



HAL
open science

Réseau social anonyme de confiance dédié aux applications communautaires du futur : une approche guidée par le capital social

Chayma Sellami

► To cite this version:

Chayma Sellami. Réseau social anonyme de confiance dédié aux applications communautaires du futur : une approche guidée par le capital social. Autre [cs.OH]. ISAE-ENSMA Ecole Nationale Supérieure de Mécanique et d'Aérotechnique - Poitiers, 2022. Français. NNT : 2022ESMA0024 . tel-03967427

HAL Id: tel-03967427

<https://theses.hal.science/tel-03967427>

Submitted on 1 Feb 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THÈSE CIFRE

pour l'obtention du Grade de
Docteur de l'École Nationale Supérieure de Mécanique et
d'Aérotechnique

Présentée par :

Chayma SELLAMI

**Réseau Social Anonyme de Confiance Dédié aux
Applications Communautaires du Futur : Une Approche
Guidée par le Capital Social**

Directeurs de thèse : **Allel HADJALI**

Co-encadrants de thèse : **Mickaël BARON, Mounir BECHCHI, Stéphane JEAN**

Soutenue le 12 Décembre 2022
devant la Commission d'Examen

JURY

| | | |
|-----------------------------|---------------------------------------|--|
| <u>Rapporteurs :</u> | Salima BENBERNOU Richard CHBEIR | Prof. LIPADE, Université Paris Cité Prof. LIUPPA, Université de Pau et des Pays de l'Adour |
| <u>Examineurs :</u> | Djamal BENSLIMANE Slimane HAMMOUDI | Prof. LIRIS, Université Claude Bernard - Lyon Docteur-HDR, ESEO - Angers |
| <u>Invité :</u> | Dominique CHABOT | Président de O°Code |

Remerciements

Il est pour moi très difficile d'écrire les remerciements, non pas parce que les personnes à remercier manquent, mais parce que je dois trouver des formules qui me permettront de témoigner de ma reconnaissance.

Je tiens à remercier tout d'abord les membres du jury, mes rapporteurs Madame Selima BENBERNOU et Monsieur Richard CHBEIR d'avoir accepté d'évaluer et de rapporter ce travail. Merci à eux pour leurs remarques et critiques constructives. Je remercie également Monsieur Djamal BEN SLIMANE et Monsieur Slimane HAMMOUDI d'avoir examiné cette thèse.

Je tiens à remercier mon équipe au laboratoire LIAS, mon directeur de thèse Allel HADJALI et mes encadrants Stéphane JEAN et Mickaël BARON. Je leur adresse mes remerciements pour le temps qu'ils m'ont consacré tout au long de cette période de thèse et le support qu'ils m'ont donné pour atteindre mes objectifs. Sans eux, ce projet ne serait pas ce qu'il est aujourd'hui !

Je tiens à remercier chaleureusement Mounir BECHCHI, mon responsable au sein de l'entreprise. Une personne spéciale, il n'y a pas de mots pour exprimer ma gratitude envers vous. Je vous remercie pour l'apprentissage scientifique mais surtout humain. Je ne peux pas oublier Dominique CHABOT, le président de l'entreprise O°Code, sans lui cette thèse ne pourrait pas être réalisée. C'est lui qui m'a donné l'opportunité de me lancer dans cette aventure. Il a été accueillant, gentil et humain depuis mon premier jour de travail jusqu'à aujourd'hui. Je vous remercie profondément.

Je remercie également tous les membres du LIAS, doctorants, chercheurs et personnel pour leur gentillesse et leur soutien.

Je tiens à exprimer mes remerciements à mes collègues au sein de l'entreprise O°Code, une famille avec laquelle j'ai appris le sens du travail en équipe. Faire une thèse CIFRE n'est pas facile au début. Mais grâce à cette équipe, j'ai pu débloquent progressivement chaque verrou et concilier mes différents domaines de vie ; merci pour sa bienveillance sans faille !

Je tiens à remercier ma famille, ma sœur et mes deux frères, et surtout mes parents. Ils n'ont cessé de m'encourager tout au long de mes études pour atteindre cet objectif. Maman, papa, merci de m'avoir fait confiance, d'avoir toujours fait les choix que vous

avez fait pour nous. Il n'est pas facile de quitter son pays pour atteindre son rêve, mais grâce à ma famille, j'ai pu le faire.

J'ai dû quitter mon petit pays bien aimé, mais j'ai réussi à avoir une deuxième famille ici. Un grand merci à tous mes amis proches qui m'ont apporté soutien et moral pendant toutes ces années : Anas, Safaa, Ishaq, Amine et Issam. Je ne vais pas citer tout le monde pour ne pas risquer d'en oublier, mais je ne peux pas oublier deux meilleures amies comme Nesrine et Ibtissem. Ces personnes m'ont aidé à libérer une énorme quantité de stress.

Pour finir, je remercie les chercheurs scientifiques rencontrés lors des différentes conférences, pour leurs questions et leurs remarques pertinentes. Je remercie l'ANRT pour le financement de ma thèse. Je remercie également toutes les personnes que j'ai pu oublier qui ont contribué de près comme de loin à la réalisation de cette thèse.

Table des matières

- Table des matières** **v**

- Liste des figures** **ix**

- Liste des tableaux** **1**

- Introduction générale** **3**

- I État de l’art** **13**

- 1 Réseaux sociaux et Anonymat** **17**
 - 1.1 Introduction 19
 - 1.1.1 Définition et Historique des réseaux sociaux 19
 - 1.1.2 Notions de base sur les réseaux sociaux 25
 - 1.2 Anonymat 28
 - 1.2.1 Définition de l’anonymat 28
 - 1.2.2 Exemples des systèmes anonymes 29
 - 1.3 Discussion 33

- 2 Confiance : modélisation, typologie et calcul** **37**
 - 2.1 Introduction 39
 - 2.2 Réputation 39
 - 2.3 Recommandation 40
 - 2.4 Capital Social 40
 - 2.4.1 Calcul de la Confiance à partir du Capital Social 43
 - 2.5 Qualités d’une bonne mesure de confiance 45
 - 2.6 Modélisation de la confiance 46

| | | |
|-----------|--|-----------|
| 2.7 | Modèles computationnels | 47 |
| 2.7.1 | Réseaux bayésiens | 48 |
| 2.7.2 | Modèle à valeurs discrètes | 50 |
| 2.7.3 | Modèles basés sur la croyance | 51 |
| 2.7.4 | Modèles flous | 51 |
| 2.7.5 | Modèles de flux | 52 |
| 2.7.6 | Exemples des systèmes basés sur la confiance | 53 |
| 2.7.7 | Approches d'évaluation des modèles computationnels de confiance | 55 |
| 2.8 | Modèles de propagation de la confiance | 56 |
| 2.8.1 | Modèles de visualisation | 56 |
| 2.8.2 | Modèles de recommandation basés sur la confiance | 58 |
| 3 | Systèmes de recommandation : un aperçu | 61 |
| 3.1 | Introduction | 63 |
| 3.2 | Systèmes de recommandation classiques | 63 |
| 3.3 | Systèmes de recommandation basés sur l'IA | 67 |
| II | Contributions | 73 |
| 4 | Un modèle basé sur l'apprentissage hybride pour la recommandation | 75 |
| 4.1 | Introduction | 76 |
| 4.2 | Analyse de l'état de l'art par rapport aux besoins métiers | 78 |
| 4.2.1 | Les besoins métiers | 78 |
| 4.2.2 | Analyse de l'état de l'art | 80 |
| 4.2.3 | Synthèse | 84 |
| 4.3 | Notre approche hybride pour la recommandation | 85 |
| 4.3.1 | Recommandation basée sur un Processus de Décision Markovien (PDM) | 85 |
| 4.3.2 | Principe du Clustering Hiérarchique | 86 |
| 4.3.3 | Fusion des deux techniques | 87 |
| 4.3.4 | Synthèse | 90 |
| 4.4 | Évaluation expérimentale | 91 |
| 4.4.1 | Base de données utilisée | 91 |

| | | |
|----------|---|------------|
| 4.4.2 | Résultats | 92 |
| 4.5 | Conclusion | 94 |
| 5 | Un cadre unifié pour la gestion de la confiance | 97 |
| 5.1 | Introduction | 98 |
| 5.2 | Définitions et Propriétés | 99 |
| 5.2.1 | Confiance | 100 |
| 5.2.2 | Réputation | 103 |
| 5.2.3 | Mesures de la confiance et de la réputation | 105 |
| 5.3 | Modèles computationnels | 106 |
| 5.4 | Les besoins métiers liés à la confiance | 109 |
| 5.5 | Analyse des modèles computationnels selon les besoins métiers | 112 |
| 5.5.1 | Modèle bayésien | 112 |
| 5.5.2 | Modèles basés sur les croyances | 113 |
| 5.5.3 | Modèles à valeur discrète | 113 |
| 5.5.4 | Modèles flous | 113 |
| 5.5.5 | Modèles de flux | 114 |
| 5.5.6 | Synthèse | 115 |
| 5.6 | Expérimentations et Résultats | 116 |
| 5.6.1 | Besoin B_1 : « Bon utilisateur vs. Mauvais utilisateur » | 116 |
| 5.6.2 | Besoin B_2 : « Un nouvel utilisateur vs. un utilisateur avec comportement mi-positif mi-négatif » | 116 |
| 5.6.3 | Besoin B_3 : « Le système se souvient des fraudes » | 117 |
| 5.6.4 | Besoin B_4 : « Récidivisme » | 117 |
| 5.6.5 | Besoin B_5 : « Droit à l'erreur » | 119 |
| 5.6.6 | Besoin B_6 : « Vol d'identité » | 119 |
| 5.7 | Conclusion | 121 |
| 6 | Recommandation du modèle computationnel de confiance : une approche guidée par les besoins métiers | 123 |
| 6.1 | Introduction | 124 |
| 6.2 | Exemple pour illustrer la contribution | 125 |
| 6.3 | Analyse de l'état de l'art par rapport aux besoins métiers | 126 |

| | | |
|-------|---|------------|
| 6.3.1 | Analyse des travaux d'évaluation des modèles computationnels . . . | 126 |
| 6.3.2 | Analyse des besoins applicatifs pour l'évaluation des modèles computationnels | 127 |
| 6.4 | Approche de sélection du modèle computationnel | 128 |
| 6.4.1 | Modélisation des exigences de l'application | 129 |
| 6.4.2 | Modélisation des exigences sur l'évolution de la confiance | 132 |
| 6.4.3 | Recommandation du modèle computationnel de la confiance | 139 |
| 6.5 | Étude de cas | 140 |
| 6.5.1 | Exigences pour l'application de covoiturage | 140 |
| 6.5.2 | Exigences de confiance pour le covoiturage | 141 |
| 6.5.3 | Recommandation du modèle computationnel de confiance | 143 |
| 6.6 | Conclusion et Perspectives | 145 |
| | Conclusion générale | 147 |
| | Bibliographie | 151 |

Liste des figures

| | | |
|------|--|-----|
| 1 | Plan du manuscrit | 10 |
| 1.1 | Chronologie des réseaux sociaux | 23 |
| 1.2 | Le fonctionnement de la blockchain | 32 |
| 1.3 | Le consensus PoW | 33 |
| 2.1 | Processus de création de la confiance sociale | 43 |
| 2.2 | Processus de construction d'un système de confiance | 56 |
| 4.1 | Les approches de recommandation | 80 |
| 4.2 | Le Processus de Décision Markovien | 82 |
| 4.3 | Les systèmes de recommandation basés sur le PDM | 86 |
| 4.4 | Dendrogramme conceptuel pour le clustering hiérarchique agglomératif et divisif | 87 |
| 5.1 | Notation graphique de la confiance | 101 |
| 5.2 | Notation textuelle de la confiance | 101 |
| 5.3 | Notation graphique du contexte | 101 |
| 5.4 | Notation textuelle du contexte | 101 |
| 5.5 | Notation graphique de la transitivité | 102 |
| 5.6 | Notation textuelle de la transitivité | 102 |
| 5.7 | Notation graphique d'un groupe | 103 |
| 5.8 | Notation graphique de la distributivité | 103 |
| 5.9 | Notation textuelle de la distributivité | 103 |
| 5.10 | Notation graphique de la réputation | 104 |
| 5.11 | Notation textuelle de la réputation | 104 |
| 5.12 | Bon utilisateur vs. Mauvais utilisateur | 117 |

| | |
|--|-----|
| 5.13 Un nouvel utilisateur vs. un utilisateur avec comportement mi-positif mi-négatif | 118 |
| 5.14 Le système se souvient des fraudes | 118 |
| 5.15 Récidivisme | 119 |
| 5.16 Droit à l'erreur | 120 |
| 5.17 Vol d'identité | 120 |
| 6.1 La méthodologie de notre approche | 129 |
| 6.2 Modélisation des actions de l'utilisateur | 129 |
| 6.3 Modélisation des exigences de l'application | 130 |
| 6.4 Un exemple qui montre notre proposition graphique via le principe des modèles de tâches. | 134 |
| 6.5 Exemple de décomposition de tâches | 135 |
| 6.6 Modélisation des exigences de confiance | 137 |
| 6.7 Compatibilité des modèles computationnels pour le critère WTCB | 143 |
| 6.8 Compatibilité des modèles computationnels pour le critère Efficace | 143 |
| 6.9 Compatibilité des modèles computationnels pour le critère Flexible | 144 |
| 6.10 Pourcentage de compatibilité des modèles computationnels pour chaque critère | 145 |

Liste des tableaux

| | | |
|-----|---|-----|
| 1.1 | Principaux caractéristiques des réseaux sociaux et des réseaux anonymes | 34 |
| 4.1 | Synthèse de l'état de l'art | 84 |
| 4.2 | Les statistiques des données physico-chimiques du vin blanc | 92 |
| 4.3 | Les statistiques des données physico-chimiques du vin rouge | 92 |
| 4.4 | Prédiction de la valeur de la qualité du vin | 93 |
| 4.5 | Taux d'erreur des valeurs de prédiction | 94 |
| 5.1 | Comparaison des différents modèles | 109 |
| 5.2 | Synthèse de notre analyse | 115 |
| 5.3 | Incertitude dans le modèle basé sur les croyances | 121 |
| 5.4 | Résumé des comportements des modèles computationnels | 121 |
| 6.1 | Association des valeurs continues aux évaluations. | 131 |
| 6.2 | Discrétisation des degrés d'évaluation. | 141 |
| 6.3 | Exemple de comportement de l'utilisateur et de ses évaluations dans le système. | 141 |
| 6.4 | Contraintes appliquées au score de confiance souhaité pour le critère WTCB.142 | |
| 6.5 | Contraintes appliquées au score de confiance souhaité pour le critère Efficace.142 | |
| 6.6 | Contraintes appliquées au score de confiance souhaité pour le critère Flexible.143 | |

Introduction générale

Ce travail de thèse a été réalisé dans le cadre d'une convention CIFRE au sein de l'équipe Data Engineering du laboratoire LIAS (Laboratoire d'Informatique et d'Automatique pour les Systèmes) en collaboration avec l'entreprise O°Code. Le LIAS, créé en janvier 2012, est le résultat de la fusion de deux laboratoires : le Laboratoire d'Informatique Appliquée (LISI, EA 1232) et le Laboratoire d'Automatique et d'Informatique Appliquée (LAI, EA 1219).

Créé en 2016 par Dominique Chabot, l'entreprise O°Code a pour mission de faire du monde numérique un endroit plus sûr, et lui donner une valeur tangible dans le monde physique, pour garantir la confiance dans tous les échanges. Les solutions de O°Code reposent notamment sur un système de marquage digital et physique unitaire inviolable et inaltérable, sous la forme d'un nuage de points, une traçabilité indépendante et collaborative, et un accès selon des droits aux informations et documents associés. Le tout est enregistré à vie dans un registre digital distribué sous blockchain pour garantir la confidentialité et la protection de l'ensemble des données.

Contexte

De nos jours, on ne peut plus imaginer comment rejoindre ses amis et ses contacts sans les réseaux sociaux. *Les réseaux sociaux* [DF04] nous ont permis de nous rapprocher de nos amis, même s'ils se trouvent à des milliers de kilomètres. Grâce à eux, nous pouvons nous connecter avec des personnes du monde entier.

Aujourd'hui, les réseaux sociaux font partie intégrante de nos vies. D'un point de vue personnel comme professionnel, on les utilise à des fins interactives, éducatives, informatives ou de divertissement. Ils se présentent sous de nombreuses formes, mais toutes sont liées : blogs, forums, podcasts, partage de photos, bookmarking social, widgets, vidéo, etc.

Au cours de l'histoire, les gens ont inventé divers moyens de communication : la poste, le télégraphe, les signaux lumineux et le téléphone. Il y a quelques années, pour obtenir des réponses, il fallait attendre des jours, voire des mois. Heureusement, l'homme n'a jamais cessé d'évoluer, il a inventé internet et son vaste réseau d'ordinateurs qui commuiquent ensemble (le World Wide Web), puis un jour de 1971, la messagerie électronique, la première forme du réseau social [CC15].

Le World Wide Web est le principal outil utilisé par des milliards de personnes pour partager, lire et écrire des informations et interagir avec d'autres personnes via Internet. Le World Wide Web a fait beaucoup de progrès depuis son avènement. La première version du Web 1.0, également appelée Web syntaxique ou Web en lecture seule, correspond à l'époque (1990-2000) où le rôle de l'utilisateur se limite à lire les informations fournies par les producteurs de contenu. L'utilisateur ou le consommateur n'a pas la possibilité de renvoyer l'information aux producteurs de contenu. Les exemples de Web 1.0 sont les sites Web statiques et les sites personnels. Le Web 2.0, également appelé Web social, est une ère (2000-2010) qui se poursuit encore aujourd'hui et qui facilite l'interaction entre les utilisateurs du Web et les sites qui permettent aux utilisateurs de communiquer avec d'autres utilisateurs. Dans cette ère, chaque utilisateur peut être un producteur de contenu et le contenu est distribué et partagé entre les sites. Certaines des applications Web 2.0 les plus connues sont Facebook¹, Youtube², Flickr³, Twitter⁴, etc. Le Web 3.0 est toujours en cours d'évolution et de définition. Ce qui est clair, cependant, c'est que le Web 3.0 mettra l'accent sur les applications décentralisées et fera un usage intensif des technologies basées sur la blockchain. Le Web 3.0 fera également appel à l'apprentissage automatique et à l'Intelligence Artificielle (IA) pour rendre les applications plus intelligentes et adaptatives.

Pour s'adapter à cette évolution du Web, les techniques de recherche d'informations ont dû intégrer des aspects sociaux et axés sur l'utilisateur et son comportement. Parmi ces techniques, on parle dans ce travail *des systèmes de recommandation*. Au cours des dernières décennies, avec l'essor de Youtube, Amazon⁵, Netflix⁶ et de nombreux autres services web de ce type, les systèmes de recommandation [KCS14] ont pris de plus en plus de place dans nos vies. Du commerce électronique (suggérer aux acheteurs des ar-

1. <https://www.facebook.com/>
2. <https://www.youtube.com/>
3. <https://www.flickr.com/>
4. <https://twitter.com/>
5. <https://www.amazon.fr/>
6. <https://www.netflix.com/>

ticles susceptibles de les intéresser) à la publicité en ligne (suggérer aux utilisateurs les bons contenus, correspondant à leurs préférences), les systèmes de recommandation sont aujourd'hui incontournables dans nos parcours quotidiens en ligne. D'une manière très générale, les systèmes de recommandation visent à prédire les centres d'intérêt des utilisateurs et à leur recommander des produits qui sont très probablement intéressants pour eux. Ils font partie des systèmes d'apprentissage automatique les plus puissants que les commerçants en ligne mettent en œuvre pour stimuler les ventes. Les données requises pour les systèmes de recommandation proviennent des évaluations explicites des utilisateurs après avoir, par exemple, regardé un film ou écouté une chanson, des requêtes implicites des moteurs de recherche et des historiques d'achat, ou d'autres connaissances sur les utilisateurs/articles eux-mêmes.

Toutefois, comme pour presque toutes les technologies, les avantages de ces systèmes s'accompagnent de facteurs de risque importants et d'un potentiel d'abus. Ces dernières années, les réseaux sociaux et les systèmes de recommandation ont fait preuve d'une capacité sans précédent à observer et à manipuler le monde physique. On peut citer par exemple le fait que les "influenceurs" jouent un rôle très important sur les réseaux. En effet, comme leur nom l'indique, ils ont une grande capacité d'influence sur les internautes, notamment les plus jeunes. Un autre exemple est celui des "fake news" qui ont un pouvoir important sur le comportement des utilisateurs. C'est une arme très utilisée par les politiciens pour contredire ou déstabiliser leurs concurrents. En effet, le partage massif d'une fausse nouvelle sur un politicien peut totalement changer le comportement d'un électeur indécis et lui faire réorienter son choix, même s'il s'avère plus tard qu'elle est fausse. On peut donc se demander comment un utilisateur peut faire confiance aux informations fournies par ces systèmes ?

Comme mentionné ci-dessus, le web social est un ensemble de relations sociales qui relie les gens par le biais du World Wide Web. Le web social englobe la manière dont les sites web et les logiciels sont conçus et développés afin de soutenir et de favoriser l'interaction sociale. *La confiance* est l'un des éléments clés qui permettent aux utilisateurs de ces systèmes d'interagir en toute sécurité. Ce concept a fait l'objet de plusieurs travaux de recherche (et continue jusqu'à aujourd'hui) afin de produire des systèmes de recommandation à base de confiance [Hay14]. Ces systèmes utilisent les relations de confiance entre les utilisateurs pour calculer et prédire les évaluations en fonction des expériences

et des commentaires.

Faire confiance à quelqu'un que vous ne connaissez pas ou qui n'appartient pas à votre entourage n'est pas une décision facile. C'est un problème courant dans la vie réelle et qui devient un critère majeur pour l'utilisation des systèmes informatiques. Dans la vie réelle, pour faire confiance à une personne, la première idée qui vient à l'esprit est de demander l'avis des personnes qui la connaissent. C'est presque le même principe pour la confiance virtuelle dans les systèmes informatiques. La différence est que dans ces derniers, ce concept doit être calculable. Ainsi, une variété de *modèles computationnels* ont été développés pour aider les utilisateurs à prendre des décisions, et pour améliorer les interactions entre les différents utilisateurs d'un système.

Bien que l'exploitation de ces relations d'interaction est souvent efficace pour améliorer les résultats fournis par les systèmes de recommandation à base de confiance, on peut néanmoins noter quelques problèmes.

Problématiques et Objectifs

(1) Nature statique des systèmes de recommandation : les systèmes de recommandation (SR) regroupent tous les systèmes capables de fournir des recommandations adaptées aux goûts et aux besoins des utilisateurs. Ils visent à aider l'utilisateur à accéder à des articles utiles ou intéressants au sein d'un vaste espace de données qui dépasse ses capacités cognitives. En effet, l'utilisateur n'a pas besoin de formuler une demande, la seule demande est implicite et peut se traduire par : quels sont les articles qui correspondent à mes goûts, mes besoins ou mes moyens ?

Aujourd'hui, les systèmes de recommandation se trouvent un peu partout, sur les plateformes de distribution de contenus multimédia (Netflix, YouTube, Spotify...), sur les plateformes de vente en ligne (Zalando, Amazon...), sur les réseaux sociaux. (Facebook, Twitter...), etc. Par conséquent, le terme « article » est un terme général pour nommer la ressource recommandée aux utilisateurs par ces systèmes, par exemple les films, les vidéos, la musique, les vêtements, les livres, les utilisateurs, etc. Les systèmes de recommandation prennent tout leur sens lorsque le nombre d'utilisateurs et d'articles devient très important, car il est peu probable que les utilisateurs connaissent toute la richesse du catalogue proposé par le service.

