la Recherche Scientifique en Algérie.
   - **Situation actuelle du thésard :** Chercheur senior à l'Ecole Supérieure de Défense Aérienne du Territoire (ESDAT), Ali Chabati , Alger (Algérie).
   - **Publications, section 5 :** 7, 9 (Revues internationales) - 3 (Chapitres d'ouvrage) - 26, 28, 29 (Conférences internationales) - 6 (Workshops internationaux) - 2 (Magazines).
6. **Algorithmes de Réplication Optimiste pour des Réseaux Sans Fil**
   - **Doctorant :** Moulay Driss Mechaoui
   - **Années :** 2012-2018

7. https://tel.archives-ouvertes.fr/tel-01139325
8. https://tel.archives-ouvertes.fr/tel-01403474/
9. https://tel.archives-ouvertes.fr/tel-01430151

- **Lieu :** Université des Sciences et de la Technologie d'Oran (USTO), Algérie
- **Co-Directeur :** Bendella Fatima (Pr, USTO, Oran)
- **Financement :** Le thésard est un enseignant chercheur en Algérie
- **Situation actuelle du thésard :** MCF, Université Ibn Badis, Mostaganem (Algérie).
- **Publications, section 5 :** 9 (Revues internationales) - 1 (Chapitres d'ouvrage) - 26, 29, 39, 42 (Conférences internationales) - 6 (Workshops internationaux) - 2 (Magazines).

7. **Attaques par Inférence d'Attributs sur les Publications des Réseaux Sociaux**[10]
   - **Doctorant :** Bizhan Alipour Pijani
   - **Années :** 2018-2022
   - **Lieu :** Université de Lorraine, Nancy, France
   - **Co-Directeur :** Michaël Rusinowitch (DR, INRIA)
   - **Financement :** Lorraine Université d'Excellence (LUE)
   - **Situation actuelle du thésard :** Ingénieur de recherche dans une entreprise à Paris.
   - **Publications, section 5 :** 6 (Revues internationales) - 8, 10, 11, 12 (Conférences internationales) - 1 (Workshops internationaux).
8. **Gestion et Analyse des Big Data Préservant la Confidentialité dans les Environnements Distribués**
   - **Doctorant :** Ala Eddine Laouir
   - **Années :** 2021-2024
   - **Lieu :** Université de Lorraine, Nancy, France
   - **Financement :** Lorraine Université d'Excellence (LUE)
   - **Publications, section 5 :** 2 (Conférences internationales).
9. **Modèle de Contrôle d'Accès pour des Données Orientées Graphe**
   - **Doctorant :** Adil Achraf BEREKSI REGUIG
   - **Années :** 2022-2025
   - **Lieu :** Université Abou-Bekr Belkaïd, Tlemcen, Algérie
   - **Co-Directeur :** Houari Mahfoud (MCF HdR, Université Abou-Bekr Belkaïd, Tlemcen, Algérie)
   - **Financement :** Le thésard est financé par l'Université Abou-Bekr Belkaïd, Tlemcen, Algérie.
10. **Edition Collaborative des Données Massives et Sémantiques**
    - **Doctorant :** Hocine OURABAH
    - **Années :** 2023-2026
    - **Lieu :** Université Ibn Badis, Mostaganem, Algérie
    - **Co-Directeur :** Moulay Driss Mechaoui (MCF HdR, Université Ibn Badis, Mostaganem, Algérie)
    - **Financement :** Le thésard est financé par l'Université Ibn Badis, Mostaganem, Algérie.

10. https://hal.inria.fr/hal-02996034

4.3.3 Encadrement de Master de recherche

Voici la liste des principaux stages Master Recherche que j'ai dirigés :

1. **Du Contrôle d'Accès Dynamique pour les Editeurs Collaboratifs**
   - **Nom :** Asma Cherif
   - **Année :** 2007-2008
   - **Master :** Services Distribués et Réseaux de Communication
   - **Lieu :** Université UHP Nancy 1

   Mme Asma Cherif a fait une thèse de doctorat sous ma direction (voir Publications, section 5).
2. **Safe and Efficient Strategies for Updating Firewall Policies**
   - **Nom :** Zeeshan Ahmad
   - **Année :** 2008-2009
   - **Master :** Information Technology for the Management of Knowledge and Network (TICOR)
   - **Lieu :** Université de Technologie de Troyes
   - **Publications, section 5 :** 31 (Conférences internationales).
3. **Security Framework for Decentralized Shared Calendar**
   - **Nom :** Jagdish Prasad Achara
   - **Année :** 2010-2011
   - **Master :** Services Distribués et Réseaux de Communication
   - **Lieu :** Université UHP Nancy 1
   - **Publications, section 5 :** 29 (Conférences internationales).
4. **Detection of Frauds on Crypto-Assets**
   - **Nom :** Wail Nidal Zellagui
   - **Année :** 2022-2023
   - **Master :** Génie Logiciel Informatique
   - **Lieu :** Université de Constantine, Algérie.
5. **Classification des fraudes dans les crypto-monnaies**
   - **Nom :** Isabella Van-Der Laan
   - **Année :** 2022-2023
   - **Master :** Economie Numérique
   - **Lieu :** Université de Strasbourg, France.
   - **Co-Encadrant :** Yamina Tadjeddine (Pr. en économie, Université de Lorraine)

4.3.4 Encadrement de stagiaires

1. **Réalisation d'un éditeur Wiki sur un réseau Pair-à-Pair**
   - **Nom :** A. Allouche
   - **Année :** 2006-2007
   - **Lieu :** Ecole des Mines, Institut National Polytechnique de Lorraine (INPL)
2. **Réalisation d'un gestionnaire de versions décentralisé**
   - **Nom :** D. Furong
   - **Année :** 2006-2007
   - **Lieu :** Département d'Informatique, Université UHP-Nancy 1
3. **Réalisation d'un outil Diff pour des documents XML**
   - **Nom :** Y. Guebbas
   - **Année :** 2006-2007
   - **Lieu :** Ecole des Mines, Institut National Polytechnique de Lorraine (INPL)
4. **Developing a dynamic access control based group editor**
   - **Nom :** A. Baouab
   - **Année :** 2007-2008
   - **Lieu :** Ecole Nationale des Sciences de l'Informatique, Université de La Manouba
5. **Conception d'un Simulateur pour la Mise-à-jour en ligne des Politiques de Sécurité pour Firewall**
   - **Nom :** A. Routier
   - **Année :** 2009-2010
   - **Lieu :** IUT Charlemagne, Université Nancy 2
6. **Stratégies sûres et efficaces pour la mise-à-jour des politiques de Pare-feu Distribués**
   - **Nom :** C. Jozefiak et C. Renk
   - **Année :** 2009-2010
   - **Lieu :** Département d'Informatique, Université UHP-Nancy 1
7. **Agenda Partagé et Sécurisé sur IPhone**
   - **Nom :** J. Achara
   - **Année :** 2009-2010
   - **Lieu :** LORIA
8. **Sécurisation de Données pour un Agenda Partagé**
   - **Nom :** C. Wiedling
   - **Année :** 2009-2010
   - **Master :** Calcul Scientifique et Sécurité Informatique
   - **Lieu :** UFR Math-Info., Université de Strasbourg
9. **Calcul des Scores d'Anonymat pour les Utilisateurs des Réseaux Sociaux**