Le premier objectif de ce travail consiste à remédier à la nature statique des systèmes de recommandation afin de leurs donner un aspect dynamique capable de s'adapter aux changements des comportements des utilisateurs.

(2) Formalisation et modélisation de la confiance : le concept de confiance est d'une importance capitale dans les sociétés humaines. Plusieurs disciplines ont recours à son utilisation de différentes manières selon leurs propres visions et perspectives. Au cours des dernières décennies, un nombre impressionnant de recherches a été mené sur les sujets liés à la confiance informatique et aux modèles de réputation. De nombreuses approches de la confiance sur des applications très connues sont encore aujourd'hui répandues. Par exemple, les cadres de réputation sur des sites web comme eBay, Amazon, ou les sites de notation de personnes comme Tripadvisor et Goodreads. Pour répondre aux défis posés par ce domaine, les recherches continuent pour développer des modèles théoriques et pratiques afin de mieux comprendre le domaine et d'améliorer les solutions existantes. Cependant, nous remarquons qu'il existe plusieurs définitions relatives à la confiance, ce qui entraîne une ambiguïté dans la compréhension de ce concept.

Le deuxième objectif de ce travail consiste à unifier les définitions liées à la confiance et à proposer un cadre de formalisation et de modélisation de ce concept.

(3) Variation des modèles computationnels : dans la littérature, il existe principalement deux types de systèmes de confiance : les systèmes de confiance basés sur les politiques et les systèmes de confiance basés sur la réputation. Le premier est basé sur le principe des compétences et des autorisations requises pour effectuer une action tandis que le second, que nous considérerons dans ce travail de thèse, fait usage de la réputation d'une entité pour accorder ou non la confiance à cette entité.

Les systèmes de confiance basés sur la réputation utilisent les interactions, ou les expériences directes, entre les entités et/ou les expériences des autres pour le choix de faire confiance ou non. Aujourd'hui, plusieurs applications modernes sont basées sur ces systèmes pour garantir la sécurité de leurs algorithmes. Afin de garantir et de calculer la confiance, plusieurs modèles computationnels ont vu le jour. Ainsi, le problème majeur est de choisir le modèle de calcul le plus approprié en fonction des besoins de l'utilisateur

et de son comportement.

Le troisième objectif de ce travail est de proposer une approche d'aide au choix du modèle computationnel le plus adéquat/approprié afin de répondre aux besoins en confiance du système cible.

Démarche et Contributions

Comme mentionné ci-dessus, les systèmes de recommandation posent encore plusieurs problèmes tels que : la difficulté de gérer les profils atypiques, la difficulté de traiter les changements de profils des utilisateurs, le manque de diversité des recommandations, le manque d'explication des recommandations, etc. Pour résoudre certains de ces problèmes, de nouvelles approches basées sur des techniques de l'IA ont émergé. L'une des idées à l'origine de ces tendances est de considérer le problème de la recommandation comme un problème de processus de décision de Markov (MDP) et d'essayer de tirer parti de l'apprentissage par renforcement pour le résoudre. Cependant, les systèmes de recommandation par renforcement existant présentent deux problèmes majeurs.

- Ils doivent parcourir un grand nombre d'états à des fins de prise de décision. Ce qui augmente la complexité algorithmique.
- Il est difficile d'expliquer leurs résultats.

Notre première contribution consiste à proposer une méthode hybride pour résoudre ces deux problèmes. Nous utilisons une technique de clustering hiérarchique qui permet de réduire l'espace des états et des actions et ainsi réduire la complexité algorithmique. L'utilisation du clustering hiérarchique permet non seulement de réduire l'espace, mais aussi d'améliorer la qualité des recommandations.

Par ailleurs, nous avons également constaté que les systèmes de recommandation exploitent les interactions entre les utilisateurs et avec le système et les produits qu'ils suggèrent. Quand on parle des relations d'interactions, on ne peut pas ignorer la notion de confiance qui joue un rôle crucial dans ces systèmes. Pour mesurer ce concept, une variété de modèles computationnels ont été développés pour aider les utilisateurs à

prendre des décisions, et pour améliorer les interactions avec le système et entre les utilisateurs. En raison d'une grande variété de définitions pour le concept de la confiance, notre deuxième contribution tente d'unifier ces définitions en proposant une formalisation unique en termes de notations graphiques et textuelles. Nous introduisons également une analyse approfondie pour comprendre le comportement et l'intuition derrière chaque modèle computationnel.

Comme mentionné précédemment, de nombreux modèles computationnels ont été développés pour aider les utilisateurs à prendre des décisions et améliorer les interactions entre les différents utilisateurs au sein d'un système. Il est donc difficile de choisir le modèle le plus approprié dans un contexte donné. Pour pallier ce problème, nous proposons dans la troisième partie de notre contribution, une approche en deux étapes qui, d'abord, permet à l'utilisateur de définir les exigences de son système cible et, ensuite, un guide pour sélectionner le modèle computationnel le plus approprié pour son application en fonction des exigences définies.

Structure de la thèse

Ce manuscrit est divisé en six chapitres, répondant à trois problématiques de recherche que nous avons identifiées concernant les liens possibles entre les techniques d'apprentissage, les systèmes de recommandation et les systèmes à base de confiance. La structure du manuscrit est schématisée dans la Figure 1.

Le chapitre 1 présente d'abord une revue de la littérature sur les réseaux sociaux, leur définition et leur genèse, ainsi que les concepts de base qui leur sont liés. Il s'intéresse ensuite aux réseaux sociaux anonymes, en discutant le concept d'anonymat et l'impact de l'utilisation de données privées sur la vie des utilisateurs de ces réseaux.

Après avoir abordé les problèmes liés à l'utilisation de données privées mais aussi à l'anonymat, le chapitre 2 introduit le concept de la confiance, sa modélisation dans la littérature et les types de modèles existants pour la calculer.

Les systèmes de recommandation font partie des systèmes qui permettent à leurs utilisateurs de s'entraider tout en garantissant la confiance et la fiabilité dans l'échange d'informations. Le chapitre 3 introduit un aperçu sur ces systèmes et souligne l'apport de

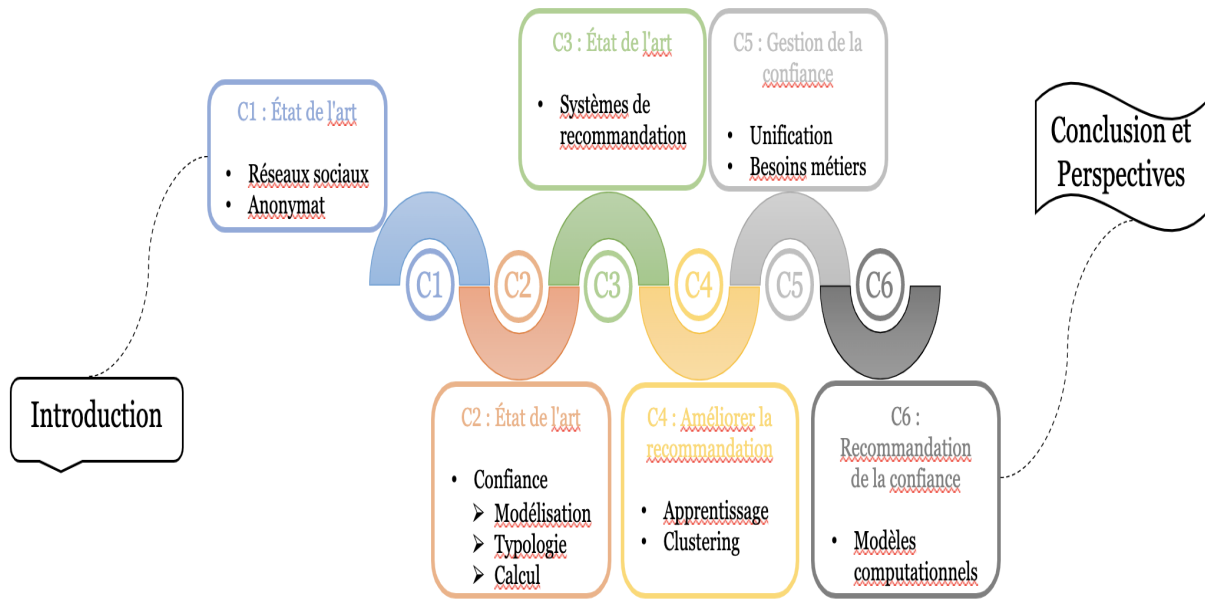


FIGURE 1 – Plan du manuscrit

l'IA dans ce domaine.

Afin de répondre aux besoins de l'entreprise O°Code en matière de recommandation, le chapitre 4 définit les différents problèmes liés aux systèmes de recommandation, la raison pour laquelle les systèmes existants ne répondent pas à ces besoins. Puis, il propose une approche hybride utilisant l'IA et les techniques de clustering pour résoudre ces problèmes.

Afin d'échanger des informations de manière sécurisée, un modèle de confiance doit être établi. Plusieurs travaux antérieurs ont défini ce concept, ce qui a conduit à une ambiguïté face à cette diversité de définitions. Le chapitre 5 propose un cadre pour unifier les définitions de la confiance et les notions connexes. Par la suite, une étude approfondie des modèles existants qui mesurent la valeur de la confiance a été proposée afin de comprendre l'intuition derrière chaque modèle. Différents critères de comparaison entre ces modèles informatiques ont également été discutés.

Le chapitre 6 aborde le problème de l'évaluation des modèles de calcul de la confiance et du choix du modèle le plus approprié en fonction des exigences de l'application et du comportement des utilisateurs.

Finalement, nous tirons les principales conclusions de la thèse dans le dernier chapitre et proposons de nouvelles perspectives de recherche.

Publications

La liste suivante présente les publications concernant le travail de cette thèse.

1. Sellami, C., Baron, M., Jean, S., Bechchi, M., Hadjali, A., & Chabot, D. (2022, May). Trust Model Recommendation Driven by Application Requirements. In International Conference on Research Challenges in Information Science (pp. 694-702). Springer, Cham.
2. Sellami, C., Baron, M., Bechchi, M., Hadjali, A., Jean, S., & Chabot, D. (2021, May). Towards a unified framework for computational trust and reputation models for e-commerce applications. In International Conference on Research Challenges in Information Science (pp. 616-622). Springer, Cham.
3. Sellami, C., Baron, M., Jean, S., Bechchi, M., Hadjali, A., & Chabot, D. (2020, September). A Hybrid Learning-Based Model for Wine Recommendation. The ACM Recommender Systems conference (RecSys 2020).



Première partie

État de l'art

Introduction

De nos jours, nous pouvons nous connecter avec des personnes du monde entier grâce au World Wide Web. Ce qui nous permet de rester facilement en contact avec nos proches et nos amis. L'avènement du web social a conduit à l'émergence *des réseaux sociaux*. Les réseaux sociaux sont en train de changer la façon dont le monde change et évolue socialement, la façon dont les gens obtiennent des informations à la façon dont ils communiquent et, surtout, à la façon dont ils interagissent. L'importance et la pertinence des réseaux sociaux se renforcent de plus en plus avec l'évolution rapide de la technologie. Les réseaux sociaux sont omniprésents dans la vie de tous les jours et prennent de nombreuses formes différentes, notamment des sites de réseaux sociaux, des sites de commerce électronique et des blogs en ligne. Le réseau social a été proposé pour la première fois par Barnes [Bar69] en 1969, qui l'a décrit comme un graphe de connexion dans lequel les « nœuds » représentent les entités du réseau et les « arêtes » les dépendances entre elles. Un nœud peut être un individu, un groupe, une organisation, etc, tandis qu'une arête peut représenter des interactions, des invitations, des transactions, des valeurs connexes, etc [Gon+20]. Il existe des relations interpersonnelles complexes dans les réseaux sociaux. Chaque réseau peut contenir des millions, voire des dizaines de millions d'utilisateurs, qui sont connectés les uns aux autres pour former un immense réseau. Alors que les réseaux sociaux sont en plein essor, le nombre d'utilisateurs ne cesse d'augmenter, les couvertures s'étendent, et différents problèmes associés apparaissent. L'augmentation du nombre d'utilisateurs des réseaux sociaux, la surcharge d'informations, l'augmentation des spams indésirables, les informations irréalistes des utilisateurs, les relations peu fiables entre les utilisateurs, le manque de confiance entre les utilisateurs et la détérioration de la qualité des connexions sociales sont des problèmes de plus en plus constatés [Gon+20]. La méfiance entre les utilisateurs est ainsi une source majeure de nombreux problèmes auxquels sont confrontés les réseaux sociaux.

Dans cette partie, le premier chapitre fait une revue de la littérature sur les réseaux sociaux, les problèmes qui se sont apparus et surtout ceux liés à l'atteinte de la vie privée des utilisateurs. Dans ce chapitre, on parle également des réseaux anonymes, une première réponse aux problèmes causés par les réseaux classiques. Le deuxième chapitre introduit le concept de la confiance, comment elle est représentée et calculée et comment elle est utilisée dans les systèmes de recommandation pour faciliter l'interaction entre les différents

utilisateurs. Le troisième chapitre passe en revue les systèmes de recommandation à la fois traditionnels et émergents basés sur des techniques d'IA.

Chapitre 1

Réseaux sociaux et Anonymat

Sommaire

| | |
|--|-----------|
| 1.1 Introduction | 19 |
| 1.1.1 Définition et Historique des réseaux sociaux | 19 |
| 1.1.2 Notions de base sur les réseaux sociaux | 25 |
| 1.2 Anonymat | 28 |
| 1.2.1 Définition de l'anonymat | 28 |
| 1.2.2 Exemples des systèmes anonymes | 29 |
| 1.3 Discussion | 33 |



1.1 Introduction

Six-Degrees est largement considéré comme le tout premier site de réseau social [BE07]. Fondé par Andrew Weinreich en mai 1996, le site a été lancé l'année suivante et combinait en un seul service des fonctionnalités populaires telles que les profils, les listes d'amis et les affiliations scolaires. Si le site comptait des millions d'utilisateurs inscrits, le réseau était limité en raison du manque de personnes connectées à Internet. Il faudra attendre quelques années pour qu'Internet devienne accessible au grand public pour propulser et rendre populaire de nombreux réseaux sociaux en ligne tels que Facebook¹, LinkedIn² ou Google+. Des plateformes populaires, où les gens du monde entier se retrouvent pour échanger [HKP12]. L'utilisation des réseaux sociaux a atteint une ampleur considérable : En mai 2021, le nombre d'utilisateurs actifs des réseaux sociaux s'élève à 4,33 milliards, soit 55,1% de la population mondiale. D'une année à l'autre, on compte plus de 521 millions de nouveaux utilisateurs dans le monde, soit 13,7% de plus qu'en avril 2020. Au cours du premier trimestre 2021, on comptabilise environ 130 millions de nouveaux socionautes [Onl22].

1.1.1 Définition et Historique des réseaux sociaux

Les sites des réseaux sociaux sont des services en ligne qui permettent aux individus de (1) construire un profil public ou semi-public au sein d'un système, (2) d'articuler une liste d'autres utilisateurs avec lesquels ils partagent une connexion, et (3) de visualiser et de parcourir leur liste de connexions et celles établies par d'autres personnes au sein du système [BE07]. La nature et la nomenclature de ces connexions peuvent varier d'un site à l'autre. Bien que nous utilisions le terme « site de réseau social » pour décrire ce phénomène, le terme « sites de réseautage social » apparaît également dans le discours public, et les deux termes sont souvent utilisés de manière interchangeable. Nous avons choisi de ne pas employer le terme « réseautage » pour deux raisons : l'accentuation et la portée. Le terme « réseautage » met l'accent sur l'établissement de relations, souvent entre étrangers. Bien que le réseautage soit possible sur ces sites, ce n'est pas la pratique principale sur beaucoup d'entre eux [BE07]. Ce qui rend les sites de réseaux sociaux uniques ce n'est pas le fait qu'ils permettent aux individus de rencontrer des inconnus, mais

1. <https://www.facebook.com/>

2. <https://www.linkedin.com/>

plutôt qu'ils permettent aux utilisateurs d'articuler et de rendre visibles leurs réseaux. Les utilisateurs de plusieurs sites des réseaux sociaux ne sont pas nécessairement en train de « réseauter » ou de chercher à rencontrer de nouvelles personnes ; ils communiquent plutôt avec des personnes qui font déjà partie de leur réseau social étendu.

L'évolution des réseaux sociaux a été alimentée par l'impulsion humaine de communiquer et par les progrès de la technologie numérique. Il s'agit d'établir et d'entretenir des liens personnels à grande échelle. Le rapport 2019 du Pew Research Center³ sur l'utilisation des réseaux sociaux aux États-Unis a montré que 72% des adultes américains utilisent une forme de réseaux sociaux. En 2005, l'année qui a suivi la création de Facebook, ce chiffre était de 5%. Ce qui suit est un examen des origines des réseaux sociaux, de leur croissance relativement rapide en tant que force sociologique et commerciale, et du changement qu'ils ont apporté au monde du marketing et de la société.

En moins d'une génération, les réseaux sociaux sont passés du stade de l'échange électronique direct d'informations à celui de lieu de rassemblement virtuel, de plateforme de vente au détail et d'outil de marketing essentiel du 21^{ème} siècle. C'est également une nouvelle manière dont les groupes politiques et les politiciens mènent les campagnes électorales, restent en contact avec leurs électeurs et forment des alliances avec d'autres groupes ou individus. Les sites des réseaux sociaux comme Facebook, Twitter, YouTube, etc. peuvent également permettre à de petits groupes aux ressources limitées de renverser des régimes gouvernementaux, stimuler des campagnes politiques et contribuer à des victoires présidentielles, susciter des protestations publiques, organiser des manifestations sociales, mobiliser des campagnes sociales, permettre des communications et des discussions sur des forums publics, sensibiliser l'opinion publique, etc.

Le télégraphe, premier réseau de communication à distance peut être considéré comme l'ancêtre directe de nos réseaux actuels. Le 24 mai 1844, Samuel Finley Breese Morse fait la démonstration de son télégraphe électromagnétique [MK82] dans le bâtiment du capitol à Washington, DC, en transmettant un message envoyé à une gare de Baltimore, Maryland, à environ trente-huit miles de là. Le message transmis par la ligne télégraphique était « What has God wrought ? », un passage biblique. Cette démonstration a convaincu de nombreux membres du gouvernement et de l'industrie de la viabilité et de l'utilité de cette nouvelle technologie.

3. <https://www.pewresearch.org/>

Si les racines de la communication numérique sont profondes, la plupart des récits contemporains sur les origines modernes de l'internet et des réseaux sociaux d'aujourd'hui font référence à l'émergence, en 1969, du réseau ARPANET [PS19] (Advanced Research Projects Agency Network). Ce premier réseau numérique, créé par le ministère de la Défense des États-Unis, permettait aux scientifiques de quatre universités interconnectées de partager des logiciels, du matériel et d'autres données. En 1987, le précurseur direct de l'internet d'aujourd'hui a vu le jour lorsque la Fondation nationale pour la science a lancé un réseau numérique national plus robuste, connu sous le nom de NSFNET [NSF22]. Dix ans plus tard, en 1997, la première véritable plate-forme de médias sociaux était lancée. Dans les années 1980 et 1990, selon [Sha22] du site d'information technologique Digital Trends, la croissance d'Internet a permis l'introduction de services de communication en ligne tels que CompuServe, America Online et Prodigy. Ces services ont initié les utilisateurs à la communication numérique par le biais du courrier électronique, de la messagerie sur tableau d'affichage et du chat en ligne en temps réel. C'est ainsi que sont nés les premiers réseaux de médias sociaux, à commencer par le service éphémère de téléchargement de profils de Six Degrees, en 1997. Ce service a été suivi en 2001 par Friendster [Boy04]. Friendster a utilisé un concept de degré de séparation similaire à celui de SixDegrees, aujourd'hui disparu, l'a affiné en une routine baptisée « cercle d'amis et a promu l'idée qu'une riche communauté en ligne ne peut exister qu'entre des personnes qui ont vraiment des liens communs. Ainsi, il a veillé à ce qu'il y ait de nombreuses façons de découvrir ces liens. Un an après son lancement, Friendster comptait plus de trois millions d'utilisateurs enregistrés et suscitait un vif intérêt de la part des investisseurs. Depuis, le service a connu un nombre non négligeable de difficultés techniques, de décisions de gestion discutables et une chute conséquente de sa fortune en Amérique du Nord. Bien qu'il ait brièvement connu le succès en Indonésie et aux Philippines, Friendster a depuis abandonné le réseau social et existe désormais uniquement en tant que site de jeux en ligne. Lancé un an plus tard, en 2003, LinkedIn⁴ [Alb+11] a adopté une approche résolument plus sérieuse et plus sobre du phénomène des réseaux sociaux. Plutôt que d'être un simple terrain de jeu pour les anciens camarades de classe et les adolescents, LinkedIn était, et est toujours, une ressource de réseautage pour les gens d'affaires qui veulent entrer en contact avec d'autres professionnels. En février 2022, LinkedIn compte 830 millions de membres dans

4. <https://www.linkedin.com/>

le monde répartis dans 200 pays [Lin22].

MySpace⁵ [Jon+08] a également été lancé en 2003. Bien qu'il ne soit plus sur le trône des réseaux sociaux dans de nombreux pays anglophones - cet honneur revient désormais à Facebook un peu partout - MySpace était autrefois l'éternel favori. Il y est parvenu en séduisant les jeunes adultes avec de la musique, des vidéos musicales et un environnement funky et riche en fonctionnalités. Dès le départ, il était plus branché que son principal concurrent Friendster, et il a mené une sorte de campagne dans les premiers jours pour montrer aux utilisateurs de Friendster ce qu'ils manquaient. Au fil des ans cependant, le nombre d'utilisateurs occasionnels de Myspace a diminué, et aujourd'hui, le site n'existe plus que sous la forme d'un site de réseau social destiné aux groupes et aux musiciens [Sha22].

Comme prévu, l'omniprésent Facebook [Brü15] est aujourd'hui en tête du peloton mondial des réseaux sociaux. Fondé, par des étudiants de l'université Harvard. Facebook a été lancé en 2004 en tant qu'exercice réservé à l'université Harvard et est resté un site axé sur le campus pendant deux années complètes avant d'être finalement ouvert au grand public en 2006. Pourtant, même à cette époque, Facebook était considéré comme une grosse entreprise. À tel point qu'en 2009, de grandes personnalités de la Silicon Valley, tels que le cofondateur de Paypal et le milliardaire Peter Thiel, ont investi des dizaines de millions de dollars juste pour le voir prospérer. Le secret du succès de Facebook - 2,912 milliards d'utilisateurs actifs mensuels en février 2022 [Ass22] - fait l'objet de nombreux débats. Certains mettent en avant sa facilité d'utilisation, d'autres sa multitude de fonctionnalités facilement accessibles, et d'autres encore, son nom mémorable.

La tentative de Google de s'imposer dans le paysage des réseaux sociaux, Google+ [Mag+12], a été lancée en 2012. Une existence mouvementée qui a pris fin en 2018, après que les informations privées de près de 500 000 utilisateurs de Google+ ont été compromises par une violation de la sécurité des données [Mar22].