- **Nom :** L. Trivino
- **Année :** 2015-2016
- **Lieu :** IUT Charlemagne, Université de Lorraine

10. **Inférence des Informations Sensibles dans les Réseaux Sociaux**
    - **Nom :** C. Pascutto
    - **Année :** 2015-2016
    - **Master :** Informatique
    - **Lieu :** Département d'Informatique de l'École Normale Supérieure de Paris
11. **Analyse des comportements dans les Réseaux Sociaux**
    - **Nom :** H. Benmessaoud
    - **Année :** 2020-2021
    - **Master :** Informatique
    - **Lieu :** École des Mines de Nancy

4.3.5 Participation aux jury de thèses

En plus de la participation aux jurys de mes doctorants (A. Cherif, H. Mahfoud, B.T. Hoang, H.H Nguyen et N. Guetmi et B. Alipour Pijani), je suis examinateur dans les thèses suivantes :

— Mumtaz Ahmad. "Memory Optimization Strategies for Linear Mappings and Indexation-based Shared Documents"[11]. Novembre 2011, Université de Lorraine.

— Younes Abid. "Automated Privacy Risk Analysis in Social Networks". Juin 2018, Université de Lorraine.

4.3.6 Organisation d'événements scientifiques

— Membre du comité d'organisation du workshop international WTS (Workshop on Formal Methods for Web Data Trust and Security), qui s'est déroulé le 11 octobre 2010 à Nancy.

— Responsable du track "Security and Privacy" dans le comité de programme de la conférence IEEE AICCSA (ACS/IEEE International Conference on Computer Systems and Applications) en 2013, qui s'est déroulé à Fès au Maroc.

— Organisateur et PC Co-Chair de la conférence FPS[12] (International Symposium on Foundations & Practice of Security), en 2017 à Nancy.

— Co-organisateur du "German-French PhD Workshop on Secure Big Data"[13]. 24-26 Octobre 2018, Landhotel Saarschleife, Saarland, Allemagne.

11. https://tel.archives-ouvertes.fr/tel-00641866/
12. http://fps2017.loria.fr/
13. https://cispa.de/en/german-french-phd-workshop

4.3.7 Comités de programme

— Depuis quelques années, je suis membre dans le comité de programme de plusieurs événements scientifiques[14] :

  — FPS (International Symposium on Foundations and Practice of Security) : **PC Chair et organisateur** ;

  — TSP (International Symposium on Trust, Security and Privacy for Emerging Applications) : membre ;

  — SpaCCS (International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage) : membre ;

  — DEXA (International Conference on Database and Expert Systems Applications) : membre ;

  — AiOfAi (Workshop on Adverse Impacts and Collateral Effects of Artificial Intelligence Technologies) : membre ;

  — EGC (Conférence Extraction et Gestion des Connaissances) : Demo Track ;

  — DASFAA (International Conference on Database Systems for Advanced Applications) : Demo Track ;

  — ICEIS (International Conference on Enterprise Information Systems) : membre ;

  — VLIoT@VLDB (International Workshop on Very Large Internet of Things) : membre.

— Rapporteur dans plusieurs revues (IEEE Transactions on Parallel and Distributed Systems, ACM Transactions on Internet Technology, IEEE Transactions on Computational Social Systems, Journal of Computer Supported Cooperative Work, etc).

4.3.8 Activités éditoriales

— Co-éditeur des actes (LNCS 10723) de la Conférence “International Symposium on Foundations & Practice of Security (FPS)”.

— Éditeur invité, Journal “Information” MDPI, pour un numéro spécial sur la protection de données personnelles dans les réseaux sociaux[15].

— Éditeur dans le journal “Information” MDPI.

4.3.9 Autres responsabilités

— Membre élu au pôle scientifique Automatique, Mathématiques, Informatique et leurs Interactions (AM2I).

— Membre de la CMI (Commission de la Mention Informatique) chargée d’expertiser, entre autres, les dossiers (inscription et réinscription en thèse, proposition d’inter-classement des candidatures pour les contrats doctoraux, avis sur les propositions de jury, avis sur l’autorisation de soutenance, et les HDR).

— Co-Responsable du club étudiants-chercheurs “Economie, Finances, Numérique” (Orion, LUE). Ce club a pour vocation de faire de la vulgarisation scientifique sur des thèmes en informatique et en économie.

14. https://members.loria.fr/AImine/activ.html
15. https://www.mdpi.com/journal/information/special_issues/privacy_social_network

4.4 Rayonnement scientifique

4.4.1 Projets de recherche

Les projets importants où je suis (ou j'étais) responsable (coordinateur) :

Projet 1 : Taxonomie des fraudes sur les crypto-actifs

— Durée : 3 ans (2023-2026)

— Partenaires : LORIA, BETA et Lorraine Université d'Excellence (LUE).

— Budget : 150 k euros (inclus le financement d'une thèse de doctorat)

— Ressources humaines : 2 membres permanents et un thésard

— Résumé : Ce projet est financé par Lorraine Université d'Excellence (LUE). Il a pour objectif d'établir une classification des fraudes et crimes sur les cryptoactifs et des modalités de sécurisation/détection/réglementation en se basant conjointement sur des expertises en économie et en informatique.

Projet 2 : Préserver la confidentialité des utilisateurs lors de la publication du graphe social ayant des attribues

— Durée : 12 mois (2022-2023)

— Partenaires : Equipe INRIA Pesto (coordinateur) et Lorraine Université d'Excellence (LUE).

— Budget : 75 k euros (Financement d'un post-doc)

— Ressources humaines : 1 membre permanent et un post-doc

— Résumé : Ce projet est financé par Lorraine Université d'Excellence (LUE). Il a pour objectif d'adapter la technique de vie privée différentielle pour traiter du problème de l'inférence d'attributs lors de publication des graphes sociaux. Ce projet nous a permis de recruter le post-doc Kamalkumar R. Macwan.

Projet 3 : Gestion et Analyse des Big Data Préservant la Confidentialité dans les Environnements Distribués

— Durée : 3 ans (2021-2024)

— Partenaires : Equipe Pesto (coordinateur) et Lorraine Université d'Excellence (LUE).

— Budget : 137 k euros (inclus le financement d'une thèse de doctorat)

— Ressources humaines : 1 membre permanents et un thésard

— Résumé : Ce projet est financé par Lorraine Université d'Excellence (LUE). Il vise à concevoir des modèles pour des environnements distribués manipulant du Big Data et préservant la propriété de confidentialité. Deux directions sont à creuser pour satisfaire une telle propriété : la protection des données lors de leur stockage ou/et la protection des requêtes sur les données. Ce projet nous a permis de recruter le thésard Ala Eddine Laouir.