Les réseaux sociaux sont en train de changer la façon dont le monde évolue et se développe socialement, la façon dont les gens obtiennent des informations à la façon dont ils communiquent et, surtout, à la façon dont ils interagissent. L'importance et la pertinence des réseaux sociaux ne cessent de croître avec l'évolution rapide de la technologie.

Comme le montre la Figure 1.1, la chronologie des réseaux sociaux est concentrée

5. <https://myspace.com/>

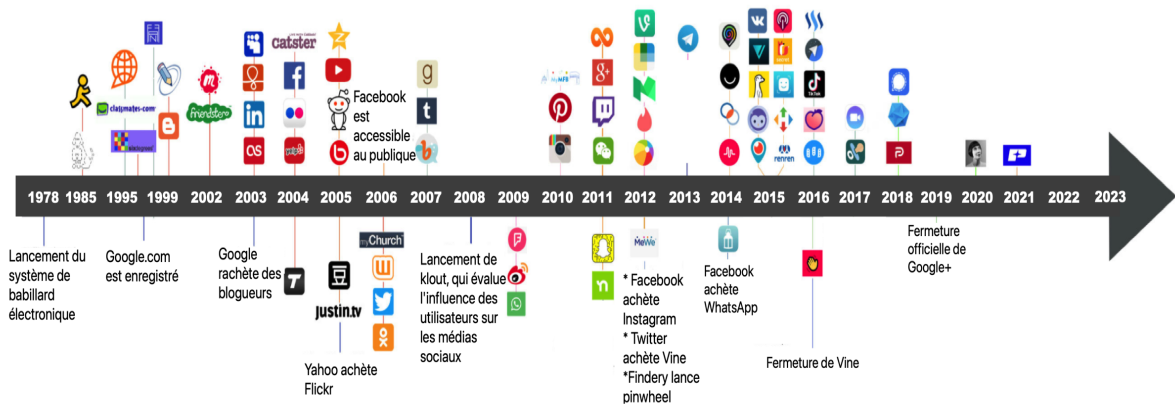


FIGURE 1.1 – Chronologie des réseaux sociaux

sur 44 ans de changement. L'évènement le plus important avec lequel cette chronologie commence est le développement et l'enregistrement de Google dont l'idée était d'extraire du sens de la masse de données qui s'accumulait sur Internet. Par la suite, Google a décidé d'acheter des bloggers. Cette initiative aiderait tout simplement Google à créer un moteur de recherche plus précis en ajoutant de nouvelles sources riches de données extraites des blogs. Le secret réside dans les dizaines de liens que les webbloggers créent chaque jour vers du contenu sur le Web. Dans la même année, en 2002, LinkedIn a été créé, dans le salon de Reid Hoffman, cofondateur de LinkedIn. Selon lui, ils ont construit LinkedIn en disant : *We're here to build a business, not to create something cool*. Après l'expérience de LinkedIn, vient l'idée de Facebook. Le 4 février 2004, Mark Zuckerberg, étudiant en deuxième année à Harvard, lance Facebook, un site web de médias sociaux qu'il a construit pour mettre en relation les étudiants de Harvard. Mark Zuckerberg a imaginé un moyen de transposer sur Internet l'expérience sociale existante à l'université. Il voulait créer un endroit qui pourrait aider les étudiants à se connecter les uns aux autres.

Plutard en 2005, YouTube a été créé comme une plateforme permettant à quiconque de publier tout contenu vidéo qu'il souhaitait. On espérait que les utilisateurs pourraient utiliser le site pour télécharger, partager et visionner du contenu sans restriction. Depuis, le site s'est développé pour devenir l'un des principaux sites de distribution de vidéos au monde. L'avantage de Youtube par rapport à Facebook est qu'il permet de créer des contenus, modifier, monter et télécharger des vidéos, et gagner de l'argent grâce aux vidéos partagées et vues.

Au début de l'année 2006, Jack Dorsey, étudiant à l'université de New York, a partagé

une nouvelle idée de communication en ligne avec certains de ses collègues d'Odeo, une société de podcasting. L'idée de Dorsey était une plateforme qui permettait aux utilisateurs de partager de courts messages avec des groupes de personnes, comme pour l'envoi de SMS, c'était « Twitter ». L'un des principaux avantages de Twitter par rapport à Facebook est la disponibilité de nombreux outils d'analyse des performances des marques. Il existe de nombreux outils que les marques peuvent utiliser sans investir trop d'argent. Un grand nombre d'options sont disponibles gratuitement, tandis que les plus premium sont payants.

En 2009, Whatsapp a été créé, c'est l'application de messagerie la plus populaire dans le monde. En termes de données, Whatsapp est beaucoup plus sûr que les autres réseaux sociaux. S'il est toujours déconseillé de partager des informations personnelles sur Facebook, compte tenu des problèmes de confidentialité et des craintes de piratage, ce problème ne se pose pas sur Whatsapp grâce à la technologie de chiffrement de bout en bout [MS16]. En février 2014, Facebook annonce avoir racheté WhatsApp. Cependant, un nouveau rapport de ProPublica⁶ affirme que les messages WhatsApp ne sont pas chiffrés de bout en bout, ajoutant que Facebook inspecte le contenu des messages sur la plateforme. Même si WhatsApp dispose d'un chiffrement de bout en bout depuis 2016, il existe certaines circonstances dans lesquelles les sous-traitants utilisant le logiciel spécial de Facebook peuvent lire les messages envoyés d'un utilisateur à un autre. Par exemple, lorsque quelqu'un signale un message, même dans une discussion privée, l'algorithme d'IA recherche les activités suspectes liées au terrorisme, à la maltraitance des enfants, etc. Il transmet ensuite le message signalé, ainsi que quatre messages précédents, à un véritable humain pour examen.

Par la suite, plusieurs autres réseaux sociaux ont vu le jour comme Instagram, TikTok, Snapchat, etc. Ces réseaux ont eu un impact dans plusieurs domaines. Autrefois, la publicité se faisait principalement sur les panneaux d'affichage ou à la télévision, aujourd'hui la plus efficace est sur les réseaux sociaux, principalement par le biais des influenceurs. Pour être présent sur le marché en ligne et être visible, il est essentiel de suivre l'évolution de ce monde numérique rapide et facilement modifiable. Les réseaux sociaux présentent plusieurs avantages pour une entreprise, surtout aujourd'hui : ils permettent de faire connaître une marque, de créer une communauté, d'avoir des adeptes et d'analyser les

6. <https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users?ref=hackernoon.com>

informations et les données. Les données sont la base de tout : on peut comprendre si les gens aiment les produits, s'ils en aiment certains, ce qu'ils aiment particulièrement ; il est pertinent d'obtenir le public et de comprendre ses intérêts. D'autre part, le consommateur d'aujourd'hui passant jusqu'à neuf Heures par jour en ligne, les réseaux sociaux se sont révélés être le moyen le plus efficace pour les entreprises d'atteindre de nouveaux publics à l'échelle mondiale. Les réseaux sociaux contribuent également à alimenter l'économie mondiale en créant de nouveaux emplois, en démocratisant l'information et en poussant les marques bien au-delà de leurs frontières. Les réseaux sociaux ont aussi un impact sur notre vie quotidienne [Pen+18]. Leurs services peuvent aider les jeunes à développer leurs centres d'intérêt et à trouver d'autres personnes partageant les mêmes intérêts. Ils peuvent contribuer à faire découvrir aux jeunes de nouvelles choses et idées, et à approfondir l'appréciation des intérêts existants. D'autre part, on constate aussi que ces réseaux jouent un rôle crucial dans le domaine de la politique [KB18]. Une plateforme de communication telle que les réseaux sociaux est persuasive et permet souvent de changer ou d'influencer les opinions en matière de politique, en raison de l'abondance d'idées, de pensées et d'opinions qui circulent sur la plateforme des réseaux sociaux.

Pour conclure cette rétrospective, l'analyse des réseaux sociaux a une grande variété d'applications. Mais le terme « réseau » est devenu vague précisément en raison de son utilisation de plus en plus répandue. Il est donc important de commencer par définir ce que les analystes des réseaux sociaux entendent lorsqu'ils parlent de réseaux.

1.1.2 Notions de base sur les réseaux sociaux

Les réseaux sociaux en ligne sont devenus l'une des sources d'information les plus puissantes et les plus importantes qui permettent à leurs utilisateurs de partager, de discuter et d'échanger des idées et des opinions sur un sujet d'intérêt [Pen+18]. L'objectif principal des réseaux sociaux est de générer des opportunités, de développer des amitiés en soutenant un système qui permet à ses utilisateurs d'organiser et de mettre à jour leur propre profil, et de partager, d'échanger des contenus d'intérêt pour les utilisateurs au sein du réseau. En outre, ils améliorent l'apprentissage de leurs utilisateurs en partageant des contenus de valeur sur le sujet qui les intéresse et permettent de créer des liens sociaux dans les préférences des utilisateurs et de trouver des personnes intéressantes en partageant des profils à des fins académiques, professionnelles ou personnelles.

Plateforme d'un réseau social

Un réseau social est constitué d'un ensemble de nœuds (parfois appelés acteurs ou sommets dans la théorie des graphes) reliés par un certain type de relations, également appelées liens, arcs ou arêtes. Les nœuds représentent généralement des acteurs, qu'il s'agisse d'individus, de groupes, d'équipes, de communautés, d'organisations, ou même de partis politiques.

Il existe des milliers de sites Web des réseaux sociaux, et les sites diffèrent dans les détails et la présentation des fonctions qu'ils proposent. En outre, ils continuent à ajouter de nouvelles fonctionnalités et à modifier les fonctionnalités existantes. Dans cette section, nous allons fournir une taxonomie des caractéristiques essentielles qui peuvent être extraites des sites populaires d'aujourd'hui. Pour rendre la description de chaque caractéristique concrète, nous fournissons de brèves descriptions de la façon dont quelques sites représentatifs manifestent la caractéristique. Nous notons que, bien que tous les sites Web des réseaux sociaux prennent en charge toutes ces caractéristiques, ils les manifestent de différentes manières et à des degrés divers de sophistication.

Profils des utilisateurs

Les profils sociaux sont les descriptions faites des individus sur les sites de réseaux sociaux tels que LinkedIn et Facebook. Les profils décrivent un certain nombre d'informations sur les individus, telles que les intérêts, l'expertise, les affiliations professionnelles, le statut, l'activité récente et l'emplacement géographique. Les profils sont l'ADN numérique d'une personne. Un profil social affiche également des informations qui aident à comprendre le type et la force des relations d'une personne avec les autres ; par exemple, son niveau de participation et de contribution à différentes initiatives, projets, communautés ou conversations ; sa réputation auprès des autres participants, etc. La création d'un profil social solide permet aux individus d'être découverts par d'autres personnes. Sur la plupart des sites Web des réseaux sociaux, les membres créent et gèrent des profils personnels via des pages d'accueil. Ces pages diffèrent d'un site à l'autre par le type d'informations qu'ils contiennent. Exemple, sur certains sites, les membres peuvent définir des paramètres de confidentialité afin de contrôler qui (par exemple, tout le monde ou seulement les amis) peut accéder à tel ou tel type d'information sur leur profil personnel [RH09].

Partage de l'information et interaction dans les réseaux sociaux

Le partage de l'information est une composante essentielle des réseaux sociaux [CHW06]. La création et le partage du contenu par l'utilisateur sont essentiels au succès d'un réseau social. L'interaction des autres utilisateurs avec ce contenu, via des likes, des commentaires, des re-partages, le sont encore plus. La perception de l'interaction par les utilisateurs peut jouer un rôle dans la satisfaction de l'utilisateur et générer ainsi de l'engagement pour le réseau social en question [SP13].

Groupes

De nombreux réseaux sociaux proposent des groupes par défaut et attribuent les nouveaux membres à un ou plusieurs d'entre eux. Ils permettent également aux membres d'en créer des nouveaux, et/ou de rejoindre des groupes créés par d'autres (des amis par exemple).

Plusieurs innovations sont mises en place par les réseaux sociaux pour encourager et faciliter la communication au sein de ces groupes. Il s'agit notamment de la messagerie instantanée ou de la téléphonie par Internet.

Les réseaux sociaux sont devenus un élément important dans quasiment tous les domaines (social, économique, politique, commercial, artistique, etc). Sur ces réseaux, tout est partagé, tout est daté et tracé. On sait ainsi que M.Dupont a publié tel post depuis un hôtel et pendant ses heures de travail. Une telle information peut avoir un impact sur la vie privée ainsi que le vie professionnelle de M.Dupont.

Par contre, certaines personnes évitent ces réseaux parce qu'elles préfèrent garder leurs données privées. Même en examinant les avantages de la collecte de données, ces personnes ont toujours tendance à aller en ligne, à naviguer, à lire les actualités, à acheter des produits, etc., sans être surveillées.

Il ne fait plus de doute aujourd'hui que l'identification d'une personne de manière directe ou indirecte, comme c'est fait par la plus part des réseaux sociaux, soulève des problèmes.

1.2 Anonymat

Les interactions sociales et la communication interpersonnelle ont connu d'importants changements ces dernières années. La sensibilisation croissante aux problèmes de protection de la vie privée et des événements ont conduit à la croissance rapide d'une nouvelle génération de réseaux sociaux et d'applications de messagerie anonymes. En supprimant les concepts traditionnels d'identités fortes et de liens sociaux, ces services encouragent la communication entre inconnus et permettent aux utilisateurs de s'exprimer sans crainte de harcèlement ou de représailles [Wan+14].

1.2.1 Définition de l'anonymat

Dans la littérature, plusieurs définitions ont été données pour l'anonymat. Selon Wallace dans son travail [Wal99] :

« Anonymity is noncoordinatability of traits in a given respect. »

En d'autres termes, une personne est anonyme lorsque les autres sont incapables de relier une caractéristique donnée de la personne à d'autres caractéristiques [Wal99]. Par exemple, l'Unabomber [Fle21] était anonyme lorsqu'il n'était connu que sous le nom d'« expéditeur de bombes à des scientifiques informaticiens » et que cette caractéristique ne pouvait pas être reliée (coordonnée) à d'autres caractéristiques telles que le nom, l'adresse, le numéro de sécurité sociale et ainsi de suite, de sorte que la personne en tant que telle pouvait être identifiée.

Une autre définition a été donné par Halpern et O'neill dans [HO05] :

« The basic intuition behind anonymity is that actions should be divorced from the agents who perform them ... the information that needs to be hidden is the identity of the agent (or set of agents) who perform a particular action »

Selon cette définition, les actions doivent être séparées des utilisateurs qui les exécutent. D'après les auteurs de cet article, l'information qui doit être cachée est l'identité de l'utilisateur qui effectue l'action.

Dans un autre article de Sudhanshu Chauhan et Nutan Kumar Panda [CP15], les auteurs ont donné une définition de base de ce terme, c'est « être sans nom ». En clair, une personne est anonyme si son identité n'est pas connue. D'un point de vue psychologique,

l'anonymat peut être perçu comme une réduction de la responsabilité des actions réalisées par la personne [CP15]. L'anonymat est également associé à la vie privée, car il est parfois souhaitable de ne pas avoir de lien direct avec une entité spécifique.

Dans la suite, nous étudions quelques systèmes qui font de l'anonymat un levier pour encourager l'échange et le partage.

1.2.2 Exemples des systèmes anonymes

Réseaux sociaux anonymes

Les réseaux sociaux anonymes sont une sous-catégorie de réseaux sociaux dont la principale fonction sociale est de partager et d'interagir autour de contenus et d'informations de manière anonyme sur des plateformes mobiles et web. En d'autres termes les contenus ou informations publiés ne sont pas liés à des identités ou profils en ligne particuliers. Apparu très tôt sur le web sous la forme de sites de confession anonyme, ce type de médias sociaux a évolué vers divers types et formats d'expression anonyme. L'un des premiers forums anonymes de réseaux sociaux a été « 2channel »⁷ [Mat+03], qui a été mis en ligne pour la première fois le 30 mai 1999 sous la forme d'un forum de discussion japonais.

Depuis, plusieurs réseaux sociaux anonymes ont vu le jour, on peut citer Yik Yak et Whisper. C'est un service qui permet d'obtenir un flux en direct de ce que disent les gens autour de nous. Ce qui différencie Yik Yak des autres applications de messagerie anonyme, est qu'il est basé sur la localisation. L'application combine les technologies GPS et de messagerie instantanée pour permettre aux utilisateurs de partager et de découvrir ce dont les gens parlent dans un rayon de 10 miles. C'est pourquoi l'application est devenue une source particulièrement populaire d'informations et de ragots sur les campus universitaires.

Yik Yak a été fondée par des étudiants, Tyler Droll⁸ et Brooks Buffington⁹, et lancée en novembre 2013. L'application a vraiment décollé lorsque les étudiants ont commencé à la partager avec de nouveaux amis rencontrés. En sept mois (7), l'application a été mise à disposition sur 200 campus universitaires. En décembre 2014, l'entreprise Yik Yak était valorisée à plus de 350 millions de dollars. Aujourd'hui, l'application est populaire dans tous les États-Unis et commence à susciter l'intérêt à l'étranger.

7. <https://5ch.net/>

8. <https://www.linkedin.com/in/tylerdroll/>

9. <https://www.linkedin.com/in/brooks-buffington-03a0178a/>

Comme l'application permet des communications anonymes, il n'y a pas de processus d'inscription. Les utilisateurs ne peuvent pas choisir un nom d'utilisateur, car ils n'en ont pas lorsqu'ils utilisent Yik Yak.

Ce qui différencie Yik Yak des autres applications de réseaux sociaux, c'est qu'il ne permet pas de publier des photos, et que les posters ou « yakker » restent anonymes.

Quant au réseau social Whisper¹⁰, il a été lancé en mars 2012 et permet aux utilisateurs d'envoyer des messages et de recevoir des réponses en utilisant des surnoms anonymes. Il a énormément gagné en popularité depuis son lancement en 2012, et compte en moyenne plus de trois(3) milliards de pages vues mensuelles au début de 2014 [Gro14].

L'accent mis par Whisper sur l'anonymat rompt certaines des hypothèses de base des réseaux sociaux traditionnels comme Facebook ou Google+. Premièrement, les utilisateurs de Whisper ne sont identifiés que par des surnoms attribués de manière aléatoire (ou choisis par l'utilisateur), qui ne sont associés à aucune information personnelle, par exemple un numéro de téléphone ou une adresse électronique. Deuxièmement, les serveurs de Whisper ne stockent que les Whispers publics, et les messages privés des utilisateurs ne sont stockés que sur les appareils des utilisateurs finaux. Il n'existe aucune fonctionnalité permettant de rechercher ou de parcourir l'historique des Whispers ou des réponses d'un utilisateur spécifique. Troisièmement, il n'y a pas de notion de lien social persistant entre les utilisateurs (par exemple, des amis sur Facebook, des followers sur Twitter). Les utilisateurs sont donc encouragés à interagir avec un large éventail d'inconnus plutôt qu'avec un groupe d'amis connu.

Dans Whisper, sans liens sociaux, les utilisateurs parcourent le contenu de plusieurs listes publiques au lieu du fil d'actualité de leurs amis (ou followees). Ces listes comprennent une liste des plus récents qui contient les whispers les plus récents (du point de vue du système); une liste proche qui affiche les whispers postés dans les zones proches (environ 40 miles de rayon); une liste populaire qui affiche uniquement les meilleurs whispers ayant reçu de nombreux commentaires et réponses; et la liste des favoris, qui affiche un sous-ensemble de whispers populaires triés sur le volet par les gestionnaires de contenu de Whisper. Toutes ces listes trient le contenu en fonction du plus récent.

L'idée des réseaux sociaux anonymes est plus forte que jamais et une nouvelle vague de services de messagerie et de communication anonyme ou pseudo-anonyme ont vu le

10. <http://whisper.sh/>

jour : Snapchat, Tinder, Signal, etc. Ces applications représentent un lieu sûr pour les personnes qui préfèrent ne pas partager ouvertement certaines pensées avec leurs amis et leur famille, ou qui s'inquiètent du respect de leur vie privée dans les réseaux sociaux traditionnels. C'est un lieu où on peut parler librement sans être jugés ou intimidés.

Les différentes formes de réseaux sociaux anonymes offrent différents degrés d'anonymat. Certaines applications, comme Snapchat ¹¹, demandent aux utilisateurs de créer un compte, même si leur profil n'est pas lié à leurs publications. D'autres comme ou Whisper ¹² utilise la liste de contacts ou l'emplacement de l'utilisateur pour développer un contexte au sein de la communauté sociale et aider à personnaliser l'expérience de l'utilisateur. Le site Yik Yak ¹³, quant à lui renforce l'anonymat et les utilisateurs ne sont pas tenus de créer un compte et les messages sont affichés par défaut sous le nom d'utilisateur « Anonyme ». Bien que les utilisateurs puissent toujours être repérés par leur adresse IP, il existe des services d'anonymisation comme I2P ¹⁴ ou divers services de serveurs proxy qui cachent l'identité d'un utilisateur en ligne en la faisant passer par différents routeurs.

Bitcoin

A l'inverse du Web2 et l'émergence des réseaux sociaux et une forte centralisation des données, le Web3 ambitionne de rendre la donnée aux utilisateurs en utilisant la technologie chaînes de blocs ou blockchain. Une technologie qui permet d'échanger des actifs sous la forme de jetons numériques mais aussi des données sans passer par des tiers, comme des établissements bancaires ou des GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Les chaînes de blocs sont des registres distribués permettant le stockage d'informations dans un réseau pairs à pairs. Chaque membre de ce réseau possède une copie de ce registre. La modification de ce registre peut se faire par le biais de transactions diffusées sur le réseau. Ces transactions sont alors traitées sous forme de lots appelés blocs, par des membres appelés mineurs ou validateurs. Un lien entre chaque bloc validé et son précédent, garantit l'intégrité de l'historique des transactions validées. Par ce lien, une « chaîne » est formée : d'où le nom chaîne de blocs.