Projet 4 : Protection des données sensibles dans les réseaux sociaux

— Durée : 3 ans et 5 mois (2018-2022)

— Partenaires : Equipe Pesto (coordinateur) et Lorraine Université d'Excellence (LUE).

— Budget : 137 k euros (inclus le financement d'une thèse de doctorat)

— Ressources humaines : 2 membres permanents et un thésard

— Résumé : Ce projet est financé par Lorraine Université d'Excellence (LUE). Il a pour objectifs d'analyser les risques sur la vie privée quant à la publication de plusieurs types de données dans les réseaux sociaux et de proposer des contre-mesures basées sur l'obscurcissement des données pour renforcer l'anonymat. Ce projet nous a permis de recruter le thésard Bizhan Alipour et un ingénieur de recherche.

Projet 5 : Protection de l'information personnelle sur les réseaux sociaux

— Durée : 3 ans (2015-2018)

— Partenaires : Equipes Pesto (coordinateur) et Orpailleur de INRIA Nancy-Grand Est, Université de Lorraine et Fondation MAIF.

— Budget : 124 k euros (inclus le financement d'une thèse de doctorat)

— Ressources humaines : 4 membres permanents et un thésard

— Résumé : Ce projet est financé par la fondation MAIF. Il a pour objectif de traiter des problèmes de la vie privée dans les médias sociaux. Plus précisément, nous avons développé des solutions logicielles (basées sur l'intelligence artificielle) pour assister les utilisateurs dans le contrôle de leurs données sensibles. Nous avons également proposé des méthodes efficaces pour prédire les risques sur la base des publications et des relations sur les réseaux sociaux. Ce projet nous a permis de recruter le doctorant Younes Abid.

Projet 6 : User-Centric Privacy Control for Online Social Networks

— Durée : 18 mois (2017-2018)

— Partenaires : Equipe INRIA Pesto (coordinateur), CISCO (Etats Unis d'Amérique), Région Grand Est

— Budget : 75 k euros (inclus le financement d'un post-doc)

— Ressources humaines : 1 membre permanent et un post-doc

— Résumé : Ce projet est financé par CISCO (San Jose, Etats Unis D'Amérique). Il a pour objectifs, d'une part, (i) de concevoir des méthodes efficaces pour l'évaluation des risques liés à la vie privée dans les réseaux sociaux sur la base des attaques communément connues dans la littérature ; et d'autre part, (ii) de synthétiser des politiques de sécurité basées sur les besoins de l'utilisateur en termes de profit social tiré des réseaux sociaux et le niveau de vie privée escompté. Ce projet nous a permis de recruter le post-doc Sourya Joyee De.

Par ailleurs, j'étais aussi partenaire (responsable d'une thématique) dans d'autres projets, à savoir :

— **ANR STREAMS (2010-2014)** (Solutions pair-à-pair pour le Web social temps réel) L'objectif du projet était de traiter les problèmes liés à la collaboration en temps réel dans le Web social. Ce projet nous a permis de financer la thèse de Bao-Thien Hoang.
Partenaires : INRIA Nancy-Grand Est, IRISA Rennes, LIP6 de Paris.

— **ARC INRIA ACCESS (2010-2012)** (Access Control Policies for XML : Verification, Enforcement and Collaborative Edition)
L'objectif de ce projet était d'étudier les problèmes de sécurité et de contrôle d'accès des données dans les applications et services Web.
Partenaires : INRIA Nancy-Grand Est, INRIA Saclay-Ile de France, INRIA Lille.

— **ARC INRIA RECALL (2006-2007)**(Réplication Optimiste pour l'Edition CoLLaborative)
L'objectif de l'ARC était de développer des algorithmes de réplication optimiste adaptés à l'édition collaborative massive. Ces algorithmes doivent permettre le déploiement des applications collaboratives classiques sur des réseaux P2P.
Partenaires : INRIA Nancy-Grand Est, LIRMM de Montpellier, IRISA de Rennes, LIP6 de Paris.

— **ARA SSIA COPS (2006-2008)** (Composition Of Policies and Services)
L'objectif de ce projet était de construire des techniques formelles pour la conception et l'analyse de politiques de sécurité pour les web services.
Partenaires : INRIA Nancy-Grand Est, IRIT de Toulouse, LIM de Marseille, MicroSoft R & D.

4.4.2 Séminaires et écoles de chercheurs

— Animation d'une série de séminaires, portant sur la "Réplication de Données Dans les Réseaux Pair-à-Pair (P2P)", au département d'informatique de la faculté des sciences d'Oran, Algérie (entre 2009 et 2011).

— Animation d'un cours intitulé "Access Control Models for Querying and Updating XML Data" dans le cadre de l'école doctorale de printemps "Trustworthy and Secure Service Composition" qui s'est déroulée, au mois de mai 2013, à l'Université de Malaga en Espagne.

4.4.3 Expertises

— En 2011, j'étais membre du comité de sélection sur le poste 27 MCF 0840 à l'Université de Franche-Comté de Besançon.

— Expert auprès de l'Association Nationale de la Recherche (ANR) pour l'évaluation des projets de recherche sur la cyber-sécurité.

— Expert pour les projets CIFRE auprès de l'Association Nationale de la Recherche et de la Technologie (ANRT).

— Expert pour Mitacs (organisme national de recherche au Canada) pour évaluer des projets de recherche portant sur la cyber-sécurité.

— Consultant auprès de la Fondation MAIF pour la rédaction d'articles portant sur la vulgarisation scientifique.

— Intervenant auprès de la CNIL pour parler de l'éthique numérique quant à la collecte des données sociales à des fins purement scientifiques.

— Membre du comité scientifique du "Groupement d'Intérêt Scientifique (InterOP Grande-Région)" (2010-2012). J'étais également le représentant de l'Université Nancy 2 dans ce groupement.

4.4.4 Participation à un réseau de recherche

— Je suis membre dans la chaire EFNUM (Économie, Finance et Numérique) qu'occupe l'économiste Pr Tadjeddine Yamina (Université de Lorraine). Avec Tadjeddine Yamina, nous menons une réflexion pour concevoir des stratégies basées sur les techniques de Machine Learning et ce pour identifier des situations de fraude dans les crypto-actifs, liées à des failles de la règlementation en vigueur et des infrastructures informatiques. De cette collaboration est né le club étudiants-chercheurs "Économie,

Finances, Numérique" dans le cadre du projet Orion (Oser la Recherche durant la formatION) de Lorraine Université d'Excellence (LUE). Nous avons également déposé un projet ANR intitulé "Crypto criminalité" et en voie de monter un réseau national et européen pour soumettre un projet européen. Par ailleurs, LUE a accepté notre soumission pour un projet de recherche d'aide à la dynamique interdisciplinaire pour un budget de 150 000 euros.