La première blockchain est apparue avec la monnaie virtuelle ou crypto-monnaie ap-

11. <https://www.snapchat.com/>

12. <http://whisper.sh/>

13. <https://yikyak.com/>

14. <https://geti2p.net/fr/>

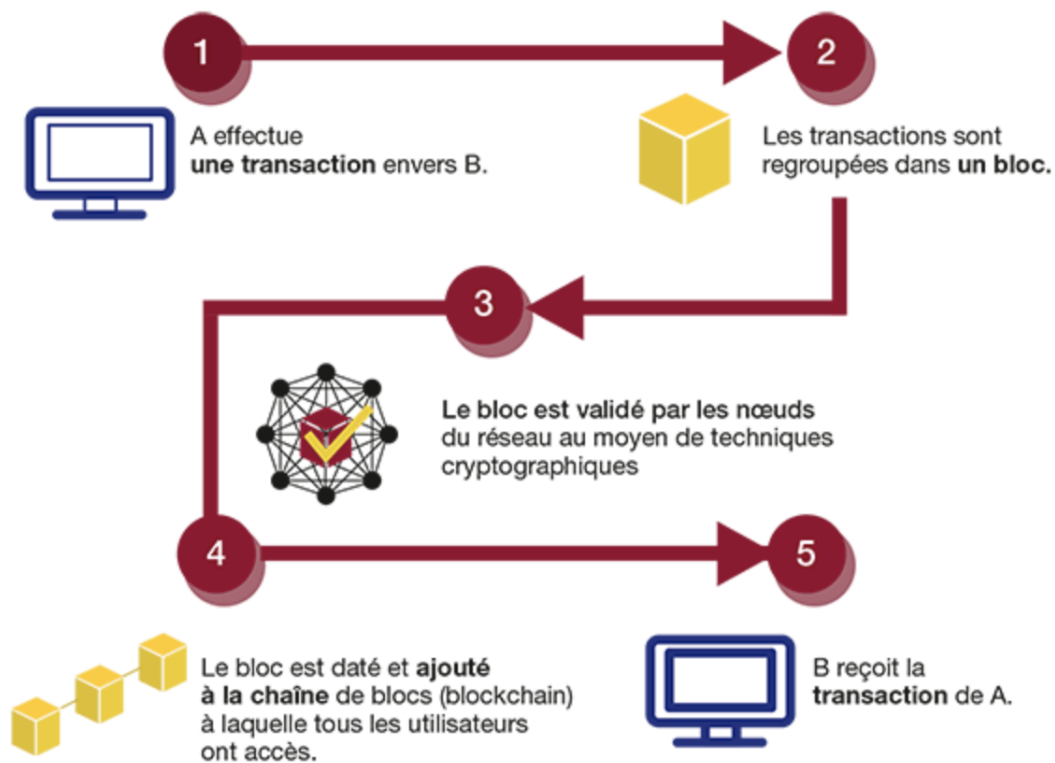


FIGURE 1.2 – Le fonctionnement de la blockchain

pelée Bitcoin [Nak08]. Elle a été inventée en 2008 par Satoshi Nakamoto dont la véritable identité reste encore un mystère, et connaît un véritable engouement depuis. En effet, les banques veulent savoir à peu près tout sur leurs clients et leurs finances, et le bitcoin offre une alternative à ce système intrusif en permettant de réaliser des paiements électroniques de manière anonyme (une paire de clé publique/privée pour authentifier l'utilisateur) et sans aucune autorité centrale (directement de pair à pair). Pas besoin de fournir son adresse personnelle (ou le siège social de son entreprise) ou d'autres informations personnelles, pas besoin non plus d'une banque pour valider la transaction (Figure 1.2 : le fonctionnement de la blockchain).

La sécurité du bitcoin réside dans le protocole de validation des blocs par preuve de travail (proof of work en anglais). La Preuve de travail, aussi appelée minage, consiste à accorder la possibilité d'ajouter un bloc à la chaîne au mineur ou validateur ayant résolu en premier un calcul mathématique complexe et gourmand en ressources. Afin d'inciter les mineurs à participer et à sécuriser le réseau, à chaque minage réussi, le mineur reçoit en contrepartie une récompense en Bitcoin (Figure 1.3 : la preuve du travail).

La chaîne de blocs a fait ses preuves et est à l'heure actuelle incontestablement la meilleure

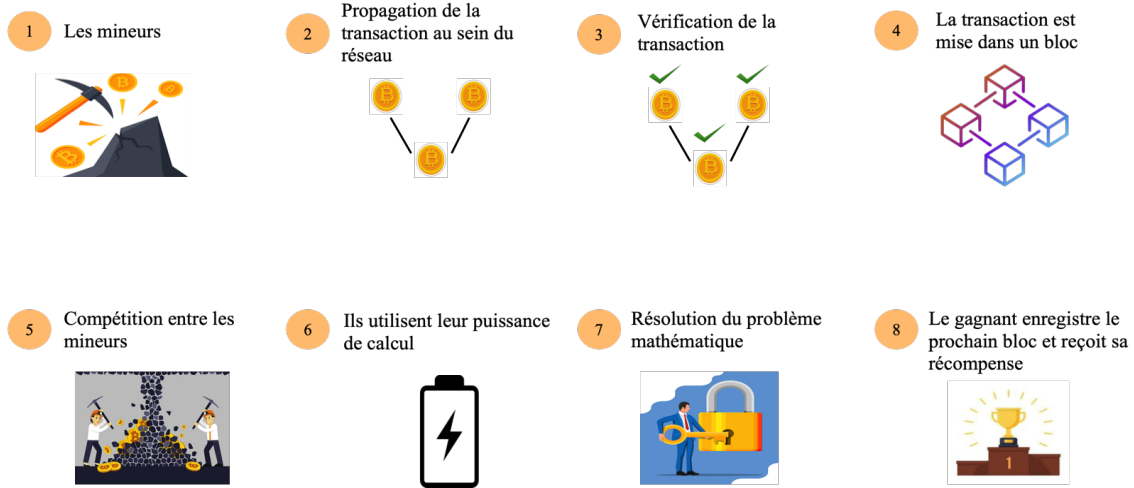


FIGURE 1.3 – Le consensus PoW

technologie permettant de sécuriser les données et les échanges. D'une part, son caractère décentralisé rend techniquement plus difficile le piratage ou l'attaque des bases de données concernées. D'autre part, l'utilisation des techniques cryptographiques pour chiffrer, hacher et signer les données accentue la protection de celles-ci. Cette double protection (décentralisation et cryptographie) garantit une sécurité renforcée par rapport à d'autres systèmes, notamment les systèmes centralisés.

De 2016 à aujourd'hui : La blockchain se généralise. Aujourd'hui, un nombre croissant d'industries considèrent la blockchain comme une technologie de valeur, distincte du bitcoin ou d'autres cybermonnaies. En 2020 près de 39% des personnes interrogées ont intégré la blockchain dans leur production, et 55% considèrent la blockchain comme une priorité stratégique majeure, selon l'enquête mondiale 2020 de Deloitte sur la blockchain [blo22]. Cette tendance se poursuit en 2021 et 2022 avec plus de gouvernements et d'entreprises qui se tournent vers la blockchain pour traiter une variété de cas d'utilisation et pour avoir des systèmes plus sécurisés qui garantissent un bon niveau de confiance pour les utilisateurs.

1.3 Discussion

Le problème majeur qu'on trouve aujourd'hui dans la plupart des réseaux sociaux et des plateformes en ligne, est la collecte de données et leur monétisation.

Après le scandale impliquant Facebook et Cambridge Analytica où les données de 87

| | Profils des utilisateurs | Partage d'informations | Réseau d'amis | La Confiance |
|----------------------|--------------------------|---|---------------|--|
| Les réseaux sociaux | Oui | Des commentaires et des messages identifiés | Oui | Par la collecte de données Profils traçables |
| Les réseaux anonymes | Non | Des commentaires, messages et transactions anonymes Nombres d'interactions | Non Non | Des techniques comme la blockchain et la cryptographie |

TABLEAU 1.1 – Principaux caractéristiques des réseaux sociaux et des réseaux anonymes

millions de personnes ont été recueillies à leur insu, les révélations d'Edward Snowden sur le système de surveillance de masse de la NSA et le scandale Yahoo qui a révélé un piratage de 500 millions de comptes utilisateurs, l'inquiétude des consommateurs concernant la protection de leur vie privée s'intensifie. Bon nombre d'entre eux se sentent vulnérables et en colère quant à la manière dont leurs données personnelles sont collectées et bien souvent revendues. On assiste ainsi à un début de rejet des nouvelles technologies, basé sur la seule crainte d'une utilisation abusive des données personnelles et des piratages.

L'anonymat peut constituer une alternative au problème ci-dessus, mais il peut aussi être utilisé à mauvais escient.

L'une des critiques les plus courantes à l'égard des réseaux sociaux anonymes est la facilité avec laquelle un utilisateur peut publier une remarque diffamatoire.

Au-delà de la préoccupation liée à la cyberintimidation et aux messages abusifs, des inquiétudes plus sérieuses sont apparues à propos de certaines de ces applications. Par exemple, des groupes de suprémacistes blancs utilisent des comptes anonymes sur les réseaux sociaux pour alimenter la violence, comme lors de l'émeute de Charlottesville en 2017¹⁵. Une action en justice a été intentée pour révéler l'identité de ceux qui ont perpétré des violences. Les réseaux sociaux anonymes peuvent également conduire au harcèlement et au meurtre, comme dans le cas de Nicole Madison Lovell. La jeune fille de 13 ans a été tuée par deux hommes de 18 ans avec lesquels elle communiquait de manière anonyme [SP16].

L'anonymat ou pseudo-anonymat des cryptomonnaies telles que le Bitcoin, ont accéléré le succès du DarkNet. Également appelé dark web, le DarkNet est la partie caché de l'internet, non indexée par les moteurs de recherche, où les trafics en tous genres prospèrent : vente de drogue, d'armes, de numéro de carte de crédit et données personnelles. Aujourd'hui, une identité avec photos personnelles, nom, prénom, adresse e-mail, se vend plus de

15. <https://www.lapresse.ca/international/etats-unis/201810/02/01-5198827-violences-a-charlottesville-quatre-supremacistes-blancs-inculpés.php>

200 euro sur le DarkNet.

Si nous approfondissons nos recherches, nous pouvons comprendre que ces données peuvent être collectées aussi à d'autres fins. Cela peut être la sécurité et la confiance. Lorsque le système sait tout sur ses utilisateurs, même s'ils ont l'intention de tricher ou de frauder, ils seront traqués [MFS15]. Cet objectif a été atteint par les réseaux anonymes en utilisant d'autres techniques que la collecte des données. Cette différence entre les réseaux sociaux et les réseaux anonymes est montrée dans le Tableau 1.1.

£En permettant aux utilisateurs de publier des messages anonymes, ces applications anonymes encouragent les confessions personnelles, les accusations et les affirmations que la plupart des gens ne se sentiraient normalement pas à l'aise de faire. « Se cacher derrière un écran » permet aux utilisateurs de dire ce qu'ils pensent librement sans être tenus responsables, induisant à la fois un manque d'empathie et de réflexion intellectuelle. En raison de l'anonymat, cependant, les gens sont plus susceptibles d'abandonner les normes sociales et la responsabilité qui auraient autrement permis de contrôler leur comportement.

En conclusion, dans tous ces systèmes, la non-collecte des données personnelles des utilisateurs est sans aucun doute la meilleure solution à adopter pour un système pour respecter la vie privée de ses utilisateurs. Mais comment instaurer la confiance au sein d'un tel système pour favoriser l'échange et le partage d'information.

Dans le prochain chapitre, nous dévoilerons la définition de la notion de confiance dans les systèmes informatiques, ainsi que les concepts dont elle dépend pour être bien garantie.



Chapitre 2

Confiance : modélisation, typologie et calcul

Sommaire

| | | |
|------------|---|-----------|
| 2.1 | Introduction | 39 |
| 2.2 | Réputation | 39 |
| 2.3 | Recommandation | 40 |
| 2.4 | Capital Social | 40 |
| 2.4.1 | Calcul de la Confiance à partir du Capital Social | 43 |
| 2.5 | Qualités d'une bonne mesure de confiance | 45 |
| 2.6 | Modélisation de la confiance | 46 |
| 2.7 | Modèles computationnels | 47 |
| 2.7.1 | Réseaux bayésiens | 48 |
| 2.7.2 | Modèle à valeurs discrètes | 50 |
| 2.7.3 | Modèles basés sur la croyance | 51 |
| 2.7.4 | Modèles flous | 51 |
| 2.7.5 | Modèles de flux | 52 |
| 2.7.6 | Exemples des systèmes basés sur la confiance | 53 |
| 2.7.6.1 | Amazon | 53 |
| 2.7.6.2 | Blablacar | 54 |
| 2.7.7 | Approches d'évaluation des modèles computationnels de confiance | 55 |
| 2.8 | Modèles de propagation de la confiance | 56 |
| 2.8.1 | Modèles de visualisation | 56 |

2.1 Introduction

L'utilisation des réseaux sociaux basés sur le web s'est d'abord limitée à la mise en relation des personnes avec leurs amis et leur famille [Hay05]. La croissance phénoménale du nombre d'utilisateurs de réseaux sociaux ces derniers temps n'est pas passée inaperçue [SNP13]. Les gouvernements et les entreprises ont commencé à exploiter l'utilisation potentielle des réseaux sociaux en tant que plateformes pour fournir et améliorer leurs services [Jae+07]. Cependant, les médias ont rapporté de nombreux incidents de violation de la vie privée des individus par les réseaux sociaux [GA05]. Compte tenu de la nature ouverte des réseaux sociaux basés sur le Web et de leur niveau de popularité actuel, les utilisateurs sont de plus en plus préoccupés par le respect de la vie privée. Afin d'équilibrer la nature ouverte des réseaux sociaux et de préserver les préoccupations des utilisateurs en matière de vie privée, il est important de créer des communautés de confiance [SNP13]. Ce sont des communautés qui créent un environnement dans lequel les membres peuvent partager leurs pensées, leurs opinions et leurs expériences de manière ouverte et honnête sans se soucier de la vie privée et sans craindre d'être jugés. Par conséquent, la confiance devient un aspect important des réseaux sociaux et des communautés en ligne.

La confiance a été étudiée dans de nombreuses disciplines, notamment la sociologie [Hel94; Möl01], la psychologie [Rot67], l'économie [Hua07] et l'informatique [MTG07]. Chacune de ces disciplines a défini et considéré la confiance sous des angles différents. En général, la confiance est une mesure de l'assurance qu'une ou plusieurs entités se comporteront de la manière attendue [SNP13]. L'atout le plus important de toute société ou d'un réseau social est la réputation et le capital social [MQR04]. Ces concepts représentent la richesse des interactions entre les membres d'un réseau social [SNP13].

2.2 Réputation

Selon Josang et al dans [JIB07], « la réputation est ce que l'on dit ou croit d'une personne ou des propriétés d'un objet ». Dans le même papier, les auteurs affirment que la réputation est « un moyen pour renforcer la confiance », puisque dans une communauté, on peut faire confiance à quelqu'un s'il a bonne réputation.

Dans un autre travail de Vu [Vu10], la réputation « est l'opinion d'une communauté envers une personne, un groupe, ou une organisation ».

Selon d'autres définitions, il faut prendre en compte deux sources d'informations principales pour estimer la réputation : les expériences passées avec le sujet et les recommandations des autres entités de la communauté. Comme dans le travail de de Abdul-Rahman et Hailes dans [AH00a], la réputation « est une estimation du comportement d'une entité dans la communauté, basée sur ses comportements passés ».

Ces définitions de la réputation font toujours référence à une communauté. Si une personne a une bonne réputation dans sa communauté, elle est reconnue comme digne de confiance et elle peut être également recommandée pour établir d'autres actions. De ces définitions, on voit que la confiance est liée aussi au concept de la recommandation.

2.3 Recommandation

Dans les systèmes de confiance, les utilisateurs sont capables d'échanger des informations sur leur réputation par le biais de recommandations, soutenant ainsi un mécanisme de réputation pour faciliter les décisions de confiance [AH00a]. La recommandation pourrait ainsi être une valeur qualitative (recommandation positive ou négative), ou quantitative (une note de 1 à 5, des étoiles, etc).

Dans un système de confiance, après chaque collaboration, chaque utilisateur peut évaluer la qualité de l'expérience. Cette évaluation est transmise à un troisième utilisateur. Ainsi, l'ensemble de ces actions permet de construire un mécanisme d'échange et de propagation des informations de réputation entre les différents utilisateurs du système. Cela permet de construire des systèmes de confiance basés sur la recommandation [Vu10].

2.4 Capital Social

Dans le contexte des réseaux sociaux, la confiance est dérivée du capital social [SNP13]. D'après l'encyclopédie Larousse [lar22], le capital social est un :

« ensemble des connaissances et des savoir-faire d'un individu acquis par formation et/ou expérience qui lui permettent d'être plus productif dans son travail. »

De cette définition, on peut voir que le capital social est un élément important de la prospérité d'une personne et cette dernière contribue automatiquement à la prospérité d'une communauté. Dans la littérature, le capital social n'a pas de signification claire et

incontestée, pour des raisons substantielles et idéologiques [DD03]. Pour cette raison, il n'existe pas de définition fixe et communément acceptée du capital social et la définition particulière adoptée par une étude dépendra de la discipline et du niveau d'investigation [RSS02]. Il n'est pas surprenant, compte tenu des différents cadres d'analyse du capital social, que les définitions du capital social soient très divergentes, voire contradictoires [AK02].

Un bon résumé introductif du capital social et un nombre considérable de définitions peuvent être trouvés dans [Cla04]. Comme nous nous concentrons sur les réseaux sociaux, nous ne considérons le capital social que sous cet aspect.

Les auteurs de [MQR04] suggèrent que le capital social peut être défini comme étant soit basé sur les préférences (altruisme dirigé), soit coopératif (interactions répétées entre paires ou groupes d'acteurs). Dans [Bru09], Brunie étudie le capital social à travers trois dimensions : relationnelle (capacité d'un membre à mobiliser des contacts sociaux afin d'obtenir des ressources valorisées), collective (ressource pour faciliter la coopération au niveau du groupe) et généralisée (valeurs et attitudes qui influencent les relations entre les personnes et qui les prédisposent à coopérer, à se faire confiance, à se comprendre et à faire preuve d'empathie). Selon [SNP13], le capital social désigne la valeur collective associée à un réseau social. Diverses approches pour le mesurer ont été proposées dans la littérature. Par exemple, dans [NG98] les auteurs proposent de mesurer le capital social selon trois dimensions : structurelle (modèles d'interactions sociales entre les acteurs), relationnelle (les relations entre les acteurs) et cognitive (représentations, interprétations et systèmes de signification partagés entre les acteurs).

Toutes ces approches sont applicables aux réseaux sociaux. Étant donné que notre sujet de recherche est la communauté et les relations entre les individus qui la composent, nous suivons la définition de Brunie dans sa dimension collective, puisqu'il considère le capital social du point de vue de l'ensemble de la communauté.

« In the collective approach, social capital is viewed as a collective resource that facilitates cooperation at the small group level. Social capital is understood as a collective property, and is essentially defined in relation to its function (i.e., facilitating coordination and cooperation for mutual benefit) ... a fundamental difference with the relational approach is that social capital no longer resides with an individual but exists through relationships between actors »

Il ressort clairement de cette définition que les interactions jouent un rôle important dans la définition et la mesure du capital social. Dans une communauté en ligne, le capital social fait référence à la valeur dérivée des interactions qui favorisent la création de liens entre des personnes partageant les mêmes idées.

La confiance est considérée comme un aspect important du capital social qui représente l'infrastructure coopérative d'une communauté [Col88]. Les distinctions entre le capital social et la confiance ont parfois été floues dans la littérature. Par exemple, dans [Pal00] Paldam définit le capital social comme la quantité de confiance qu'un membre a dans les autres membres de la communauté. Ce type de définition ne distingue pas le capital social de la confiance. La confiance est un élément important du capital social, mais ce n'est pas la même chose [SNP13]. En revanche, d'autres travaux sont parvenus à lever cette ambiguïté et à souligner la distinction entre ces deux concepts. Prenons l'exemple du travail de Putnam dans [Put00], il a défini le capital social comme suit :

« By analogy with notions of physical capital and human capital—tools and training that enhance individual productivity— ‘social capital’ refers to features of social organization such as networks, norms, and social trust that facilitate coordination and cooperation for mutual benefit. »

Cette définition montre que le capital social est un concept plus général qui englobe la confiance. Selon la théorie de Putnam, il y a présence de capital social dans la communauté lorsque les membres de la communauté font preuve d'un bon comportement. Un bon comportement n'est possible que si la confiance règne entre les membres. Bien qu'ils ne soient pas équivalents, la confiance et le capital social sont interconnectés à bien des égards et se renforcent réciproquement. Le terme de capital social traduit l'idée que les relations humaines coopératives sont cruciales pour améliorer divers aspects de la vie des gens, et qu'il s'agit d'un stock qui doit être préservé et développé pour la durabilité du bien-être.

Plus tard en 2007, Huang dans [Hua07] a donné une définition pour le capital social en prenant en considération les tendances coopératives individuelles et leurs rôles dans la construction de la confiance. Dans son travail, Huang étudie la relation entre la confiance et le capital social (il l'a nommé aussi « capital humain ») en se concentrant sur la façon dont le capital social pourrait être cultivé pour augmenter la confiance. Sa théorie est basée sur le principe que les individus diffèrent dans leur prédisposition à coopérer. Certaines personnes sont intrinsèquement plus confiantes que d'autres, comme

les personnes altruistes qui aident les autres sans calculer leur gain personnel. Huang les a décrits comme des personnes ayant une « tendance coopérative ». La tendance à la coopération est considérée comme une composante du capital social qu'il est coûteux de développer, mais qui génère un flux de bénéfices à l'avenir (notamment en augmentant la confiance). Lorsqu'un plus grand nombre de personnes ont des tendances coopératives plus élevées dans une société, elles sont plus confiantes, et donc la confiance de la société est plus élevée.

D'après ces définitions, on comprend que le capital social représente toutes les informations nécessaires pour garantir la confiance dans une communauté. Cette confiance est mesurable dans les systèmes informatiques.

Une bonne valeur d'une personne donne confiance aux autres utilisateurs et les incite à se coopérer avec cette personne. Elle représente donc un véritable enjeu pour la réussite des communautés.

2.4.1 Calcul de la Confiance à partir du Capital Social

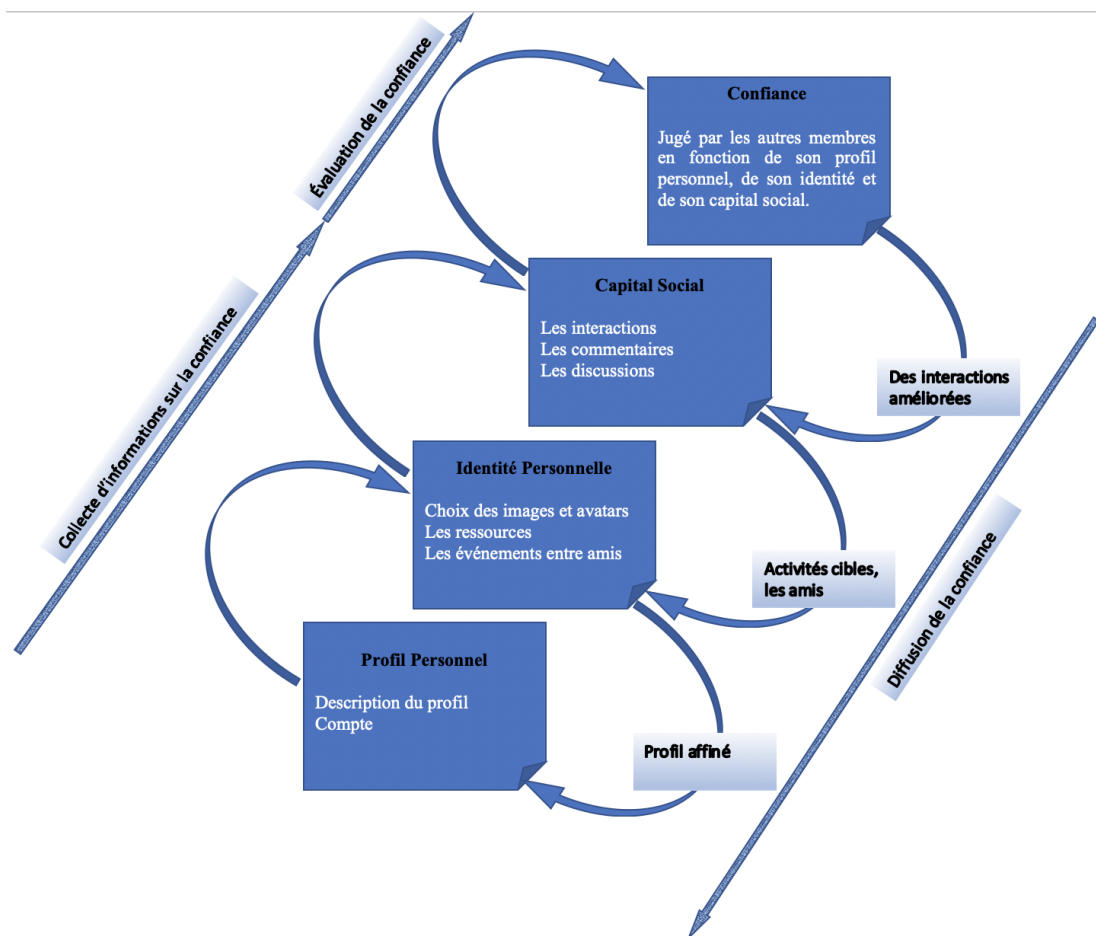


FIGURE 2.1 – Processus de création de la confiance sociale

Le processus de calcul de la confiance (appelée aussi confiance sociale) à partir du capital social dans un réseau social est illustré dans la Figure 2.7.1. Ce processus a été traité dans le papier de Sherchan et al. [SNP13].