— Je suis membre dans le groupe de travail sur la détection des fraudes dans les transactions financières, animé par Mme Asma Cherif, Professeure Associée à l'Université du Roi Abdulaziz (Jeddah, Arabie Saoudite). Ce groupe mène actuellement des réflexions pour résoudre le problème de détection de la fraude par carte de crédit sous plusieurs angles, à savoir : (i) la méthode d'apprentissage automatique utilisée et son efficacité pour résoudre le problème de détection, (ii) le déséquilibre des classes et son impact sur la classification des données. Nous avons publié cette année un article journal qui passe en revue les techniques existantes pour détecter les fraudes et propose de nouvelles directions de recherche dans ce domaine.

— J'ai participé à un réseau de chercheurs européens (Allemagne, Autriche, Espagne, France, Pologne, Portugal) sur la conception d'outils basés sur l'intelligence artificielle pour la protection et la prévention contre le cyber-harcèlement chez les femmes et les adolescents ainsi que la protection de la vie privée dans les applications mobiles. Nous avons soumis deux projets européens H2020 (2019 et 2020) qui n'ont malheureusement pas été retenus.

— J'étais membre dans le groupe de travail "Secure Society" pour l'Université Internationale de la Grande Région (UniGR) (2018-2019). Ce groupe formait un réseau de chercheurs en cyber sécurité venant des universités européennes : France (Université de Lorraine), Luxembourg (Université du Luxembourg), Belgique (Université de Liège), et Allemagne (Universités de Kaiserslautern, Trier et Munich). Ce réseau participait à la création de l'université européenne en proposant des formations diplômantes (Licence, Master, Doctorat) portant sur les thèmes de la cyber sécurité.

— J'étais membre dans le comité scientifique du "Groupement d'Intérêt Scientifique (InterOP Grande-Région)" (2010-2012). J'étais également le représentant de l'Université Nancy 2 dans ce groupement.

4.4.5 Vulgarisation

J'ai cofondé avec les collègues Sophie Bereau (Pr en Economie à l'UL), Nazim Fatès (CR Inria de Nancy) et Yamina Tadjeddine (Pr en Economie à l'UL) le club étudiants-chercheurs "Economie, Finances, Numérique" dans le cadre du projet Orion (Oser la Recherche durant la formatION) de Loraine Université d'Excellence (LUE)[16].

J'ai rédigé des articles dans des magazines pour la vulgarisation des résultats de mes recherches : Ercim News, la revue Préventique[17], News de la Fondation Maif.

Pour sensibiliser les internautes autour des risques liés à la divulgation des données personnelles dans les réseaux sociaux, j'ai participé à des reportages animés par la Fondation Maif et l'équipe "L'esprit Sorcier"[18].

16. https://factuel.univ-lorraine.fr/node/19140
17. http://crd.ensosp.fr/index.php?lvl=notice_display&id=27865
18. https://www.lespritsorcier.org/dossier-semaine/objets-connectes/

PUBLICATIONS

5.1 Revues internationales à comité de lecture

1. A. CHERIF, A. BADHIB, H. AMMAR, S. ALSHEHRI, M. KALKATAWI and A. IMINE. "Credit card fraud detection in the era of disruptive technologies : A systematic review". *Computer and Information Sciences - Journal of King Saud University*, 35(1) : 145-174, Elsevier, 2023.

2. N. ALSULAMI, A. CHERIF and A. IMINE. "Collaborative editing over opportunistic networks". *International Journal of Ad Hoc and Ubiquitous Computing*, 39(3) : 141-156, Inderscience, 2022.

3. M. ALGHAMDI, A. CHERIF and A. IMINE. "EdgeDoc : An edge-based distributed collaborative editing system". *Pervasive and Mobile Computing Journal*, 79 : 101-121, Elsevier, 2021.

4. M. D. MECHAOUI and A. IMINE. "Lightweight Coordination Model for Mobile Collaborative Mapping". *International Journal of Communication Networks and Distributed Systems*, 26(3) : 334-366, Inderscience, 2021.

5. S. J. DE and A. IMINE. "Consent for targeted advertising : the case of Facebook". *Journal of AI and Society*, 35(4) : 1055-1064, Springer, 2020.

6. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Inferring attributes with picture metadata embeddings'. *Journal of ACM SIGAPP Applied Computing Review*, 20(2) :36-45, 2020.

7. N. GUETMI and A. IMINE. "Cloud Patterns for Mobile Collaborative Applications". *International Journal of Intelligent Information and Database Systems*, 10(3/4) :191-223, Inderscience, 2017.

8. H.H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Network Structure Release under Differential Privacy". *Journal of Transactions on Data Privacy*, 9(3) :215-241, 2016.

9. M. D. MECHAOUI, N. GUETMI and A. IMINE. "MiCa : Lightweight and mobile collaboration across a collaborative editing service in the cloud". *Journal Peer-to-Peer Networking and Applications*, 9(6) : 1242-1269, Springer, 2016.

10. H. MAHFOUD and A. IMINE. "Efficient Querying of XML Data Through Arbitrary Security Views". *Journal of Transactions Large-Scale Data- and Knowledge-Centered Systems*, 22 : 75-114, Springer, 2015.

11. A. RANDOLPH, H. BOUCHENEB, A. IMINE and A. QUINTERO. "On Synthesizing a Consistent Operational Transformation Approach". *Journal IEEE Transactions on Computers Journal*, 64(4) : 1074-1089, 2015.

12. M. AHMAD, A. IMINE and H. MAHFOUD. "A Highly Concurrent Replicated Data Structure". *Journal EAI Endorsed Trans. Collaborative Computing*, 1(6) : e4, 2015.

13. A. CHERIF, A. IMINE and M. RUSINOWITCH. “Practical access control management for distributed collaborative editors”. *Journal Pervasive and Mobile Computing Journal*, 15 : 62-86, Elsevier, 2014.
14. A. IMINE, “Component-based Specification of Collaborative Objects”. Electronic Notes in Theoretical Computer Science 168 :175-190 2007.
15. A. IMINE, M. RUSINOWITCH, G. OSTER and P. MOLLI. “Formal Design and Verification of Operational Transformation Algorithms for Copies Convergence”. *Journal of Theoretical Computer Science (TCS)*, 351(2) :167-183, 2006.
16. A. IMINE and P. URSO. “Automatic Detection of Copies Divergence in Collaborative Editing Systems”. Electr. Notes Theor. Comput. Sci. 80 :1-17, 2003.
17. A. IMINE, P. MOLLI, G. OSTER and P. URSO. “VOTE : Group Editors Analyzing Tool : System Description”. Electr. Notes Theor. Comput. Sci. 86(1) :1-9, 2003.
18. A. IMINE, P. MOLLI, G. OSTER and M. RUSINOWITCH. “Development of Transformation Functions Assisted by Theorem Prover”. IEEE Distributed Systems Online, pages 1-9, November, 2002.

5.2 Revues nationales à comité de lecture

1. A. RANDOLPH, A. IMINE, H. BOUCHENEB and A. QUINTERO. “Spécification et Analyse d’un Protocole de Contrôle d’Accès Optimiste pour des Editeurs Collaboratifs Répartis”. *Journal Ingénierie des Systèmes d’Information*, 19(6) : 9-32, 2015.

5.3 Ouvrages

1. S. J. DE and A. IMINE. “Privacy Risk Analysis of Online Social Networks”. *Privacy Risk Analysis. Synthesis Lectures on Information Security, Privacy, & Trust*, Morgan & Claypool Publishers, 2020.

5.4 Edition d’ouvrages

1. A. IMINE, J. M. FERNANDEZ, J. M. MARION, L. LOGRIPPO and J. GARCIA-ALFARO. “Foundations and Practice of Security - 10th International Symposium, FPS 2018”. *Lecture Notes in Computer Science 10723*, Springer, 2018.

5.5 Chapitres d’ouvrage

1. M. D. MECHAOUI and A. IMINE. “Concurrency Control for Mobile Collaborative Applications in Cloud Environments”. *In the book “Advances in Mobile Cloud Computing and Big Data under the 5G Era”*, Springer, 2017.
2. A. CHERIF and A. IMINE. “Optimistic Access Control for Collaborative Applications”. *In the Handbook of Research on Innovations in Access Control and Management*, IGI Global, 2016.
3. N. GUETMI and A. IMINE. “Designing Mobile Collaborative Applications for Cloud Environments”. *Modern Software Engineering Methodologies for Mobile and Cloud Environments*, IGI Global, 2016.

5.6 Magazines avec comité de lecture

1. A. IMINE. "La recherche pour défendre nos vies privées : appel à la vigilance sur les réseaux sociaux". *Revue Préventique*, Num. 156, Janvier, 2018.

2. N. GUETMI, M. D. MECHAOUI and A. IMINE. "Resilient Collaboration for Mobile Cloud Computing". *ERCIM News*, No. 102, 2015.

3. A. IMINE and M. RUSINOWITCH. "Secure Collaboration for Smartphones". *ERCIM News*, No. 93, 2013.

5.7 Conférences invitées

1. A. IMINE and M. RUSINOWITCH. "Applying a Theorem Prover to the Verification of Optimistic Replication Algorithms". *Workshop on Rewriting, Cachan, June 20-21, 2007 Proceedings in LNCS 4600, Springer Verlag*.

5.8 Conférences internationales avec comité de sélection

1. N.D. FERREYRA, A. IMINE, M.C. VIDONI, and R. SCANDARIATO. "Developers Need Protection, Too : Perspectives and Research Challenges for Privacy in Social Coding Platforms". *To appear in The 16th International Conference on Cooperative and Human Aspects of Software Engineering (CHASE 2023)*, Melbourne, Australia, 14-15 May, 2023.

2. A.E. LAOUIR and A. IMINE. "On Privacy of Multidimensional Data Against Aggregate Knowledge Attacks". *The 16th International Conference on Privacy in Statistical Databases (PSD 2022)*, LNCS 13463, pp. 92–104, Paris, France, September 21-23, 2022.

3. K. MACWAN, A. IMINE and M. RUSINOWITCH. "Differentially Private Friends Recommendation". *to appear in The 15th International Symposium on Foundations and Practice of Security (FPS 2022)*, Ottawa, Canada, 2022.

4. K. MACWAN, A. IMINE and M. RUSINOWITCH. "Privacy Preserving Recommendations for Social Networks". *The 9th International Conference on on Social Networks Analysis, Management and Security (SNAMS 2022)*, IEEE Publisher, pp. 1-8, Milan, Italy, 2022.

5. A. CHERIF, S. ALSHEHRI, M. KALKATAWI and A. IMINE. "Towards an intelligent adaptive security framework for preventing and detecting credit card fraud". *The 19th ACS/IEEE International Conference On Computer Systems And Applications (AICCSA)*, pp. 1-8, Abu Dhabi, United Arab Emirates, December 5-8, 2022.

6. B. AL-ZAHRANI, S. ALSHEHRI, A. CHERIF and A. IMINE. "Property Graph Access Control Using View-Based and Query Rewriting Approaches". *The 19th ACS/IEEE International Conference On Computer Systems And Applications (AICCSA)*, pp. 1-2, Abu Dhabi, United Arab Emirates, December 5-8, 2022.

7. N. BELHADJ-CHEIKH, A. IMINE and M. RUSINOWITCH. "FOX : Fooling with Explanations - Privacy Protection with Adversarial Reactions in Social Media". *The 18th Annual Conference on Privacy, Security and Trust (PST)*, IEEE Publisher, pp. 1-10, Auckland, New Zealand, December 13-15, 2021.

8. S. EIDIZADEHAKHCHELOO, B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Divide-and-Learn : A Random Indexing Approach to Attribute Inference Attacks in Online Social Networks". *The 35th IFIP Data and Applications Security and Privacy Conference (DBSec)*, (LNCS 12840), pp. 338-354, Calgary, Canada, July 19-20, 2021.

9. A. ALLAHIM, A. CHERIF and A. IMINE. "A Hybrid Approach for Optimizing Arabic Semantic Query Expansion". *The 18th ACS/IEEE International Conference On Computer Systems And Applications (AICCSA)*, pp. 1-8, Tangier, Morocco, November 30 - Dec. 3, 2021.

10. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Online Attacks on Picture Owner Privacy". *The 31th International Conference of Database and Expert Systems Applications (DEXA)*, (LNCS 12392), pp. 33-47, Bratislava, Slovakia, September 14-17, 2020.

11. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "You are what Emojis say about your Pictures : Language-independent Gender Inference Attack on Facebook". *The 35th ACM Symposium on Applied Computing (SAC), Social Network and Media Analysis Track*, Brno, Czech Republic, March 30-April 3, 2020.

12. B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Gender Inference for Facebook Picture Owners". *The 16th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, Linz, Vienna, August 26-29, 2019.

13. O. ABUSALEM, A. CHERIF and A. IMINE. "Towards Optimistic Access Control In cloud-Based-Collaborative Editors". *The 16th ACS/IEEE International Conference On Computer Systems And Applications (AICCSA)*, Abu Dhabi, UAE, November 3-7, 2019.

14. N. ALGHAMDI, A. CHERIF and A. IMINE. "Towards An Edge-Based Architecture For Real-Time Collaborative Editors". *The 16th ACS/IEEE International Conference On Computer Systems And Applications (AICCSA)*, Abu Dhabi, UAE, November 3-7, 2019.

15. S. J. DE and A. IMINE. "Enabling Users to Balance Social Benefit and Privacy in Online Social Networks". *The 16th Annual Conference on Privacy, Security and Trust (PST)*, IEEE Publisher, Belfast, Northern Ireland, UK, August 28-30, 2018.