Un utilisateur d'un réseau social doit en premier lieu créer un profil personnel, après s'être enregistré dans ce réseau. Ce profil contient généralement des informations personnelles que l'utilisateur souhaite partager avec les autres membres de la communauté (Exemple : son nom et prénom, sa date de naissance, ses loisirs, etc.). Par la suite, l'utilisateur doit créer une identité personnelle. Dans les réseaux sociaux non anonymes, cette identité peut-être son nom complet, sa photo de profil, invitations à des amis spécifiques, etc. Dans les réseaux sociaux anonymes, l'utilisateur choisit par exemple un pseudonyme, un avatar au lieu d'une photo de profil, etc. La troisième étape consiste à interagir avec les autres membres de la communauté, contribuant ainsi au capital social. Les interactions peuvent être sous la forme de publications, de commentaires sur ces publications, de réponses sur les autres commentaires, des avis, etc. La dernière étape consiste à calculer la confiance à partir du capital social, qui peut à son tour être utilisée pour améliorer le capital social du réseau par le biais de systèmes de recommandation.

Comme le montre la Figure 2.1, l'obtention de la confiance comprend généralement trois étapes : (i) la collecte d'informations sur la confiance, (ii) l'évaluation de la confiance (c'est le calcul de la confiance), et (iii) la diffusion de la confiance.

Comme mentionné ci-dessus, la confiance dépend tout le temps des informations, des interactions et des commentaires des utilisateurs de la communauté. Ces informations et interactions représentent le comportement des utilisateurs dans le réseau.

Chaque utilisateur a son comportement spécifique dans les communautés en ligne, et ce comportement peut changer avec le temps et selon le contexte de la situation. Ce changement affecte bien sûr la valeur de la confiance. Les systèmes et les réseaux qui calculent une valeur de confiance, doivent toujours s'adapter à ce changement en le détectant et en agissant à tout comportement anormal. Pour y parvenir, il faut que ces systèmes répondent à certains critères.

2.5 Qualités d'une bonne mesure de confiance

Les systèmes basés sur la confiance permettent de calculer une valeur de confiance pour chaque utilisateur. Ces systèmes dépendent des notes données par l'ensemble des utilisateurs pour donner une certaine signification aux évaluations dans leur ensemble. Les notes peuvent être très simples ou impliquer plusieurs échelles et des calculs compliqués. Le fonctionnement détaillé de ces systèmes va être expliqué plus tard.

Dans un système de confiance, les utilisateurs peuvent donner des notes - c'est-à-dire des chiffres qui reflètent leur satisfaction à l'égard d'une transaction donnée - pour une variété de dimensions différentes. Par exemple, dans le cas d'un achat, un fournisseur donné peut avoir de bonnes performances en termes de temps de réponse ou de service à la clientèle, mais son emplacement géographique peut être peu pratique. Les acheteurs donnent leur avis sur plusieurs de ces critères d'évaluation à la fois, afin de fournir une vision globale de l'entité. Le travail du système de confiance consiste à agréger ces évaluations en une ou plusieurs notes publiées qui sont significatives et utiles aux participants du système. Un bon système de confiance possédera un grand nombre de qualités [Ora01]. Ces qualités sont les exigences auxquelles le système doit satisfaire. Donc, si on doit trouver un moyen de calculer la confiance, ça serait bien qu'il ait ces qualités.

Précision pour une performance à long terme

Le système reflète la confiance (la probabilité d'exactitude) d'un score donné. Il peut également distinguer entre un nouvel utilisateur de qualité inconnue et un utilisateur ayant de mauvaises performances à long terme.

Pondération vers le comportement actuel

Le système reconnaît et reflète les tendances récentes de la performance des utilisateurs. Par exemple, un utilisateur qui s'est bien comporté pendant longtemps, mais qui soudainement se dégrade, est rapidement reconnue et on ne lui fait plus confiance.

Efficacité

Il est pratique que le système puisse recalculer rapidement un score. Les calculs qui peuvent être effectués de manière incrémentale sont importants.

Robustesse contre les attaques

Le système doit résister aux tentatives d'un utilisateur d'influencer les scores autrement qu'en étant plus honnête ou en ayant une meilleure qualité.

Evaluation statistique

Il devrait être facile de trouver les valeurs aberrantes et les autres facteurs qui peuvent faire que le système évalue les scores différemment.

Confidentialité

Personne ne devrait être en mesure de savoir comment un évaluateur donné a évalué un utilisateur, sauf l'évaluateur lui-même.

Souplesse de calcul

L'ajout d'une seule note ou d'un petit nombre de notes ne doit pas modifier beaucoup le score.

Compréhensibilité

Il devrait être facile d'expliquer aux personnes qui utilisent ces scores ce qu'ils signifient - non seulement pour qu'elles sachent comment le système fonctionne, mais aussi pour qu'elles puissent évaluer elles-mêmes ce que chaque score implique.

Vérifiabilité

Un score contesté peut être étayé par des données.

2.6 Modélisation de la confiance

Les architectes des technologies de l'information doivent créer des applications, des systèmes et des réseaux qui répondent aux attentes des utilisateurs en matière de confiance.

Une architecture de sécurité basée sur un modèle de confiance acceptable fournit un cadre pour la mise en œuvre de mécanismes de sécurité. La modélisation de la confiance

est le processus qui sert à définir un profil de menace complémentaire et un modèle de confiance basé sur une analyse des flux de données axée sur les cas d'utilisation. Le résultat de cet exercice intègre des informations sur les menaces, les vulnérabilités et les risques d'un comportement anormal d'un ou plusieurs utilisateurs. De plus, la modélisation de la confiance identifie les mécanismes spécifiques qui sont nécessaires pour répondre à un profil de menace spécifique [AWW02].

Selon Deutsch [Deu62], les personnes fiables (qui ont une bonne réputation dans le système) sont plus susceptibles de faire confiance que les personnes moins fiables. D'après cette théorie, si une personne est fiable et digne de confiance, elle est encline à croire innocemment que tout le monde lui ressemble. Par contre, si une personne est non fiable et a un comportement malveillant, elle connaît les méthodes et techniques de tricherie et donc elle sait de quoi les autres sont capables. Marsh a utilisé cette notion dans [Mar94], en expliquant qu'on peut estimer la valeur de confiance d'un agent en connaissant à quelle valeur de confiance cet agent nous estime.

D'après cette définition, on peut déduire que dans les systèmes informatiques, cette relation de confiance doit être mesurable. En fonction du comportement de chaque utilisateur et de ses expériences, le système calcule une valeur de confiance qui le présentera aux autres utilisateurs afin de décider s'ils veulent coopérer avec lui ou non. Cette mesure de confiance a été utilisée par les systèmes basés sur la confiance pour établir la sécurité dans l'échange d'informations entre les utilisateurs. Pour obtenir cette valeur, ces systèmes reposent sur des mécanismes de calcul, ce sont les modèles computationnels.

Un état de l'art sur ces modèles ainsi que les approches de leur évaluation vont être présentés dans la section suivante.

2.7 Modèles computationnels

Les principaux problèmes caractérisant les systèmes de confiance sont la métrique de la confiance (comment modéliser et calculer la confiance) et la gestion des données de réputation (comment récupérer de manière sûre et efficace les données requises par le calcul de la confiance) [AD01].

Marsh [Mar94] a fait l'une des premières tentatives de formalisation de la confiance en utilisant des mesures de confiance simples basées sur des équations linéaires. Ce modèle a

été étendu par Abdul-Rahman et Hailes pour traiter la confiance basée sur la réputation dans les communautés virtuelles [AH00a]. Un certain nombre de mécanismes de réputation pour les systèmes P2P, tels que [AD01; KSG03; DSC05], ont suivi des modèles de confiance et de réputation similaires.

Comme mentionné ci-dessus, les systèmes à base de confiance reposent sur des mécanismes de calcul. Ce mécanisme doit fournir un résultat qui aide à prendre une décision de coopération; c'est-à-dire si le résultat est une valeur élevée, celle-ci permet de juger une entité digne de confiance, ainsi on peut lui faire confiance et interagir avec elle. Dans le cas contraire, une faible valeur de confiance permet de juger une entité non fiable et de ne pas lui faire confiance. De nombreux chercheurs ont proposé des méthodes pour représenter et calculer la confiance. Ces méthodes sont appelés « *les modèles computationnels* ».

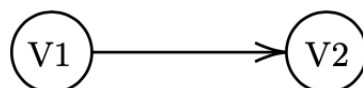
Les modèles computationnels ont été classés dans différentes catégories : modèles bayésiens, modèles à valeurs discrètes, modèles basés sur la croyance, modèles flous et modèles de flux. Un tour d'horizon de ces modèles est nécessaire pour comprendre leur fonctionnement et la différence entre eux.

2.7.1 Réseaux bayésiens

Les modèles bayésiens prennent des scores d'entrée binaires (c'est-à-dire positifs ou négatifs) et sont basés sur le calcul de scores de confiance et de réputation par la mise à jour statistique de fonctions de distribution de probabilité. Formellement, un réseau bayésien est défini comme un graphe orienté acyclique noté $G = (V, E)$ où V est l'ensemble des variables aléatoires (nœuds) et E est l'ensemble des arcs représentant les liens de causalité entre les variables. Naturellement, une organisation bayésienne est à la fois :

- un modèle de représentation des connaissances ;
- une « machine à calculer » des probabilités conditionnelles ;
- une prémisse pour les systèmes d'aide à la décision.

Intuitivement, pour représenter une relation de cause à effet à l'aide d'un graphique, une flèche est généralement utilisée comme suit :



Implicitement, cela signifie que la connaissance que nous avons de V1 influence notre connaissance de V2, ce qui est souvent noté V1 implique V2. Cette référence est réciproque dans les réseaux bayésiens : dès lors que l'on connaît la loi de probabilité de V2, on peut donc déduire V1 en observant V2.

Parmi les modèles de la littérature, il y en a plein qui ont utilisé cette catégorie pour représenter et calculer la confiance entre les entités d'un système [CJI02; AXJ15; Wie+13; Lee+13; AA14; HWA15].

On peut prendre le modèle de Jøsang comme exemple [CJI02] « Beta reputation system ». Ce modèle repose sur la loi de distribution bêta qui est une famille de distributions de probabilité continues définies sur l'intervalle $[0, 1]$ paramétrées par deux paramètres, dénotés par alpha (α) et bêta (β). La fonction de cette loi est définie comme suit :

$$f(p|\alpha\beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \times \Gamma(\beta)} p^{(\alpha-1)} (1-p)^{\beta-1} \quad (2.1)$$

Avec $0 \leq p \leq 1$, $\alpha > 0$, $\beta > 0$, Γ la fonction Gamma et :

$$\alpha = r+1; \beta = s+1$$

Dans cette équation, r représente le nombres d'interactions positives et s le nombre d'interactions négatives.

Jøsang modélise la confiance par la probabilité subjective qui correspond à la valeur de probabilité d'espérance de la bêta distribution :

$$E(p) = \frac{\alpha}{\alpha + \beta} \quad (2.2)$$

Jøsang utilise ces définitions pour proposer une fonction de réputation correspondant à la bêta distribution de la fonction 4.1 :

$$\vartheta(p|r_T^X s_T^X) = \frac{\Gamma(r_T^X + s_T^X + 2)}{\Gamma(r_T^X + 1)\Gamma(s_T^X + 1)} p^{r_T^X - 1} (1-p)^{s_T^X} \quad (2.3)$$

ϑ est appelé la confiance de T en X. r_T^X représente les expériences positives de X avec la cible T, tandis que s_T^X représente les expériences négatives de X avec T. D'après la fonction d'espérance définie dans l'équation 2.2, Jøsang modélise la valeur de probabilité

d'espérance de la fonction de réputation comme suit :

$$E(\vartheta(p|r_T^X s_T^X)) = \frac{r_T^X + 1}{r_T^X + s_T^X + 2} \quad (2.4)$$

Ainsi, l'auteur propose une valeur de confiance qu'il appelle aussi la valeur de réputation de T en se basant sur ses expériences positives et négatives avec X notées respectivement r_T^X et s_T^X :

$$Rep(r_T^X s_T^X) = E(\vartheta(p|r_T^X s_T^X) - 0.5) \times 2 = \frac{r_T^X - s_T^X}{r_T^X + s_T^X + 2} \quad (2.5)$$

Ce score représente alors une mesure de la réputation, c'est-à-dire comment l'utilisateur T est évalué pour ses futures interactions.

2.7.2 Modèle à valeurs discrètes

Les humains sont souvent plus aptes à évaluer les performances sous la forme de déclarations verbales discrètes que de mesures continues. Cela est également vrai pour déterminer les mesures de confiance, et certains auteurs ont proposé un modèle de confiance discret. L'inconvénient des mesures discrètes est qu'elles ne se prêtent pas facilement à la manipulation informatique. Ce que l'on constate dans la littérature, c'est qu'il n'y a pas beaucoup de modèles qui ont utilisé ce type de données. Parmi ceux étudiés, on peut citer [AH00a; Lin+15] qui ont évalué la confiance et la réputation sous la forme de déclarations verbales discrètes.

La croyance d'un agent envers un autre agent dans un contexte spécifique est représenté par 4 valeurs : très fiable, fiable, douteux, très douteux. L'expérience directe d'un agent avec un autre agent admet 4 valeurs : très bonne, bonne, mauvaise, très mauvaise [Gai11].

Le but dans ce modèle est d'obtenir une mesure de la distance sémantique entre la recommandation d'un utilisateur y pour un utilisateur z faite à l'utilisateur x et l'expérience personnelle directe que x a réellement perçue. Par exemple, « si Alice demande à Bob à quel degré elle peut avoir confiance en Jean et que Bob lui répond que Jean est très fiable et qu'Alice s'aperçoit finalement que Jean n'est pas très fiable mais juste fiable, alors Alice adaptera les prochaines recommandations de Bob en les abaissant d'un niveau. Cette distance sémantique se nomme valeur de recommandation de confiance » [Gai11].

2.7.3 Modèles basés sur la croyance

Un modèle basé sur la croyance peut être un système similaire à l'hypothèse de probabilité, mais où l'ensemble de probabilités sur tous les résultats possibles ne correspond essentiellement pas à 1, et la probabilité restante conduit à l'incertitude. En examinant les modèles de la littérature étudiée, nous avons constaté plusieurs modèles prenaient en compte l'idée d'incertitude ou d'incrédulité, on peut citer à titre d'exemple [AXJ15; ŠHZ16; MB15; Aca+16]. Non seulement ils ont calculé la valeur de la confiance ou de la réputation, mais ils ont également indiqué qu'un utilisateur dans une telle situation pourrait ne pas être en mesure de juger ou d'évaluer un autre utilisateur, surtout s'il n'y a pas de transactions entre les deux.

Jøsang a enrichi son modèle développé dans [CJI02] par une théorie de la croyance. Une mesure spécifique de la croyance, appelée l'opinion, est calculée pour représenter une croyance spécifique. La mesure de la croyance est utilisée dans des situations d'ignorance et d'incertain. L'opinion est un triplet défini de la manière suivante :

$$\omega_x^A = (b, d, u)$$

Dans cette équation, $b + d + u = 1$ avec $b \in [0, 1]$ représente la probabilité de vérité, $d \in [0, 1]$ la probabilité de fausseté et $u \in [0, 1]$ la probabilité d'incertitude. La valeur u permet à un utilisateur d'exprimer son incapacité à évaluer la valeur de probabilité de x . Jøsang a proposé une combinaison du modèle de bêta probabilité et du modèle de croyance :

$$b = \frac{r}{r + s + 2}$$

$$d = \frac{s}{r + s + 2}$$

$$u = \frac{2}{r + s + 2}$$

2.7.4 Modèles flous

La confiance et la réputation peuvent être considérées comme des concepts linguistiques flous, où les fonctions d'appartenance décrivent la mesure dans laquelle un acteur peut être décrit, par exemple, comme : « digne de confiance » ou « indigne de confiance ». Les modèles flous ne sont pas des outils de calcul mais aident à représenter la confiance et

la réputation de manière qualitative à partir de valeurs numériques. Certains modèles de la littérature appartiennent à cette catégorie de modèles [JT14; Trč14; TMP15; AA16a].

Le système REGRET proposé par Sabater et Sierra dans [SS02] est un exemple des systèmes qui sont basés sur le modèle flou. C'est un système de commerce électronique dans lequel la réputation est un concept multi dimensionnel (individuelle, sociale et ontologique). Dans ce système, les utilisateurs peuvent coopérer, être en compétition ou commercer.

La dimension individuelle représente « l'expérience directe entre l'utilisateur et l'utilisateur cible. Un contrat entre deux utilisateurs est défini par le prix, la qualité et la date de livraison du produit. La confiance est modélisée en fonction de la différence entre le contrat initial et les résultats de la vente. Cette différence va permettre de classer l'utilisateur cible dans une catégorie, par exemple, la catégorie {fait payer trop chère} » [Gai11].

Dans la dimension sociale un utilisateur fait appel à des témoins qui ont déjà un score de réputation pour l'utilisateur cible ou à des voisins de l'utilisateur cible. En fonction de la relation du témoin avec la cible et du degré de cette relation, l'utilisateur donnera un degré de croyance aux informations apportées par le témoin ou le voisin. Par exemple, si le témoin coopère fortement avec l'utilisateur cible alors les informations du témoin sont très mauvaises [Gai11]. La dimension ontologique combine la réputation de différents aspects afin de calculer une réputation complexe. Par exemple, mettre l'utilisateur cible dans une nouvelle catégorie qui est une combinaison de deux catégories [Gai11].

2.7.5 Modèles de flux

Les systèmes, qui calculent la confiance ou la réputation par itération transitive à travers des chaînes en boucle ou arbitrairement longues, sont appelés modèles de flux [JIB07]. Quelques modèles de flux supposent un poids constant de confiance/réputation pour la communauté dans son ensemble, et ce poids peut être transmis entre les membres de la communauté. Les participants ne peuvent augmenter leur confiance/réputation qu'au détriment des autres. Le PageRank de Google [Pag+99] et le système de réputation d'Advogato [Lev09] appartiennent à cette catégorie. En général, la réputation d'un utilisateur augmente avec le flux entrant et diminue avec le flux sortant. Pour ce type de modèle, on peut citer le modèle « Flow-Based Reputation with Uncertainty » présenté dans [ŠHZ16], et le modèle « EigenTrust » développé au départ en 2000 dans [DFM01], puis une version

dynamique de ce dernier a été implémentée en 2016 dans [LWL16].

Le modèle EigenTrust par exemple est basé sur les systèmes Pair-à-Pair, il permet d'assigner à chaque pair une valeur de confiance unique dérivée grâce à l'historique de ce dernier. L'interaction d'un pair i avec un pair j peut être positive ou négative. Le nombre d'interactions positives qu'a eu i avec j est noté $sat(i, j)$ et le nombre d'interactions négatives qu'a eu i avec j est noté $unsat(i, j)$ [DFM01]. Ainsi, une valeur de réputation est calculée :

$$C_{ij} = \frac{\max(S_{ij}, 0)}{\sum_{l \in L} \max(S_{il}, 0)} \in [0, 1] \quad (2.6)$$

Avec L l'ensemble des pairs qui ont eu une expérience direct avec l'utilisateur cible et $S = sat(i, j) - unsat(i, j)$.

2.7.6 Exemples des systèmes basés sur la confiance

2.7.6.1 Amazon

Amazon¹ est une vaste entreprise basée sur Internet qui vend des livres, de la musique, des films, des articles ménagers, des appareils électroniques, des jouets et de nombreux autres biens, soit directement, soit en tant qu'intermédiaire entre d'autres détaillants et les millions de clients d'Amazon. Amazon, détaillant en ligne, fabricant de lecteurs de livres électroniques et fournisseur de services Web, est devenu l'exemple emblématique du commerce électronique.

Les commentaires des vendeurs Amazon sont une mesure permettant d'évaluer les performances d'un vendeur sur Amazon. Il est disponible pour les clients d'Amazon qui achètent des produits auprès de grossistes et de revendeurs.

Amazon permet aux clients de donner leur avis sur les vendeurs dans un délai de 90 jours à compter de la date de leur commande. Les clients peuvent attribuer des notes aux vendeurs et laisser des commentaires, ce qui est facultatif. L'évaluation du vendeur est la moyenne agrégée des commentaires reçus des acheteurs.

Un client peut noter un vendeur ou un produit à l'aide d'un système d'étoiles allant de 1 à 5. Les autres utilisateurs peuvent voter si un commentaire est utile ou non, ces utilisateurs peuvent être membres ou non membres du site. Les commentaires sont ainsi classés selon leur utilité. Chaque utilisateur peut voir, pour chaque commentaire, combien

1. <https://www.amazon.com>

de personnes ont dit qu'il était utile. De cette façon, les utilisateurs peuvent décider de faire confiance au vendeur en fonction des expériences des autres utilisateurs, même s'ils ne se connaissent pas.

Ce processus est utile pour aider les utilisateurs à prendre une décision. Cependant, il y a aussi des problèmes, car les non-membres peuvent voter pour dire que le commentaire est utile. En raison de cette faille du système, une personne peut voter plusieurs fois pour un même commentaire. Ce qui soulève ce commentaire dans le classement. Les vendeurs peuvent utiliser cette technique pour augmenter les commentaires positifs sur leur produit, augmentant ainsi le nombre de ventes de ce produit, car le vendeur peut voter sur un commentaire sans avoir à se connecter. Les développeurs du site ont essayé de trouver une solution pour ce problème en limitant un vote pour un commentaire donné par adresse IP.

2.7.6.2 Blablacar

Blablacar² est une plateforme communautaire payante de covoiturage. Le covoiturage, c'est l'expérience de partager un trajet ensemble entre des conducteurs qui ont des places libres avec des personnes qui voyagent vers la même destination et qui ne se connaissent pas. Il y a deux types de membres : le conducteur et le passager. Après avoir terminé un trajet, les membres peuvent laisser des notes. Un conducteur peut noter le passager pour l'évaluer et le recommander à la communauté de Blablacar. Un passager peut aussi noter le conducteur pour évaluer l'expérience de covoiturer avec lui. Un passager ne peut pas évaluer un autre passager. Chaque membre est invité à laisser des avis afin d'aider les autres membres à mieux le connaître avant de voyager ensemble. (Mon passager sera-t-il ponctuel ? La conduite de cet conducteur est-elle sécurisante ?...). Le principe de la notation dans Blablacar est d'évaluer la performance sous forme d'énoncés verbaux discrets (Excellent, Bon, Correct, Décevant, Très décevant). Le principe de notation permet d'introduire le concept de la confiance qui est un des piliers de la communauté de covoiturage. Cela permet à un membre de la communauté de décider de covoiturer avec quelqu'un qu'il ne connaît pas.

Chacun de ces systèmes, et d'autres, utilise sa propre façon et algorithme pour représenter et mesurer une valeur de confiance. La diversité des algorithmes et démarches

2. <https://www.blablacar.fr/>

mathématiques conduit à des résultats différents. D'où la nécessité des approches pour évaluer ces différents modèles.

2.7.7 Approches d'évaluation des modèles computationnels de confiance

En raison de l'absence d'un cadre d'évaluation communément accepté, les concepteurs de systèmes de réputation tentent de répondre au besoin d'évaluation des systèmes de réputation en décidant eux-mêmes de l'approche qu'ils choisiront. Ils peuvent choisir d'utiliser des expériences de simulation et des critères d'évaluation personnalisés, des expériences conçues et utilisées par d'autres chercheurs, ou encore des outils ou des cadres disponibles conçus pour faciliter la simulation et l'évaluation objective [KT15]. Les systèmes de réputation individuels proposés dans la littérature ont été principalement évalués à l'aide de simulateurs et d'expériences sur mesure. En outre, certains travaux de recherche ont proposé des mécanismes d'évaluation pour la comparaison de différents systèmes de réputation dans un ensemble spécifique de scénarios, qui ne peuvent pas être appliqués directement à tous les cas. Ces mécanismes comprennent des expériences basées sur le jeu du dilemme du prisonnier, ainsi que des expériences qui spécifient des scénarios de test spécifiques et ont été utilisées pour l'évaluation et la comparaison de systèmes de réputation spécifiques pour les environnements de commerce électronique. Ces expériences communes ont été explicitement conçues pour des scénarios spécifiques partagés par un certain nombre de systèmes de réputation. Elles ne peuvent cependant pas être considérées comme des approches d'évaluation génériques pour l'évaluation et la comparaison de systèmes de réputation hétérogènes. Le besoin d'approches d'évaluation génériques a conduit à un certain nombre de travaux de recherche qui se concentrent sur le développement et l'utilisation de cadres génériques pour l'évaluation et la comparaison des systèmes de réputation. Ces travaux sont soit théoriques (c'est-à-dire qu'ils étudient comment un système de réputation traite un certain nombre de critères ou d'attaques), soit ils proposent des plateformes/outils de simulation et de mise en œuvre pour l'évaluation, la comparaison et le réglage fin des systèmes de réputation par l'expérimentation.

En général, selon la littérature [SNP13], les systèmes de confiance peuvent être classés en fonction de trois critères : (i) la collecte d'informations sur la confiance, (ii) l'évaluation de la valeur de la confiance, et (iii) la diffusion de la valeur de la confiance, comme le montre la Figure 2.2. Chacun de ces critères peut à son tour être classé : la collecte d'informations

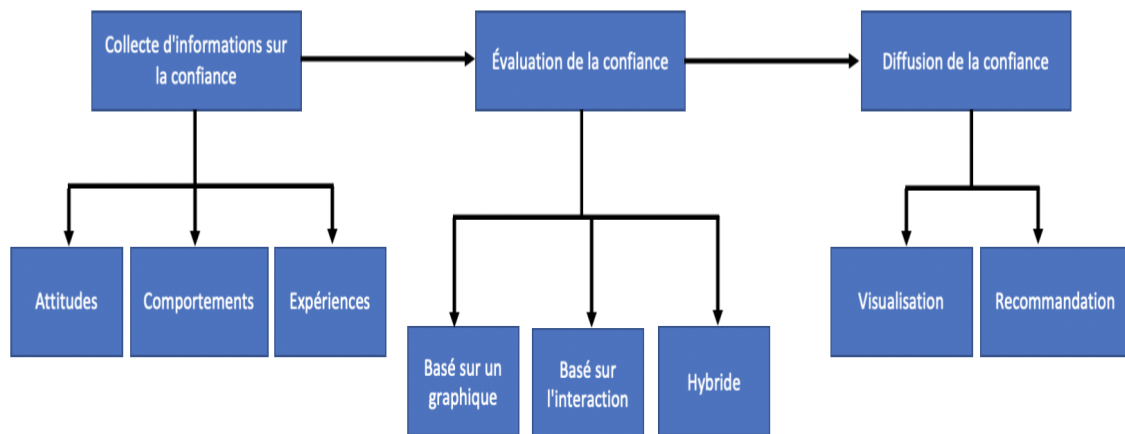


FIGURE 2.2 – Processus de construction d'un système de confiance

sur la confiance en trois sources, à savoir (i) les attitudes, (ii) les comportements et (iii) les expériences ; l'évaluation de la valeur de la confiance selon le modèle de données, à savoir (i) le graphique, (ii) l'interaction et (iii) l'hybride ; et la diffusion de la valeur de la confiance en modèles de recommandation et de visualisation basés sur la confiance.

À partir de cette classification, on constate qu'après la collecte des informations et le calcul des valeurs de confiance, il faut des modèles pour diffuser les résultats obtenus. Il pourrait y avoir de nombreuses façons de diffuser les informations de confiance. La recommandation est une approche pour la diffusion de la valeur de confiance dans un réseau social, la visualisation est une autre approche [SNP13]. Nous les abordons chacune à leur tour.

2.8 Modèles de propagation de la confiance

Il pourrait y avoir plusieurs façons de propager les informations sur la confiance. La recommandation est une approche permettant la propagation des valeurs de confiance au sein d'un réseau social. La visualisation est une autre approche.

2.8.1 Modèles de visualisation

La visualisation des relations de confiance sous la forme d'un graphique est un moyen de propager des informations sur la confiance. Les graphiques montrent la force de la connexion entre deux nœuds, c'est-à-dire les voies de connexion entre deux nœuds : un

nombre plus élevé de connexions signifie une relation plus étroite [SNP13]. De nombreux outils de visualisation de réseaux sociaux sont disponibles sur Internet, tels que SocNetV³ (Social Network Visualization) et Graphviz⁴ (Graph Visualization).

Vigas et Donath [VD04] proposent une approche alternative pour la visualisation des réseaux sociaux représentant la fréquence des connexions dans le temps (appelée PostHistory). Les auteurs observent les connexions des participants en utilisant les en-têtes TO et CC de leurs courriels. L'application dispose d'un calendrier et d'un panneau pour afficher les contacts. Pour chaque point dans le temps (jour dans le calendrier), le panneau des contacts montre les personnes qui sont le plus fréquemment en contact. Contrairement aux visualisations graphiques qui montrent la force des liens entre les membres d'un réseau social, cette visualisation décrit la fréquence des contacts entre les membres. De la même manière, les connexions de confiance ainsi que le degré de confiance entre les membres peuvent être visualisés à l'aide de graphiques. O'Donovan et al. [ODo+07] proposent un modèle qui extrait les informations négatives des commentaires sur eBay, calcule la confiance personnalisée et basée sur les caractéristiques, et présente ces informations sous forme de graphique. Le graphique montre la valeur de la confiance et la force de la confiance calculée sur la base du nombre de transactions/commentaires entre deux utilisateurs. Guerriero et al. [GKH09] proposent une visualisation basée sur la confiance du contexte de coopération entre les membres. Bimrah et al. [BMP08] proposent un langage de visualisation pour l'élicitation des exigences liées à la confiance. Le langage vise à aider à comprendre comment la confiance peut être modélisée et raisonnée lors du développement de systèmes d'information.

Les approches de visualisation de la confiance sont très utiles aux exploitants de réseaux sociaux pour analyser et déterminer le niveau de confiance dans la communauté. Elles les aident à identifier les membres les plus et les moins dignes de confiance. En outre, les responsables peuvent prendre des mesures préventives, comme l'introduction de nouvelles informations intéressantes et pertinentes, si le niveau de confiance dans la communauté descend en dessous d'un certain seuil. La visualisation de la confiance permet au utilisateur de contrôler le réseau social pour encourager les comportements positifs et décourager les comportements perturbateurs [SNP13].

3. <https://socnetv.org/>

4. <https://www.graphviz.org/>

2.8.2 Modèles de recommandation basés sur la confiance

La recommandation basée sur la confiance est un autre moyen de diffuser des informations sur la confiance. Cette technique implique généralement la construction d'un réseau de confiance où les nœuds sont des utilisateurs et les arêtes représentent la confiance qui leur est accordée. L'objectif d'un système de recommandation basé sur la confiance est de générer des recommandations personnalisées en agrégeant les opinions des autres utilisateurs du réseau de confiance. Les techniques de recommandation qui analysent les réseaux de confiance fournissent des résultats très précis et hautement personnalisés [SNP13]. Hang et al. [HS10] utilisent une approche basée sur les graphes pour recommander un nœud dans un réseau social en utilisant la similarité dans les réseaux de confiance. Massa et Aversani [MA07] proposent un système de recommandation basé sur la confiance dans lequel il est possible de rechercher des utilisateurs fiables en exploitant la propagation de la confiance sur le réseau de confiance. Andersen et al. [And+08] explorent une approche axiomatique de la recommandation basée sur la confiance et proposent plusieurs modèles de recommandation, dont certains sont compatibles avec les incitations (c'est-à-dire que les membres malveillants ne peuvent pas inciter d'autres membres à fournir des informations et des liens de confiance faux ou trompeurs, car il est toujours dans l'intérêt du membre de fournir des informations factuelles).

Hess [Hes06] étend les recommandations basées sur la confiance pour des éléments uniques tels que les films à des ressources liées. À cette fin, l'auteur construit un deuxième type de réseau, appelé réseau de référence de documents. Les recommandations pour les documents sont généralement faites par des mesures de visibilité basées sur la référence qui considèrent qu'un document est plus important s'il est souvent référencé par des documents importants. Les réseaux de documents et de confiance, ainsi que des réseaux tels que les réseaux d'organisations, sont intégrés dans un réseau multicouche. Cette architecture permet de combiner des mesures de visibilité classiques avec des recommandations basées sur la confiance, ce qui donne des mesures de visibilité renforcées par la confiance. Les techniques de recommandation basées sur la confiance offrent un moyen de propagation des informations de confiance au sein d'un réseau social ou un système e-commerce. Dans ces systèmes, la première question qu'un utilisateur doit poser c'est « Pourquoi je fais confiance à un vendeur ou un produit sur Amazon ou un avis d'un passager sur Bla-bla-car ? ». Pour cette raison, ces systèmes utilisent des techniques de recommandation

pour fournir aux utilisateurs les vendeurs et les conducteurs les mieux notés. De cette façon, le système garantit la fidélité de ses utilisateurs.

C'est pour cette raison que, dans ce travail de thèse, nous nous sommes d'abord penchés sur le domaine de la recommandation, pour comprendre son fonctionnement, explorer les différentes approches qui l'englobent et comprendre comment on peut l'utiliser dans le cadre de la confiance pour analyser le comportement des utilisateurs.



Chapitre 3

Systemes de recommandation : un aperçu

Sommaire

| | | |
|------------|--|-----------|
| 3.1 | Introduction | 63 |
| 3.2 | Systemes de recommandation classiques | 63 |
| 3.3 | Systemes de recommandation basés sur l'IA | 67 |



3.1 Introduction

Du commerce électronique (suggérer aux acheteurs des articles susceptibles de les intéresser) à la publicité en ligne (suggérer aux utilisateurs les bons contenus, correspondant à leurs préférences), les systèmes de recommandation sont aujourd’hui incontournables dans nos parcours quotidiens en ligne. D’une manière très générale, les systèmes de recommandation sont des algorithmes visant à suggérer des éléments pertinents aux utilisateurs (les éléments pouvant être des films à regarder, des textes à lire, des produits à acheter ou tout autre élément dépendant des domaines d’activités).

Les systèmes de recommandation sont vraiment essentiels dans certains secteurs, car ils peuvent générer des revenus considérables lorsqu’ils sont efficaces ou constituer un moyen de se démarquer considérablement de la concurrence. Comme preuve de l’importance des systèmes de recommandation, nous pouvons mentionner qu’il y a quelques années, Netflix a organisé un défi (le « prix Netflix ») dont l’objectif était de produire un système de recommandation plus performant que son propre algorithme avec un prix d’un million de dollars à gagner.

L’utilisation de données liées à la confiance pour fournir des recommandations est apparue comme une nouvelle façon de faire de meilleures recommandations. Il est difficile pour les utilisateurs d’atteindre l’élément le plus approprié et le plus fiable pour eux parmi un grand nombre d’éléments et de commentaires sur ces éléments. Les systèmes de recommandation et les systèmes de confiance/réputation sont une des solutions pour traiter ce problème à l’aide de services personnalisés. Ces systèmes suggèrent des articles à l’utilisateur en estimant les notes qu’il leur attribuera.

Il existe différentes approches utilisées dans les systèmes de recommandation, celles qui ont émergé avec l’apparition des systèmes traditionnels et celles qui ont été adaptées avec les techniques d’apprentissage automatique et de l’IA.

3.2 Systèmes de recommandation classiques

Les systèmes de recommandation sont définis comme des entrées de recommandation fournies par les personnes, que le système agrège ensuite et dirige vers les destinataires appropriés. On peut également les définir comme des systèmes qui produisent des recommandations individualisées ou qui ont pour effet de guider l’utilisateur de manière

personnalisée vers des objets intéressants dans un espace plus large d'options possibles. Il existe principalement six types de systèmes de recommandation : Les systèmes de recommandation de filtrage collaboratif, les systèmes de recommandation basés sur le contenu, les systèmes de recommandation basés sur la démographie, les systèmes de recommandation basés sur l'utilité, les systèmes de recommandation basés sur la connaissance et les systèmes de recommandation hybrides.

- **Le filtrage collaboratif [Sch+07]** : il s'agit de la technologie la plus recherchée, la plus largement mise en œuvre et la plus mature qui soit disponible sur le marché. Les systèmes de recommandation collaborative regroupent les évaluations ou les recommandations d'objets, reconnaissent les points communs entre les utilisateurs sur la base de leurs évaluations, et génèrent de nouvelles recommandations sur la base de comparaisons entre utilisateurs. La plus grande force des techniques collaboratives est qu'elles sont complètement indépendantes de toute représentation lisible par une machine des objets recommandés et qu'elles fonctionnent bien pour les objets complexes où les variations de goût sont responsables d'une grande partie de la variation des préférences. Le filtrage collaboratif repose sur l'hypothèse que les personnes qui étaient d'accord dans le passé le seront aussi dans le futur et qu'elles aimeront le même type d'objets que dans le passé.

Le filtrage collaboratif est l'une des principales technologies qui alimenteront le web adaptatif. La personnalisation basée sur le contenu peut s'avérer efficace dans des circonstances limitées, mais dans l'ensemble, il faudra probablement des décennies ou plus avant que la technologie matérielle et logicielle puisse commencer à reconnaître automatiquement les subtilités de l'information qui sont importantes pour les gens, en particulier les aspects du goût esthétique [Sch+07].

Les systèmes de recommandation peuvent briser la confiance lorsque des utilisateurs malveillants donnent des évaluations qui ne sont pas représentatives de leurs véritables préférences. Qu'advient-il d'un système de filtrage collaboratif si un ou plusieurs utilisateurs décident d'attaquer un article en abaissant délibérément leur(s) évaluation(s) de cet article ? Que se passe-t-il si une entreprise bombarde un système de recommandation avec des évaluations exagérées de ses propres produits ? Il y a eu de nombreux exemples de ces attaques de « shilling ». O'Mahoney et al [OMa+04] ont montré que les utilisateurs pouvaient, en fait, augmenter et diminuer artificiel-

lement les notes de prédiction.

- **Systèmes de recommandation basé sur le contenu [PB07]** : ce type de systèmes est principalement classé comme une excroissance et une continuation de la recherche sur le filtrage de l'information. Dans ce système, les objets sont principalement définis par leurs caractéristiques associées. Un système de recommandation basé sur le contenu apprend un profil des intérêts du nouvel utilisateur sur la base des caractéristiques présentes dans les objets que l'utilisateur a évalués. Il s'agit essentiellement d'un système de recommandation spécifique par mots-clés, dans lequel les mots-clés sont utilisés pour décrire les éléments. Ainsi, dans un système de recommandation basé sur le contenu, les algorithmes utilisés sont tels qu'ils recommandent aux utilisateurs des éléments similaires à ceux que l'utilisateur a aimés dans le passé ou qu'il examine actuellement.

Les systèmes basés sur le contenu sont conçus pour exploiter des scénarios dans lesquels les éléments peuvent être décrits avec des ensembles descriptifs d'attributs. Dans de tels cas, les évaluations et les actions d'un utilisateur sur d'autres produits sont suffisantes pour découvrir des recommandations significatives. Cette approche est particulièrement utile lorsque l'élément est nouveau et qu'il y a peu d'évaluations disponibles pour cet élément [Agg16].

- **Systèmes de recommandation basés sur l'utilité [Hua08]** : le système de recommandation basé sur l'utilité fait des suggestions basées sur le calcul de l'utilité de chaque objet pour l'utilisateur. Bien entendu, le problème central de ce type de système est de savoir comment créer une utilité pour chaque utilisateur. Dans un système basé sur l'utilité, chaque industrie aura une technique différente pour arriver à une fonction d'utilité spécifique à l'utilisateur et l'appliquer aux objets considérés. Le principal avantage d'un système de recommandation basé sur l'utilité est qu'il peut prendre en compte des attributs autres que le produit, tels que la fiabilité du fournisseur et la disponibilité du produit, dans le calcul de l'utilité. Cela permet de vérifier l'inventaire en temps réel de l'objet et de l'afficher à l'utilisateur. Dans ce type de systèmes de recommandation, le système a besoin des avis des autres utilisateurs pour avoir une idée sur la fiabilité du fournisseur. Ainsi, cette fiabilité est obtenue en se basant sur le degré de confiance des autres utilisateurs au fournisseur cible.

-
- **Systèmes de recommandation basés sur la connaissance [Bur00]** : ce type de système de recommandation tente de suggérer des objets en se basant sur des déductions concernant les besoins et les préférences d'un utilisateur. La recommandation basée sur la connaissance fonctionne sur la base de la connaissance fonctionnelle : le système a des connaissances sur la façon dont un article particulier répond à un besoin particulier de l'utilisateur, et peut donc raisonner sur la relation entre un besoin et une recommandation possible. Pour pouvoir des connaissances sur un article, le système peut analyser les évaluations des autres utilisateurs. À partir de ces évaluations, le système peut comprendre si l'article répond à certain besoin ou non, pour le recommander à l'utilisateur cible. De cette façon, si l'utilisateur est satisfait de la recommandation qui lui a été fournie, il fait donc confiance aux évaluations des autres membres du système.
 - **Systèmes de recommandation hybrides [Bur02]** : la combinaison de deux systèmes d'une manière qui convient à un secteur particulier est connue sous le nom de système de recommandation hybride. C'est le système de recommandation le plus recherché par de nombreuses entreprises, car il combine les forces de plus de deux systèmes de recommandation et élimine également toute faiblesse qui existe lorsqu'un seul système de recommandation est utilisé. Dans ce type de systèmes, les algorithmes utilisés combinent toujours les avis des utilisateurs avec d'autres techniques. Les utilisateurs font confiance à ces recommandations parce qu'ils ont les mêmes intérêts. Il existe plusieurs façons de combiner les systèmes, par exemple :
 - **Recommandeur hybride pondéré** : dans ce système, le score d'un élément recommandé est calculé à partir des résultats de toutes les techniques de recommandation disponibles dans le système. Par exemple, le système P-Tango [Cla+99] combine les systèmes de recommandation collaboratifs et ceux basés sur le contenu en leur donnant un poids égal au départ, mais en ajustant progressivement la pondération au fur et à mesure que les prédictions sur les évaluations des utilisateurs sont confirmées ou non. La combinaison hybride de Pazzani [Paz99] n'utilise pas de scores numériques mais traite plutôt la sortie de chaque recommandeur comme un ensemble de votes, qui sont ensuite combinés dans un schéma de consensus.
 - **Switching Hybrid Recommender** : ce système permet de passer d'une tech-

nique de recommandation à une autre en fonction de critères particuliers. Supposons que nous combinions les systèmes de recommandation basés sur le contenu et sur la collaboration, le système de recommandation hybride de commutation peut d'abord déployer le système de recommandation basé sur le contenu et s'il ne fonctionne pas, il déploiera le système de recommandation basé sur la collaboration.

- **Recommandeur hybride mixte** : lorsqu'il est possible de faire un grand nombre de recommandations simultanément, nous devrions opter pour des systèmes de recommandation mixtes. Ici, les recommandations de plus d'une technique sont présentées ensemble, de sorte que l'utilisateur peut choisir parmi un large éventail de recommandations. Le système PTV, principalement un programme de recommandation pour suggérer aux clients de regarder la télévision, développé par Smyth et Cotter [CS00] est utilisé par la majorité des entreprises de médias et de divertissement.

Les systèmes de recommandation fournissent un service d'assistance personnalisé aux utilisateurs en apprenant leurs comportements antérieurs et en prédisant leurs préférences actuelles pour des produits particuliers. L'Intelligence Artificielle (IA), en particulier l'intelligence computationnelle et les méthodes et algorithmes d'apprentissage automatique, a été naturellement appliquée au développement des systèmes de recommandation pour améliorer la précision des prédictions et résoudre les problèmes de rareté des données et de démarrage à froid.

3.3 Systèmes de recommandation basés sur l'IA

Comme c'est le cas pour les systèmes de recommandation mentionnés précédemment, un système de recommandation basé sur l'IA est une classe d'algorithmes d'apprentissage automatique utilisés par les développeurs pour prédire les choix des utilisateurs et leur proposer des suggestions pertinentes. Grâce à l'utilisation de la science des données et des données des utilisateurs, les systèmes de recommandation en IA filtrent et recommandent les articles les plus appropriés à un utilisateur spécifique. On dit que le système de recommandation de contenu ressemble à un vendeur expérimenté qui connaît les besoins, les préférences et les exigences de l'utilisateur et peut recommander des produits plus

attractifs, tout en augmentant le taux de conversion.

Le rôle et la popularité de l'IA sont évidents dans la nouvelle ère numérique. En particulier avec l'utilisation de l'IA, les recommandations rapides sont plus répandues, ce qui est efficace en termes de temps et pragmatique. Elles aident le client à comprendre ce dont il a besoin pour prendre une décision d'achat plus rapidement. En conséquence, leur fidélité augmente et, avec une forte probabilité, ils reviendront dans le magasin pour de nouveaux achats.

Diverses techniques d'IA ont été appliquées plus récemment aux systèmes de recommandation, contribuant à améliorer l'expérience des utilisateurs et à accroître leur satisfaction. L'IA permet d'obtenir une qualité de recommandation supérieure à celle que les méthodes de recommandation classiques peuvent atteindre et de répondre aux exigences accrues en matière de recommandation liées à l'explosion des données. Cela a ouvert une nouvelle ère pour les systèmes de recommandation, en permettant de mieux comprendre les relations entre les utilisateurs et les articles, en présentant des représentations de données plus complexes et en découvrant des connaissances complètes dans les données démographiques, textuelles, virtuelles et contextuelles [ZLJ21].