16. S. J. DE and A. IMINE. "On Consent in Online Social Networks : Privacy Impacts and Research Directions". *The 13th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Arcachon, France, October 16-18, 2018.

17. S. J. DE and A. IMINE. "To Reveal or Not To Reveal : Balancing User-Centric Social Benefit and Privacy in Online Social Networks". *The 33th ACM Symposium on Applied Computing (SAC), Privacy by Design Track*, Pau, France, April, 2018.

18. S. J. DE and A. IMINE. "Privacy Scoring of Social Network User Profiles through Risk Analysis". *The 12th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, (LNCS 10694), Dinard, France, September, 2017.

19. Y. ABID, A. IMINE, A. DI NAPOLI, C. RAISSI and M. RUSINOWITCH. "Two-Phase Preference Disclosure in Attributed Social Networks". *The 28th International Conference of Database and Expert Systems Applications (DEXA)*, (LNCS 10438), Lyon, France, August, 2017.

20. N. ALSULAMI, A. CHERIF and A. IMINE. "Evaluating Data Convergence of Collaborative Editors in Opportunistic Networks". *The 6th International Conference on Information and Communication Technology and Accessibility (ICTA)*, Muscat, Sultanate of Oman, December, 2017.

21. Y. ABID, A. IMINE, A. DI NAPOLI, C. RAISSI and M. RUSINOWITCH. "Online link disclosure strategies for social networks". *The 11th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, (LNCS 10158), Roscoff, France, September, 2016.

22. A. CHERIF and A. IMINE. "Using CSP for Coordinating Undo-Based Collaborative Applications". *The 2016 ACM Symposium on Applied Computing (SAC)*, pages 1928-1935, Pisa, Italy, April, 2016.

23. B. T. HOANG and A. IMINE. "Efficient and Decentralized Polling Protocol for General Social Networks". *The International Conference Stabilization, Safety, and Security of Distributed Systems (SSS)*, (LNCS 9212), pages 171-186, Edmonton, Canada, August, 2015.

24. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Differentially Private Publication of Social Graphs at Linear Cost". *In IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pp. 596 - 599, August 25 - 28, Paris, France, 2015.

25. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Anonymizing Social Graphs via Uncertainty Semantics". *In International ACM Conference on Computer and Communications Security (ASIA CCS)*, pages 495-506, April 14 - 17, Singapore, 2015.

26. N. GUETMI, M. D. MECHAOUI, A. IMINE and B. LADJEL. "Mobile Collaboration : a Collaborative Editing Service in the Cloud". *In International ACM Symposium on Applied Computing (ACM SAC)*, pp. 509-512, April 14 - 17, Barcelone, 2015.

27. M. AHMAD and A. IMINE. "Decentralized Collaborative Editing Platform". *In IEEE International Conference on Mobile Data Management (MDM)*, pp. 323-326, Pittsburgh, PA, USA, June 15-18, 2015.

28. N. GUETMI and A. IMINE. "A Cloud-Based Reusable Design for Mobile Data Sharing". *In Model and Data Engineering - 5th International Conference, (MEDI)*, (LNCS 9344), pp. 62-73, Rhodes, Greece, September 26-28, 2015.

29. M. D. MECHAOUI, N. GUETMI and A. IMINE. "Towards Real-Time Co-authoring of Linked-Data on the Web". *In the 5th IFIP TC 5 International Conference on Computer Science and its Applications (CIIA)*, Saida, Algeria, May 20-21, pp 538-548, 2015.

30. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "A Maximum Variance Approach for Graph Anonymization". **(BEST PAPER)**, *In International Symposium on Foundations and Practice of Security (FPS)*, pp. 49-64, (LNCS 8930), Montreal, Canada, 2014.

31. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Enforcing Privacy in Decentralized Mobile Social Networks". *In International Symposium on Engineering Secure Software and Systems (Essos)*, February 26 - 28, Munich, Germany, 2014.

32. H. MAHFOUD, A. IMINE and M. RUSINOWITCH. "SVMAX : a system for secure and valid manipulation of XML data". *In 17th International Database Engineering and Applications Symposium (IDEAS)*, pp. 154-161, ACM Publisher, October 9 - 11, Barcelona, Spain, 2013.

33. B. T. HOANG and A. IMINE. "On Constrained Adding Friends in Social Networks". *In Social Informatics - 5th International Conference (SocInfo)*, pp. 467-477, (LNCS 8238), Kyoto, Japan, November 25-27, 2013.

34. H. MAHFOUD and A. IMINE. "On Securely Manipulating XML Data". *In Foundations and Practice of Security - 5th International Symposium (FPS)*, pp. 293-307, (LNCS 7743), Montreal, QC, Canada, October 25-26, 2012.

35. B. T. HOANG and A. IMINE. "On the Polling Problem for Social Networks". *In Principles of Distributed Systems, 16th International Conference (OPODIS)*, pp. 46-60, (LNCS 7702), Rome, Italy, December 18-20, 2012.

36. H. MAHFOUD and A. IMINE. "Secure querying of recursive XML views : a standard XPath-based technique". *In the 21st ACM World Wide Web Conference (WWW)*, Lyon, France, April 16-20, pages 575-576, 2012.

37. A. CHERIF, A. IMINE and M. RUSINOWITCH. "Optimistic access control for distributed collaborative editors". *In the 2011 ACM Symposium on Applied Computing (SAC)*, TaiChung, Taiwan, March 21 - 24, pages 861-868, 2011.

38. J. P. ACHARA, A. IMINE and M. RUSINOWITCH. "DeSCal - Decentralized Shared Calendar for P2P and Ad-Hoc Networks". *In 10th IEEE International Symposium on Parallel and Distributed Computing (ISPDC)*, Cluj-Napoca, Romania, July 6-8, pages 223-231, 2011.

39. M. D. MECHAOUI, A. IMINE and F. BENDELLA. "Un Modèle Générique de Garbage Collection pour les Editeurs Collaboratifs Basé sur l'Approche TO dans les environnements P2P et mobiles". *In the Third International Conference on Computer Science and its Applications (CIIA)*, Saida, Algeria, December 13-15, 2011, pages 1-10, 2011.

40. Z. AHMAD, A. IMINE and M. RUSINOWITCH. "Safe and Efficient Strategies for Updating Firewall Policies". *Trust, Privacy and Security in Digital Business, 7th International Conference, TrustBus 2010*, (LNCS 6264), Spain, August 30-31, 2010

41. H. BOUCHENEB, A. IMINE and M. NAJEM. "Symbolic Model-Checking of Optimistic Replication Algorithms". *The 8th International Conference of Integrated Formal Methods, IFM 2010,* (LNCS 6396), Nancy, France, 11-14 October , 2010.

42. M. D. MECHAOUI, A. CHERIF, A. IMINE and F. BENDELLA. "Log Garbage Collector-based Real Time Collaborative Editor for Mobile Devices". *The 6th International Conference on Collaborative Computing : Networking, Applications and Worksharing, CollaborateCom 2010*, Hotel Allegro, Chicago, Illinois, USA, October 9-12, 2010.