- **Réseaux neuronaux profonds dans les systèmes de recommandation** : les réseaux neuronaux sont rarement utilisés dans les systèmes de recommandation car la tâche de recommandation concerne le classement des éléments plutôt que la classification. Dans leurs premiers travaux, Salakhutdinov et al. ont proposé une machine de Boltzmann restreinte (RBM) à deux couches pour explorer la propriété ordinale des évaluations. Cette méthode a attiré l'attention lors de la compétition du prix Netflix 2009 [SMH07], mais il y a eu peu de travaux de suivi, à l'exception des recherches de Truyen et al. [TPV12] qui ont étendu ces travaux en étudiant les options de paramétrage de la RBM dans la recommandation. En revanche, l'apprentissage profond a connu un grand succès dans les domaines du traitement du langage naturel, de la reconnaissance vocale et de la vision par ordinateur [LBH15]. Avec la disponibilité d'un plus grand nombre de données (par exemple, les commentaires générés par les utilisateurs ou les photos visuelles des articles), la nécessité d'intégrer toutes les informations et de fournir des recommandations pour les articles multimédias, tels que les images ou les vidéos, a incité le développement de systèmes de recommandation basés sur l'apprentissage profond [Zha+19].

-
- **Apprentissage par transfert dans les systèmes de recommandation** : ce type d'apprentissage a connu un grand succès et un avenir prometteur dans le domaine de l'apprentissage automatique. Dans le domaine des systèmes de recommandation, l'apprentissage par transfert étend les demandes de recommandation d'un seul domaine à plusieurs domaines. En exploitant la corrélation de plusieurs domaines, tous les domaines peuvent bénéficier de l'exploration des préférences des utilisateurs qui ne peuvent être trouvées avec les données d'un seul domaine. Par exemple, un utilisateur actif dans un domaine cinématographique est susceptible de s'intéresser aux livres et à la musique liés aux films qu'il aime. Une autre raison d'exploiter plusieurs domaines est de résoudre le problème de la rareté des données ou du démarrage à froid, car il peut y avoir des données insuffisantes dans un domaine mais des données relativement riches dans un autre domaine. Par exemple, un utilisateur peut avoir peu d'enregistrements dans une catégorie de livres dans un système d'évaluation et de notation en ligne, mais peut avoir un grand nombre d'évaluations de films, ainsi une abondance de données dans un domaine secondaire peut aider la recommandation dans le domaine cible. Cette demande d'une recommandation riche et diversifiée, ainsi que la capacité à atténuer le problème de la manque des données, ont conduit au développement de systèmes de recommandation inter-domaines (cross-domain recommender systems (CDRS)).

La plus grande différence entre la CDRS et les autres méthodes d'apprentissage par transfert est qu'il n'y a pas d'espace caractéristique explicite dans la CDRS. Cela signifie que les CDRS ne peuvent pas être classées comme un seul type de méthode d'apprentissage par transfert, car elles impliquent l'application pratique de plusieurs techniques d'apprentissage par transfert. D'un point de vue pratique, les CDRS fournissent une recommandation multi-domaine pour les détaillants d'achats en ligne qui vendent une variété de produits, tout en offrant une solution au problème de la manque des données. Certaines méthodes relient deux domaines par le biais d'informations auxiliaires autres que les données de préférence [SLH14], tandis que les CDRS basés sur les données de préférence peuvent être conçus stratégiquement en fonction du chevauchement des utilisateurs et des articles, de la forme que prennent les données ou des tâches que le système doit traiter [Can+15].

- **Apprentissage par renforcement dans les systèmes de recommandation** : la nature

de l'utilisation d'un système de recommandation est un processus interactif entre l'utilisateur et le système avec une série d'états et d'actions, ce qui est conforme à l'apprentissage par renforcement. Contrairement aux systèmes de recommandation traditionnels, qui se concentrent généralement sur la prédiction des intérêts des utilisateurs à un moment précis, les systèmes de recommandation basés sur l'apprentissage par renforcement visent à maximiser l'engagement et la satisfaction des utilisateurs sur le long terme. Dans le cadre de l'apprentissage par renforcement, le système de recommandation est traité comme un agent d'apprentissage, les comportements des utilisateurs correspondent aux états et les actions sont des recommandations générées par le système. La récompense est le retour d'information des utilisateurs sur les résultats de la recommandation, comme le taux de clics ou le temps passé sur la page web. L'objectif est de trouver une politique ou une fonction de valeur pour les utilisateurs afin de maximiser les récompenses à long terme. Le défi de l'apprentissage par renforcement réside dans le grand nombre d'éléments disponibles pour les utilisateurs, ce qui crée un grand espace d'action pour les agents d'apprentissage et augmente la complexité du système.

Les premiers travaux étudient principalement l'équilibre entre l'exploration et l'exploitation, qui est également connu sous le nom de problèmes de bandit [BF85]. Une implémentation directe du MDP aux systèmes de recommandation sans tenir compte de l'équilibre est proposée dans [Sha+05] pour recommander le prochain article avec les k articles consommés précédemment. Plus tard, le compromis entre l'exploration et l'exploitation est abordé avec l'apprentissage par renforcement linéaire avec une garantie théorique [WLM18]. Il existe également des travaux qui traitent le processus interactif entre l'utilisateur et le système de recommandation comme un problème de bandit à bras multiples [145], puis l'étendent avec des informations contextuelles [Zen+16].

Pornthep Rojanavas, et al [RSP05] se sont attaqués au problème des systèmes de recommandation traditionnels où les utilisateurs étaient confrontés aux mêmes éléments similaires dans chaque recommandation. Ces recommandations dépendaient donc des choix passés de l'utilisateur. Par conséquent, l'utilisateur peut ne jamais découvrir de nouveaux éléments qu'il pourrait aimer. Les auteurs ont utilisé un nouveau système de recommandation sur le Web dans lequel ils ont combiné

une politique de type ϵ -greedy avec une méthode de prédiction SARSA. Le système se composait de deux parties : (1) Un modèle global permettant à tous les utilisateurs de découvrir les fonctionnalités du système ; (2) Le modèle local permettant de conserver les journaux de l'historique de navigation de chaque utilisateur. Deux conclusions ont été tirées de cette étude. La première était que la politique ϵ -greedy aidait à explorer de nouveaux éléments tout en exploitant la tendance du système. La seconde était que si un utilisateur explorait trop un type d'article particulier, la probabilité de lui recommander de nouveaux articles diminuait.

- **Techniques floues dans les systèmes de recommandation** : les caractéristiques des éléments et les comportements des utilisateurs dans les systèmes de recommandation du monde réel sont généralement subjectifs, incomplets et vagues. La théorie des ensembles flous, notamment le concept des relations floues, offre un moyen approprié de traiter les problèmes d'incertitude de l'information, et peuvent également être adoptées dans les systèmes de recommandation [HR07].

Prenons l'exemple des systèmes de recommandation basés sur le contenu, les techniques floues sont appliquées à deux phases du processus : le profilage et la mise en correspondance des éléments appropriés. Les ensembles flous sont utilisés pour exprimer l'incertitude des caractéristiques des articles, en particulier les descriptions vagues et incomplètes, ainsi que les commentaires subjectifs des utilisateurs sur ces articles. Les approches de recommandation sont aussi développées, au moyen des ensembles flous pour découvrir les préférences des utilisateurs et créer des représentations d'articles [Yag03 ; ZZN10]. Étant donné que les informations sur les produits se présentent souvent sous la forme d'informations de contenu structurées en arbre et que les préférences des utilisateurs sont vagues et floues, un certain nombre de systèmes de recommandation basés sur des arbres flous ont été développés pour le commerce électronique [Mao+15], les services électroniques interentreprises et les systèmes d'apprentissage en ligne [WZL14].



Deuxième partie

Contributions

Chapitre 4

Un modèle basé sur l'apprentissage hybride pour la recommandation

Sommaire

| | | |
|------------|---|-----------|
| 4.1 | Introduction | 76 |
| 4.2 | Analyse de l'état de l'art par rapport aux besoins métiers | 78 |
| 4.2.1 | Les besoins métiers | 78 |
| 4.2.2 | Analyse de l'état de l'art | 80 |
| 4.2.2.1 | Approches basées sur le contenu | 81 |
| 4.2.2.2 | Filtrage collaboratif | 81 |
| 4.2.2.3 | Processus de Décision Markovien | 81 |
| 4.2.2.4 | Clustering | 83 |
| 4.2.3 | Synthèse | 84 |
| 4.3 | Notre approche hybride pour la recommandation | 85 |
| 4.3.1 | Recommandation basée sur un Processus de Décision Markovien (PDM) | 85 |
| 4.3.2 | Principe du Clustering Hiérarchique | 86 |
| 4.3.3 | Fusion des deux techniques | 87 |
| 4.3.3.1 | Construction des Clusters | 89 |
| 4.3.3.2 | Apprentissage de la fonction Q | 89 |
| 4.3.3.3 | Génération des recommandations | 89 |
| 4.3.4 | Synthèse | 90 |
| 4.4 | Évaluation expérimentale | 91 |

| | | |
|------------|------------------------------------|-----------|
| 4.4.1 | Base de données utilisée | 91 |
| 4.4.2 | Résultats | 92 |
| 4.5 | Conclusion | 94 |

4.1 Introduction

Dans le chapitre précédent, nous avons présenté les différentes techniques des systèmes de recommandation. Trois approches sont principalement utilisées dans les systèmes de recommandation, celles basées sur le contenu, celles basées sur le filtrage collaboratif, et enfin les approches hybrides, qui fusionnent différents algorithmes et fournissent des recommandations plus précises et plus efficaces qu'un seul algorithme, car les inconvénients d'une technique simple peuvent être surmontés par une autre technique. Les systèmes de recommandation sont une forme spécifique de filtrage de l'information permettant de présenter des éléments d'information susceptibles d'intéresser l'utilisateur. Dans ce contexte, l'élément peut être un livre, un film, un article à acheter, un lieu à rechercher, etc. Pour être en mesure de fournir ces recommandations, le système doit disposer des informations nécessaires sur les utilisateurs pour établir des profils d'utilisateurs et connaître les préférences de chacun. Ces informations sont collectées à partir des traces laissées par les utilisateurs lors de leur navigation. Il existe deux types de traces, les traces explicites et les traces implicites. Les traces explicites sont celles fournies volontairement par l'utilisateur. À l'opposé, les traces implicites sont celles collectées en traçant les actions spontanées des utilisateurs lors de la navigation.

Comme nous venons de le voir la plupart des approches de recommandation se basent sur des données, que ce soit des traces ou préférences, centrées sur les utilisateurs. Ceci est à l'encontre de deux des principes de l'entreprise O°CCode qui sont « l'anonymat » et « l'échange en toute confiance ». L'entreprise O°CCode se base souvent sur le principe « Sans confiance pas d'échange ! », et les sources de rupture de cette confiance sont nombreuses : usurpation d'identité, fraudes diverses, piratage, exploitation abusive des données personnelles, etc.

Les systèmes de recommandation peuvent être classés en deux grandes catégories : les systèmes traditionnels et les systèmes à base d'intelligence artificielle (IA).

Les systèmes ci-dessus souffrent néanmoins de plusieurs problèmes.

-
- **Difficulté de gestion des profils atypiques** : un utilisateur peut avoir des goûts particuliers et des préférences très inhabituelles et ne rassemble à aucun autre utilisateur du système.
 - **Difficulté de la gestion de la dynamique des profils utilisateurs** : les systèmes de recommandation reposent sur le principe selon lequel un utilisateur ayant manifesté un comportement donné auparavant aura tendance à répéter ce même comportement. Cependant, ce principe n'est pas nécessairement vrai dans le monde réel. Par exemple, un utilisateur peut changer complètement d'intérêts ou en avoir plusieurs.
 - **Manque de diversité des recommandations** : les systèmes de recommandation ont tendance à enfermer les utilisateurs dans leur propre chambre d'écho [Ngu20], car seuls les articles similaires aux articles déjà aimés sont recommandés. Par conséquent, ce manque de diversité et de nouveauté dans les recommandations fait que certains utilisateurs sont frustrés par ces recommandations monotones et cessent d'utiliser ces systèmes.
 - **Manque d'équité dans les recommandations** : les systèmes de recommandation ont souvent tendance à recommander des articles qui sont déjà populaires. En d'autres termes, ces systèmes donnent plus de visibilité aux articles qui sont déjà visibles et négligent ceux qui ne le sont pas ou le sont moins et qui peuvent être intéressants.
 - **Manque d'explication des recommandations** : les systèmes de recommandation fonctionnent comme des boîtes noires et l'utilisateur est souvent incapable de comprendre pourquoi une recommandation lui a été présentée.
 - Enfin, tous ces systèmes, pour fonctionner, collectent **des quantités massives de données** à caractère personnel dont les dérives sont difficiles à contenir : atteinte à la vie privée, discrimination, cyberattaques, etc.

C'est pour ces raisons que les systèmes de recommandations actuels sont insuffisants pour répondre aux besoins de O°Code. Cette contribution a été publiée dans l'article [Sel+20] qui a été présenté à la conférence ACM Recommender Systems (RecSys) qui est le premier forum international pour la présentation de nouveaux résultats de recherche, de systèmes et de techniques dans le vaste domaine des systèmes de recommandation.

Dans ce chapitre, nous commençons par identifier et justifier les besoins métiers de l'entreprise O°code. Nous montrons ensuite que ces besoins métiers ne sont pas satisfaits par les principales approches de recommandations actuelles. Nous proposons donc une

approche hybride qui combine différentes approches de recommandation actuelles et des techniques d'intelligence artificielle. Au travers d'une expérimentation, nous montrons l'intérêt de notre proposition sur un cas d'étude d'intérêt pour l'entreprise O°Code.

Le reste du chapitre est composé comme suit : la section 4.2 décrit brièvement une analyse de l'état de l'art qui contextualise notre travail, les besoins de l'entreprise en terme de recommandation ainsi qu'une synthèse de cette analyse . La section 4.3 aborde les différentes étapes de notre approche afin de proposer une technique de recommandation qui réponde au mieux à nos besoins. Pour valider notre proposition, nous fournissons dans la section 4.4 une étude expérimentale, couvrant tous les aspects de la contribution. Enfin, les points à retenir et les perspectives sont présentés dans la section 4.5.

4.2 Analyse de l'état de l'art par rapport aux besoins métiers

Dans cette section, nous définissons des besoins de l'entreprise O°Code ainsi que les critères que devrait remplir un système de recommandation pour satisfaire ces besoins. Une analyse de l'état de l'art sera présentée afin de montrer quels critères sont remplis ou non. Enfin, nous concluons cette section par une synthèse.

4.2.1 Les besoins métiers

Dans tous ces projets, O°Code est initialement basé sur l'anonymat et la confiance.

Premier Besoin

Un système de recommandation répondant aux besoins de l'entreprise O°Code ne doit pas être basé sur des données personnelles des utilisateurs.

La société O°Code souhaite mettre en relation des individus tout en respectant deux principes fondamentaux.

- **L'anonymat** : pour O°Code, l'anonymat consiste à respecter la vie privée des utilisateurs, c'est-à-dire à ne pas collecter les informations liées à leur identité : nom, prénom, numéro de téléphone, e-mail, etc.

-
- **La confiance** : la mission d'O°Code est de rendre le monde numérique plus sûr et de lui donner une valeur tangible dans le monde physique, afin de garantir la confiance dans tous les échanges. Plus précisément, chez O°Code, un individu doit démontrer sa fiabilité en fonction de son comportement dans un système et non de son identité.

En effet, pour considérer ces deux principes, il faut étudier les systèmes de recommandation qui se basent principalement sur les caractéristiques du contenu vu ou apprécié par l'utilisateur sans utiliser ses données pour garantir à la fois le respect des données personnelles et la confiance des utilisateurs dans les recommandations du système. Le problème qui se pose ici est celui du démarrage à froid. Un bon système de recommandation doit être capable de découvrir les préférences d'un nouvel utilisateur sans avoir besoin de révéler son identité.

Deuxième Besoin

Un système de recommandation répondant aux besoins de l'entreprise O°Code doit fournir une diversité de recommandations et doit évoluer avec les goûts des utilisateurs.

Dans la plupart des systèmes de recommandation, des articles similaires à des articles déjà appréciés sont souvent recommandés. Cela conduit à un manque de diversité et de nouveauté dans les recommandations. Par conséquent, certains utilisateurs sont frustrés par ces recommandations monotones et cessent d'utiliser ces systèmes. D'autre part, les systèmes de recommandation sont basés sur le principe qu'un utilisateur qui a déjà eu un certain comportement auparavant aura tendance à répéter ce même comportement. Cependant, ce principe n'est pas nécessairement vrai dans le monde réel ; un utilisateur peut changer complètement ses intérêts ou avoir plusieurs intérêts. Pour y répondre, il faut une technique de recommandation qui essaie souvent de parcourir de nouveaux contenus pour satisfaire toutes les préférences des utilisateurs, de découvrir de nouveaux contenus et de s'adapter à la dynamique des profils des utilisateurs.

Troisième Besoin

Un système de recommandation répondant aux besoins de l'entreprise O°Code doit pouvoir fournir des explications sur les recommandations faites.

Les systèmes de recommandation fonctionnent comme des boîtes noires et l'utilisateur est souvent incapable de comprendre pourquoi une recommandation lui a été proposée. Ceci est contre les principes d'O°Code ; un utilisateur ne peut pas faire confiance à des résultats sans explications. Pour cette raison, nous devons étudier un système de recommandation comme une boîte transparente pour contribuer à cette confiance des utilisateurs envers le système et avoir des résultats compréhensibles.

4.2.2 Analyse de l'état de l'art

Le système de recommandation est constitué d'un ensemble d'utilisateurs, d'un ensemble d'articles, et d'une base d'informations (notes, annotations, etc) selon les besoins de l'approche.

Cet ensemble d'entrées est utilisé par l'approche pour prédire l'appréciation d'un article par un utilisateur. Pour cela, le système utilise une fonction pour calculer l'évaluation que l'utilisateur attribuerait à chaque article.

Ce qui change d'une approche à l'autre est la fonction d'évaluation/prédiction utilisée ainsi que les données à l'origine de cette évaluation.

Passons maintenant à l'explication des principales approches des systèmes de recommandation (Figure 4.1) qui sont généralement classées en trois catégories : les systèmes basés sur le contenu, les systèmes basés sur les utilisateurs et les systèmes hybrides.

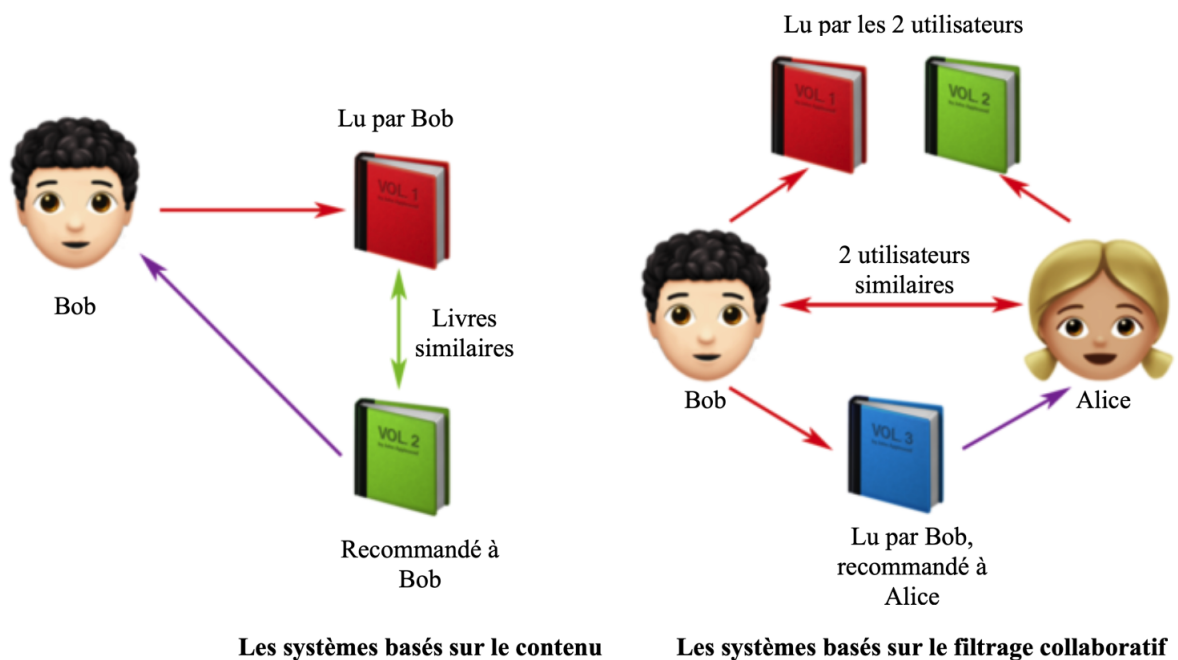


FIGURE 4.1 – Les approches de recommandation

4.2.2.1 Approches basées sur le contenu

Le principe consiste à estimer la similarité entre les caractéristiques ou le contenu des nouveaux articles et des articles déjà vus par l'utilisateur. Les articles avec une similarité élevée sont recommandés à l'utilisateur. Ce type d'approche peut répondre au premier besoin de l'entreprise puisqu'il n'utilise en aucun cas les données des utilisateurs. Cependant, cela ne répond pas au deuxième besoin, car les articles similaires sont toujours recommandés, et l'utilisateur ne découvrira donc pas de nouvelles préférences.

4.2.2.2 Filtrage collaboratif

Le principe consiste à estimer la ressemblance entre les utilisateurs du système et ainsi recommander à un utilisateur cible les articles appréciés par les autres ayant des caractéristiques similaires. Cette approche ne répond pas au premier besoin. En effet, afin d'estimer la similarité entre les utilisateurs, le système doit enregistrer certaines données les concernant, qu'il s'agisse de traces de navigation ou de données personnelles. Il existe encore des systèmes hybrides qui exploitent les avantages des deux approches précédentes en les combinant.

Il existe également d'autres types d'approches dans ce domaine. L'une des plus populaires est l'adaptation d'un processus de décision de Markov (PDM).

4.2.2.3 Processus de Décision Markovien

Dans cette approche, un agent apprend un comportement optimal dans un environnement donné par le biais de récompenses et de punitions (voir Figure 4.2). L'agent doit apprendre l'action optimale à entreprendre, étant donné l'état dans lequel il se trouve. Lorsque ce processus est répété plusieurs fois, le problème est appelé **Processus de Décision Markovien**.

- **PDM** : c'est un cadre qui aide à décider sur un ensemble d'actions pour maximiser les récompenses, étant donné que l'état actuel est dans un environnement stochastique. Il fonctionne sur l'hypothèse que la propriété de Markov est satisfaite, ce qui signifie que l'effet d'une action particulière dans un état spécifique dépend uniquement de cet état et des états futurs et non des états précédents.
- **PDM Model** :
 - S : Ensemble d'états.

A : Ensemble des actions possibles.

$R(S,A)$: Fonction de récompense ; donne une récompense pour un état et une action donnés.

T : Fonction de transition ; qui indique l'effet de l'action sur l'état.