43. A. IMINE. "Coordination Model for Real-Time Collaborative Editors". *Coordination Models and Languages, 11th International Conference, COORDINATION 2009* (LNCS 5521), Lisboa, Portugal, June 9-12, 2009.

44. H. BOUCHENEB and A. IMINE. “On Model-Checking Optimistic Replication Algorithms”. *Formal Techniques for Distributed Systems, Joint 11th IFIP WG 6.1 International Conference FMOODS 2009 and 29th IFIP WG 6.1 International Conference FORTE 2009*, (LNCS 5522), Lisboa, Portugal, June 9-12, 2009, pages 73-89.

45. A. CHERIF and A. IMINE. “Undo-Based Access Control for Distributed Collaborative Editors”. *In Proceedings of Cooperative Design, Visualization, and Engineering, 6th International Conference, CDVE 2009* (LNCS 5738), pages 101-108, Luxembourg, September 20-23, 2009.

46. A. IMINE. “Decentralized concurrency control for real-time collaborative editors”. *In Proceedings of the 8th international conference on New technologies in distributed systems, NOTERE 2008*, June 23-27, 2008, Lyon, France, ACM Publisher.

47. G. OSTER, P. URSO, P. MOLLI and A. IMINE. “Data Consistency for P2P Collaborative Editing”. *In Proceedings of the 2006 ACM Conference on Computer Supported Cooperative Work, CSCW 2006*, Banff, Alberta, Canada, pages 259-268, November 4-8, 2006.

48. G. OSTER, P. URSO, P. MOLLI and A. IMINE. “Tombstone Transformation Functions for Ensuring Consistency in Collaborative Editing Systems”. *In The Second International Conference on Collaborative Computing : Networking, Applications and Worksharing (CollaborateCom 2006)*, Atlanta, Georgia, USA, pages 1-10, November 2006.

49. A. IMINE, M. RUSINOWITCH, G. OSTER and P. MOLLI. “Towards Synchronizing Linear Collaborative Objects with Operational Transformation”. *Formal Techniques for Networked and Distributed Systems - FORTE 2005, 25th IFIP WG 6.1 International Conference*, (LNCS 3731), pages 411-427, Taipei, Taiwan, October 2-5, 2005.

50. A. IMINE, P. MOLLI, G. OSTER and M. RUSINOWITCH. “Deductive Verification of Operational Transformation Algorithms”. *In 10th International Conference on Algebraic Methodology And Software Technology (AMAST’2004)* (LNCS 3116), pages 226-240, July 12th - 16th, 2004, Stirling, Scotland, UK.

51. D. DÉHARBE, A. IMINE and S. RANISE. “Abstraction-Driven Verification of Array Programs”. *the 7th International Conference on Artificial Intelligence and Symbolic Computation* (AISC’04), (LNCS 3249), LNCS vol. 3249, pages 271-275, Linz, Austria, September 2004.

52. P. MOLLI, , G. OSTER, H. SKAF-MOLLI and A. IMINE. “Using the Transformational Approach to Build a Safe and Generic Data Synchronizer”. *Proceedings of the 2003 international ACM SIGGROUP conference on Supporting group work*, pp. 212–220, Sanibel Island, Florida, USA, November 2003.

53. A. IMINE, P. MOLLI, G. OSTER and M. RUSINOWITCH. “Proving Correctness of Transformation Functions in Real-Time Groupware”. *Proceedings of The 8th European Conference on Computer-Supported Cooperative Work, (ECSCW’03)*. pp. 277–294, Helsinki, Finland, September 2003.

54. A. IMINE and S. RANISE. “Building Satisfiability Procedures for Verification : The Case Study of Sorting Algorithms”. *Proc. of the International Symposium on Logic-based Program Synthesis and Transformation (LOPSTR’03)*, pages 65-80, Uppsala, Sweden, August 2003.

55. Y. SLIMANI, A. IMINE, B. DJELLALI and L. SEKHRI. "Modelling and Verifying Parallel Programs". *THE Tenth International Symposium on Computer and Information Sciences (ISCIS'95)*, Izmir,Turkey, October 30 - November 1, 1995.

56. Y. SLIMANI, A. IMINE, B. DJELLALI and L. SEKHRI. "Designing Parallel Programs". *The Second Annual Joint Conference on Information Science (JCIS'95)*, North Carolina, USA, September 28 - October 1, 1995.

57. Y. SLIMANI, A. IMINE, B. DJELLALI and L. SEKHRI. "Reliability Enhancement of Parallel and Distributed Programs". *The Second Annual Joint Conference on Information Science (JCIS'95)*, North Carolina, USA, September 28 - October 1, 1995.

58. Y. SLIMANI, A. IMINE, B. DJELLALI and L. SEKHRI. "Detecting Stable Properties in Occam Programs". *The Fifth International Conference on Parallel Computing (PARCO'95)*, Gent, Belgium, September 19-22, 1995.

5.9 Workshops internationaux avec comité de sélection

1. S. EIDIZADEHAKHCHELOO, B. ALIPOUR PIJANI, A. IMINE and M. RUSINOWITCH. "Your Age Revealed by Facebook Picture Metadata". *The Second International Workshop on BI and Big Data Applications, BBIGAP 2020, in conjunction with ADBIS 2020 Conference*, Springer vol. 1260, pp. 259-270, Lyon, France, August, 2020.

2. Y. ABID, A. IMINE and M. RUSINOWITCH. "Online Testing of User Profile Resilience Against Inference Attacks in Social Networks". *The First International Workshop on Advances on Big Data Management, Analytics, Data Privacy and Security, BigDataMAPS 2018, in conjunction with ADBIS 2018 Conference*, Budapest, Hungary, September, 2018.

3. Y. ABID, A. IMINE and M. RUSINOWITCH. "Sensitive attribute prediction for social networks users". *The 2nd International workshop on Data Analytics solutions for Real-LIfe Applications (DARLI-AP), in conjunction with EDBT/ICDT 2018 Joint Conference*, Vienna, Austria, March, 2018.

4. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Detecting Communities under Differential Privacy". *the 15th ACM Workshop on Privacy in the Electronic Society (WPES)*, October 24, Vienna, Austria, 2016.

5. A. CHERIF and A. IMINE. "A Constraint-based Approach for Generating Transformation Patterns". *In International Workshop on Foundations of Coordination Languages and Self-Adaptive Systems (FOCLASA'2015)*, pp. 48-62 (EPTCS 201), Madrid, Spain, April, July, 2015.

6. M. D. MECHAOUI, N. GUETMI and A. IMINE. "Mobile Co-Authoring of Linked Data in the Cloud". *In New Trends in Databases and Information Systems – (ADBIS) Workshop OAIS*, pp. 371-381, Volume 539, Springer, Poitiers, France, 2015.

7. A. RANDOLPH, A. IMINE, H. BOUCHENEB and A. QUINTERO. "Specification and Verification Using Alloy of Optimistic Access Control for Distributed Collaborative Editors". *In Formal Methods for Industrial Critical Systems - 18th International Workshop (FMICS)*, pp. 184-198, LNCS 8187, Madrid, Spain, September, 2013.

8. H. MAHFOUD and A. IMINE. "A General Approach for Securely Updating XML Data". *In Proceedings of the 15th International Workshop on the Web and Databases (WebDB)*, Scottsdale, AZ, USA, May 20, pages 55-60,2012.

9. A. RANDOLPH, H. BOUCHENEB, A. IMINE and A. QUINTERO. "On Consistency of Operational Transformation Approach". *In 14th International Workshop on Verification of Infinite-State Systems (Infinity)*, Paris, France, 27th August, pages 45-59, 2012.

10. A. IMINE, H. BOUCHENEB and M. RUSINOWITCH. "Enforcing Commutativity Using Operational Transformations". *In Workshop on Verification of Concurrent Data-Structures (VERICO), Co-located with POPL'2011*, Austin, Texas, USA, January 29, 2011.

11. A. IMINE, "On Coordinating Collaborative Objects". *In Proceedings 9th International Workshop on Foundations of Coordination Languages and Software Architectures (FOCLASA'2010)*, Electronic Proceedings in Theoretical Computer Science 30 :78-92 (2010).

12. A. IMINE, A. CHERIF and M. RUSINOWITCH. "A Flexible Access Control Model for Distributed Collaborative Editors". *In Proceedings of Secure Data Management, 6th VLDB Workshop, SDM 2009*, Lyon, France, August 28, 2009. Proceedings. Lecture Notes in Computer Science 5776, pages 89-106.

13. A. IMINE. "Flexible Concurrency Control for Real-Time Collaborative Editors". *In Proceedings of the 28th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2008 Workshops)*, 17-20 June 2008, Beijing, China. IEEE Computer Society, pages 423-428.

5.10 Conférences nationales avec comité de lecture

1. H. H. NGUYEN, A. IMINE and M. RUSINOWITCH. "Towards Differentially Private Community Detection". *32ème Conférence sur la Gestion de Données (BDA)*, 15-18 Novembre, Poitiers, France, 2016.

2. Y. ABID, A. IMINE, A. DI NAPOLI, C. RAISSI and M. RUSINOWITCH. "Stratégies de divulgation de lien en ligne pour les réseaux sociaux". *32ème Conférence sur la Gestion de Données (BDA)*, 15-18 Novembre, Poitiers, France, 2016.

3. Y. ABID, A. IMINE, A. DI NAPOLI, C. RAISSI, M. RIGOLOT and M. RUSINOWITCH. "Analyse d'activité et exposition de la vie privée sur les médias sociaux". *16èmes journées Francophones Extraction et Gestion des Connaissances (EGC)*, Reims, France, Janvier 2016.

4. H. MAHFOUD, A. IMINE. "On Securely Manipulating XML Data". *28ème Journées Bases de Données Avancées (BDA)*, Clermont-Ferrand, France, Octobre 2012.

5. G. OSTER, P. URSO, P. MOLLI and A. IMINE. "Edition collaborative sur réseau pair-à-pair à large échelle". *Journées Francophones sur la Cohérence des Données en Univers Réparti, (CDUR'05)*, pages 1-9, Paris, France, Novembre 2005.

6. G. OSTER, P. MOLLI, H. Skaf-Molli and A. IMINE. "Un modèle sûr et générique pour la synchronisation de données divergentes". Premières Journées Francophones : Mobilité et Ubiquité 2004, pages 1-6, Mardi 1-3 juin 2004, Nice, Sophia-Antipolis.

7. A. IMINE, Y. SLIMANI and S. STRATULAT. "Using Automated Induction-based Theorem Provers for Reasoning on Concurrent Systems". *Proceedings of Onzièmes Journées Francophones de Programmation Logique et Programmation par Contraintes (JFPLC'02)*, pp. 71-85, Hermès Science Publications. Nice, France, May 27-30, 2002.

5.11 Thèses

1. *Partage de Données dans les Systèmes Collaboratifs. De la synchronisation à la protection de données.* Habilitation à Diriger des Recherches. LORIA INRIA Lorraine, Décembre 2016.

2. *Conception Formelle d'Algorithmes de Réplication Optimiste. Vers l'Edition Collaborative dans les Réseaux Pair-à-Pair.* Thèse de Doctorat. LORIA INRIA Lorraine, Décembre 2006.

3. *Spécification et Analyse de Programmes Parallèles.* Thèse de Magistère. Université des Sciences et de la Technologie d'Oran (Algérie), Novembre 1995.

5.12 Rapports de recherche

1. B. T. HOANG and A. IMINE. "On the Polling Problem for Social Networks". *Rapport de Recherche RR-8055*, INRIA Nancy-Grand Est, October 2012.
2. H. MAHFOUD and A. IMINE. "A General Approach for Securely Querying and Updating XML Data". *Rapport de Recherche RR-7870*, INRIA Nancy-Grand Est, January 2012.
3. H. MAHFOUD and A. IMINE. "Secure Querying of Recursive XML Views : A Standard XPath-based Technique". *Rapport de Recherche RR-7834*, INRIA Nancy-Grand Est, December 2011.
4. A. IMINE, A. CHERIF and M. RUSINOWITCH. "An Optimistic Mandatory Access Control Model for Distributed Collaborative Editors". *Rapport de recherche RR-6939*, INRIA Lorraine, February 2009.
5. Z. AHMAD, A. IMINE and M. RUSINOWITCH. "Safe and Efficient Strategies for Updating Firewall Policies". *Rapport de recherche RR-6940*, INRIA Lorraine, Mai 2009.
6. H. BOUCHENEB and A. IMINE. "Experiments in Model-Checking Optimistic Replication Algorithms". *Rapport de recherche RR-6510*, INRIA Lorraine, Avril 2008.
7. G. OSTER, P. URSO , P. MOLLI, H. SKAF-MOLLI and A. IMINE. "Optimistic replication for massive collaborative editing". *Rapport de recherche RR-5719*, INRIA Lorraine, October 2005.
8. G. OSTER, , P. URSO , P. MOLLI and A. IMINE. "Real time group editors without operational transformation". *Rapport de recherche RR-5580*, INRIA Lorraine, May 2005.
9. A. IMINE, P. MOLLI, G. OSTER and M. RUSINOWITCH. "Achieving Convergence with Operational Transformation in Distributed Groupware Systems". *Rapport de Recherche RR-5188*, INRIA, Mai 2004.
10. P. MOLLI, H. SKAF-MOLLI, G. OSTER and A. IMINE. "Safe Generic Data Synchronizer". *Rapport de Recherche A03-R-062*, LORIA, Nancy (France), Mai 2003.