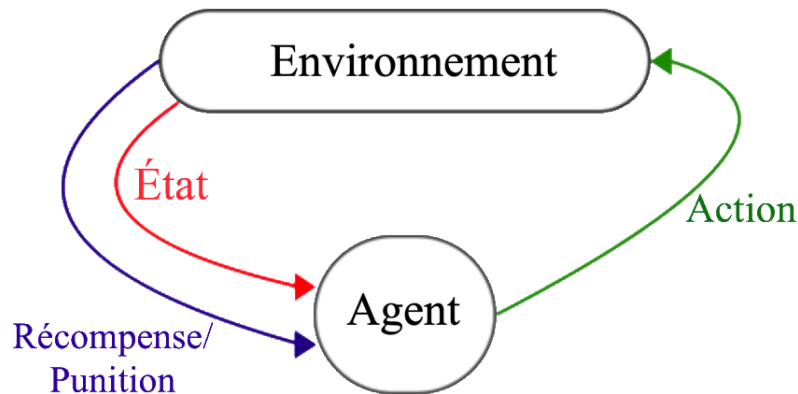


FIGURE 4.2 – Le Processus de Décision Markovien

La technique utilisée pour traiter ce type de problème est l'apprentissage par renforcement, qui a trouvé son application dans les systèmes de recommandation.

Dans un système de recommandation, il est important de présenter aux utilisateurs ce qui pourrait les intéresser le plus. La recommandation peut être formulée comme un processus de décision Markovien : le contenu est l'état, l'action est le meilleur contenu à recommander et la récompense est la satisfaction ou l'insatisfaction de l'utilisateur ou son avis. Pour satisfaire la propriété de Markov, le système doit suggérer une nouvelle recommandation à un utilisateur qui soit indépendante des recommandations précédentes. Ce principe de fonctionnement fournit un autre avantage de l'apprentissage par renforcement, à savoir la prise en compte d'un équilibre adéquat entre exploration et exploitation. D'une part, l'algorithme recommande des contenus susceptibles d'intéresser l'utilisateur en fonction de ses préférences, et d'autre part, il suggère également des recommandations aléatoires, et l'utilisateur peut donc aussi découvrir de nouveaux centres d'intérêt.

Cela répond au deuxième besoin et permet à l'utilisateur de découvrir de nouveaux contenus qui ne sont pas nécessairement similaires à ceux qu'il a déjà appréciés.

Dans la littérature, plusieurs travaux ont été effectués pour étudier les systèmes de recommandation utilisant des Processus de Décision Markovien. Guy Shani, et al [Sha+05] ont traité du principal problème de certains systèmes classiques, à savoir leur nature sta-

tique. Ils ont interprété que ces systèmes utilisaient un aspect statique pour leur procédure de recommandation et l'ont ensuite considéré comme un problème de prédiction. Ils ont proposé que les approches basées sur les MDP disposent d'un modèle initial solide, et entraînent moins de complexité spatiale et temporelle. Pour initialiser leur modèle MDP, ils se sont basés sur un modèle prédictif. Dans un premier temps, ils ont initialisé la fonction de transition. Et dans un second temps, ils sont passés à la génération de recommandations en partant du principe que toutes les recommandations sont indépendantes les unes des autres.

Nima Taghipour, et al [LSS14] ont travaillé sur un système de recommandation musicale utilisant l'apprentissage par renforcement. Ils ont discuté du fait que presque tous les systèmes de recommandation musicale ont un problème : ils recommandent des chansons individuelles à l'utilisateur plutôt qu'une séquence de chansons recommandées. Ils ont donc travaillé à la création d'un nouveau système de recommandation musicale qui non seulement recommande des chansons individuelles aux utilisateurs, mais propose également des séquences de chansons ou des listes de lecture pour les chansons et les transitions de chansons.

Xiangyu Zhao, et al [Zha+17] ont travaillé sur la façon dont les recommandations de listes peuvent être rendues dynamiques par nature. Pour mener à bien cette tâche, ils ont conçu un simulateur d'environnement d'interaction utilisateur-agent en ligne pour pré-entraîner les paramètres et effectuer l'évaluation de ces paramètres avant de les appliquer à un système de recommandation. Le modèle utilisé dans leur mise en œuvre est le LIRD (List-wise Recommendation framework based on deep reinforcement learning).

Ces méthodes ont un problème majeur ; puisque l'espace à parcourir est presque infini, le temps pour avoir un modèle robuste est non négligeable.

4.2.2.4 Clustering

Dans les systèmes de recommandation, les mesures basées sur la similarité ont traditionnellement été utilisées pour déterminer les utilisateurs voisins d'un utilisateur cible. Dans les systèmes de recommandation en temps réel, tous les utilisateurs ne peuvent pas évaluer, s'intéresser ou se familiariser avec tous les éléments disponibles. Lorsqu'il y a une relation ou une interaction entre un utilisateur et un article, la matrice d'évaluation utilisateur-article sera éparse. Ce problème critique affecte la précision des prédictions

de notation par le moteur de recommandation et est connu sous le nom de problème de sparsité. Compte tenu du besoin croissant de résoudre le problème de la rareté, mais de l'incapacité à le faire, les modèles basés sur la similarité sont inadéquats pour définir une liste efficace d'utilisateurs ou d'articles similaires. En parallèle, les mesures de similarité sont complexes sur le plan informatique, et leur utilisation à mesure que l'échelle des données augmente entraînera une augmentation exponentielle de la complexité. Pour résoudre ces problèmes, des techniques de clustering peuvent être utilisées pour séparer les utilisateurs et les articles en différents clusters. Ainsi, lorsqu'un utilisateur cible est similaire à un groupe d'utilisateurs, il est ajouté à ce groupe et les éléments qui intéressent les utilisateurs de ce groupe particulier sont recommandés à l'utilisateur cible. De même pour les articles, ceux qui sont similaires et ont les mêmes caractéristiques sont regroupés dans le même cluster. Lorsqu'un utilisateur est intéressé par un article de ce cluster, le système va lui recommander les autres articles du même cluster.

4.2.3 Synthèse

| | Premier Besoin | Deuxième Besoin | Troisième Besoin |
|--|----------------|-----------------|------------------|
| La recommandation basée sur le contenu | ✓ | × | × |
| Le filtrage collaboratif | × | ✓ | × |
| PDM | ✓ | ✓ | × |
| Le clustering | | | ✓ |

TABLEAU 4.1 – Synthèse de l'état de l'art

Le tableau 4.1 récapitule notre analyse. D'après la définition des systèmes de recommandation basés sur le contenu, nous pouvons voir qu'ils traitent principalement les caractéristiques des articles sans utiliser les données de l'utilisateur. Cela répond à notre premier besoin. En revanche, ce type de recommandation ne permet pas la découverte de nouvelles préférences, car il calcule souvent la similarité entre les autres articles et les articles vus précédemment. Cela ne répond pas à notre deuxième besoin. Et enfin, pour trouver des articles similaires aux goûts de l'utilisateur, cette approche parcourt toutes les données existantes en appliquant à chaque fois la méthode de calcul de similarité. Ainsi, notre troisième besoin n'est pas non plus satisfait.

Pour les systèmes basés sur le filtrage collaboratif, ils estiment la similarité entre les utilisateurs, ce qui ne répond pas à notre critère de respect de la vie privée des utilisateurs. En contrepartie, cette technique peut aider un utilisateur à découvrir de nouveaux contenus parcourus ou aimés par d'autres utilisateurs du système qui lui ressemblent davantage. Ainsi, notre deuxième critère est satisfait. Enfin, et comme la plupart des systèmes de recommandation, ils parcourent les différentes bases d'utilisateurs et de contenus qui les ont aimés, ce qui augmente l'espace de recherche et ne permet pas une bonne explication des résultats fournis.

Parlons des systèmes basés sur le PDM. Dans ces systèmes, l'agent est intelligent, il interagit avec son environnement, observe l'effet de ses actions et tente d'améliorer ses prochaines actions. Ce principe permet à la fois de recommander du contenu en fonction des préférences de l'utilisateur, et de suggérer de nouvelles recommandations. Cette technique nous permet de satisfaire nos premiers et seconds besoins. Cependant, nous avons toujours le problème de l'espace de recherche. L'agent sera obligé de parcourir toutes les données disponibles pour trouver les préférences de l'utilisateur.

4.3 Notre approche hybride pour la recommandation

Dans cette section, nous modélisons le problème des systèmes de recommandation comme un problème de décision de Markov et nous proposons une solution hybride qui combine une technique clustering et un algorithme d'apprentissage par renforcement approprié.

À ce jour, l'apprentissage par renforcement est la technique d'apprentissage la plus dynamique. Il s'agit d'un agent intelligent qui interagit avec son environnement, observe les effets de ses actions sur cet environnement, déduit de ses observations la qualité de ses actions et tente d'améliorer ses actions futures.

4.3.1 Recommandation basée sur un Processus de Décision Markovien (PDM)

Comme le montre la Figure 4.3, dans un système de recommandation basé sur le PDM, le contenu vu par l'utilisateur est l'état, le prochain contenu qui pourrait l'intéresser est l'action, le retour de l'utilisateur est la récompense, et cela peut être formulé par un clic,

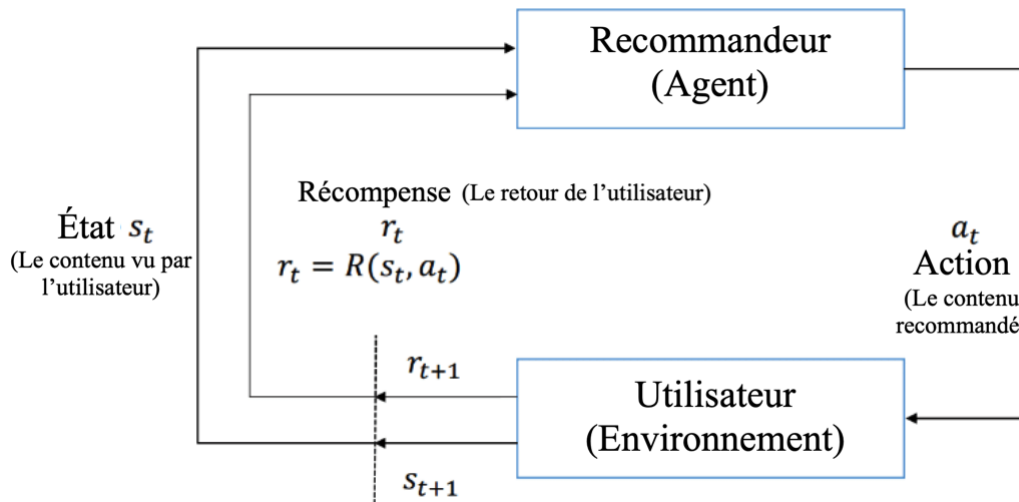


FIGURE 4.3 – Les systèmes de recommandation basés sur le PDM

un commentaire, une note ou si l'utilisateur a acheté ce produit. Le modèle peut être construit et validé sur la base de différents algorithmes d'apprentissage par renforcement comme l'actor-critic, le Q-learning, le DDPG ou l'apprentissage temporel. L'algorithme le plus utilisé dans la littérature et qui a donné les meilleurs résultats est l'algorithme Q-learning qui utilise la formule ci-dessous :

$$\underbrace{\text{New}Q(s, a)}_{\text{Nouvelle valeur Q-Value}} = Q(s, a) + \underbrace{\alpha}_{\text{Taux d'apprentissage}} \left[\underbrace{R(s, a)}_{\text{Récompense}} + \underbrace{\gamma}_{\text{Taux de Discount}} \underbrace{\max_{a'} Q'(s', a')}_{\text{Récompense maximale prédite, compte tenu du nouvel état et de toutes les actions possibles}} - Q(s, a) \right] \quad (4.1)$$

La fonction Bellman

4.3.2 Principe du Clustering Hiérarchique

Le clustering est une technique qui permet de regrouper des objets similaires de telle sorte que les objets d'un même groupe soient plus similaires entre eux que les objets des autres groupes. Le groupe d'objets similaires s'appelle un Cluster [RM05]. L'algorithme de clustering hiérarchique, également appelé analyse de cluster hiérarchique (HCA), est un algorithme de clustering non supervisé qui implique la création de clusters ayant un ordre prédominant de haut en bas [Joh67]. Le point final est un ensemble de clusters ou de groupes, où chaque cluster est distinct de tous les autres, et où les objets au sein de chaque cluster sont globalement similaires les uns aux autres. Cette technique de clustering est

divisée en deux types.

- Le clustering hiérarchique agglomératif : c'est le type le plus courant de clustering hiérarchique utilisé pour regrouper des objets en clusters sur la base de leur similarité. Il est également connu sous le nom d'AGNES (Agglomerative Nesting). Il s'agit d'une approche « ascendante » : chaque observation commence dans son propre cluster, et les paires de clusters sont fusionnées à mesure que l'on monte dans la hiérarchie [SB13].
- Le clustering hiérarchique divisé : ou DIANA (DIvisive ANALysis Clustering) est une méthode de clustering descendante dans laquelle nous assignons toutes les observations à un seul cluster, puis nous partitionnons le cluster en deux clusters moins similaires. Enfin, nous procédons récursivement sur chaque cluster jusqu'à ce qu'il y ait un cluster pour chaque observation. Cette approche de clustering est donc exactement opposée au clustering agglomératif [Sav+02].

Le but de tout cela est de démontrer la façon dont le clustering hiérarchique fonctionne, il conserve une mémoire de la façon dont on a traversé ce processus et cette mémoire est stockée dans le Dendrogram. Un dendrogramme est un type de diagramme arborescent montrant les relations hiérarchiques entre différents ensembles de données [LZH08].

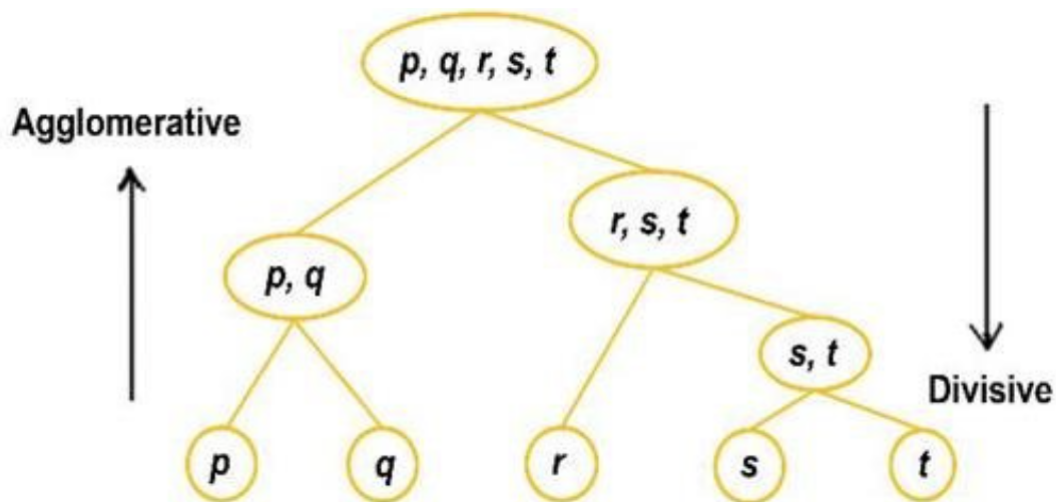


FIGURE 4.4 – Dendrogramme conceptuel pour le clustering hiérarchique agglomératif et divisif

4.3.3 Fusion des deux techniques

Dans le contexte de la recommandation, l'agent est le système, l'environnement est l'ensemble des produits à recommander, les actions sont les recommandations faites à l'uti-

lisateur et le feedback indique à l'agent la pertinence et l'utilité de ses actions. Ce processus d'apprentissage par essais et erreurs est particulièrement pertinent dans le contexte de la recommandation. D'une part, il permet une personnalisation systématique de la recommandation. Il se prête aussi particulièrement bien à la gestion de l'évolution des profils utilisateurs et des profils atypiques. D'autre part, il garantit la diversité et l'équité des recommandations, notamment en recherchant un bon compromis entre l'exploration de l'environnement et l'utilisation des informations déjà acquises.

Le clustering, comme mentionné, est une technique d'apprentissage non supervisée qui consiste à regrouper les données en ensembles cohérents appelés clusters. On parle de clustering hiérarchique lorsque les différents niveaux de clusters s'emboîtent les uns dans les autres, dessinant ainsi une structure arborescente. L'utilisation de cette technique dans le contexte de la recommandation, c'est-à-dire en travaillant avec des clusters et non des produits séparés, a plusieurs objectifs.

- Réduire l'espace à explorer par l'algorithme d'apprentissage par renforcement. En effet, la taille de l'environnement constitué de produits est presque infinie, et produire des recommandations pertinentes nécessitera plusieurs retours (essais et erreurs). Les erreurs potentielles peuvent frustrer l'utilisateur et le conduire à abandonner complètement l'utilisation du système.
- Expliquer les recommandations faites à l'utilisateur pour augmenter sa confiance dans le système. La description des différents clusters, au moyen d'étiquettes linguistiques, permettra bien sûr d'expliquer à l'utilisateur pourquoi telle recommandation lui a été présentée, mais surtout l'aidera à comprendre/décrire ces goûts et à acquérir/apprendre de nouvelles connaissances au fur et à mesure de son interaction avec le système.
- Protéger la vie privée des consommateurs. Le clustering conduit à l'agrégation et à la compression des données. Il garantit ainsi un premier niveau d'anonymisation et facilite la mise en place d'une solution de stockage local des données garantissant à l'utilisateur un contrôle et une confidentialité totale des données.

Notre méthode est divisée en trois parties : la construction des clusters (c'est-à-dire des états), l'apprentissage de la fonction Q de l'algorithme Q-learning et la génération des recommandations.

4.3.3.1 Construction des Clusters

Pour réduire l'espace et le nombre d'états traversés, il était nécessaire d'utiliser une technique qui à la fois réduit la complexité algorithmique de l'approche et aide à faire des recommandations personnalisées. C'est pourquoi nous avons utilisé une technique de clustering pour regrouper les données. Plusieurs méthodes existent, nous avons choisi d'appliquer la technique qui permet de construire des relations entre les différents clusters pour faciliter les transitions entre les états. Le clustering hiérarchique permet d'atteindre cet objectif. Pour réaliser toutes les probabilités de transition entre n données distinctes, une complexité de l'ordre de $O(n^2)$ était nécessaire. Alors qu'en regroupant les données, on peut itérer sur des classes de données similaires au lieu de traiter des données séparées, ce qui permet de diminuer la complexité jusqu'à $O(n)$. Enfin, la hiérarchie obtenue permet d'effectuer deux transitions à partir de chaque cluster.

Le clustering hiérarchique permet de construire un arbre, où à chaque niveau, chaque cluster est composé de deux sous-clusters. Ainsi, dans chaque état, le système a la possibilité de choisir l'un des deux sous-clusters, et donc il a deux actions possibles.

4.3.3.2 Apprentissage de la fonction Q

Après la construction des états, l'agent effectue une boucle sur tous les états et évalue la fonction Q pour chacune des deux actions possibles. Le Q-learning [WD92] est fréquemment utilisé pour les problèmes d'apprentissage par renforcement. Ensuite, la politique est mise à jour pour sélectionner les actions qui maximisent la valeur Q à chaque état. Finalement, une politique optimale peut être trouvée par l'équation de Bellman (4.2).

$$Q(s, a) = R(s, a) + \gamma \max_{a'} Q'(s', a') \quad (4.2)$$

L'itération de ces mises à jour conduit à la convergence vers la politique optimale [SB+98]. En d'autres termes, cela correspond aux actions qui guident l'utilisateur pour obtenir de bonnes recommandations, tout en maximisant les récompenses.

4.3.3.3 Génération des recommandations

Après avoir appliqué le Q-learning, chaque cluster aura un poids. En commençant par le cluster le plus général de la hiérarchie, on choisit à chaque fois la branche d'action

qui maximise les récompenses. Le clustering hiérarchique modélisé sous forme de dendrogramme permet de couper l'arbre au niveau souhaité, et donc de recommander le cluster qui a le poids le plus élevé avant d'atteindre les données feuilles. Cette méthode permet de recommander des classes de données plutôt que des données distinctes, et permet donc d'identifier le cluster préféré de l'utilisateur plutôt qu'un produit unique, facilitant ainsi la personnalisation des profils. Après chaque recommandation, le système reçoit un retour de l'utilisateur, qui peut être une note positive (satisfaction) ou une note négative (insatisfaction). En fonction de ce retour, l'algorithme recalcule les poids des clusters, met à jour le modèle et génère ensuite de nouvelles recommandations en fonction des nouveaux poids.

4.3.4 Synthèse

Pour conclure, notre idée est de proposer une approche hybride pour satisfaire tous nos besoins. Dans ce travail, nous proposons un nouveau système de recommandation basé sur l'apprentissage par renforcement. Nous formulons un système de recommandation sous la forme d'un arbre hiérarchique en utilisant une technique de regroupement hiérarchique [MC12] qui peut réduire de manière significative l'état et l'espace d'action. Il existe de nombreuses techniques statistiques visant à diviser une population en différentes classes ou sous-groupes. L'une d'entre elles est la Classification Ascendante Hiérarchique (CAH) [RV13]. On cherche à ce que les individus regroupés au sein d'une même classe (homogénéité intra-classe) soient les plus semblables alors que les classes sont les plus dissemblables (hétérogénéité inter-classe). Le principe du CAH est de rassembler les individus selon un critère de ressemblance défini au préalable qui sera exprimé sous la forme d'une matrice de distances, exprimant la distance existante entre chaque individu pris deux à deux. Deux observations identiques auront une distance nulle. Plus les deux observations sont dissemblables, plus la distance est grande. Le CAH va ensuite rassembler les individus de manière itérative afin de produire un dendrogramme ou un arbre de classification. La classification est ascendante car elle part des observations individuelles ; elle est hiérarchique car elle produit des classes ou groupes de plus en plus grands, y compris des sous-groupes à l'intérieur de ceux-ci. En coupant cet arbre à une certaine hauteur choisie, nous produirons la partition souhaitée. Un utilisateur qui a aimé un produit, il est très probable qu'il aime des produits similaires à celui qu'il a apprécié. Ainsi, en regroupant les

données, nous pouvons itérer à travers des classes de données similaires au lieu de traiter des données séparées. Nous avons donc choisi de regrouper les données avant d'appliquer l'approche afin d'optimiser la complexité de l'algorithme. Dans le clustering classique, il n'existe pas de méthodes pour choisir le nombre optimal de clusters sans générer un grand nombre de k . Un arbre de cluster est construit en utilisant le principe du clustering k -means. Cela permet de conserver les avantages du clustering sans introduire de grandes matrices de transition.

4.4 Évaluation expérimentale

Cette section présente l'évaluation expérimentale de la méthode proposée en analysant un jeu de données réel sur la qualité du vin extrait du référentiel d'apprentissage automatique de l'UCI¹ qui contient les détails du vin rouge et du vin blanc.

4.4.1 Base de données utilisée

Dans le cadre de ses projets, O°CCode travaille sur la recommandation de vin. Le jeu de données sur la qualité du vin qui est accessible au public à des fins de recherche est utilisé pour expérimenter l'approche proposée. Ce jeu de données représente les variantes rouge et blanche du vin portugais. Le vin blanc est composé de 4898 échantillons et le vin rouge de 1599 échantillons. Chaque échantillon des deux types de vin est composé de 11 variables physiochimiques : acidité fixe, acidité volatile, acide citrique, sucre résiduel, chlorures, dioxyde de soufre libre, dioxyde de soufre total, densité, pH, sulfates et alcool. Une 12ème variable est basée sur des données sensorielles (la moyenne d'au moins 3 évaluations faites par des experts du vin). Chaque expert a noté la qualité du vin entre 0 (très mauvaise) et 10 (très excellente). Les variables de la base de données nous permettent de comprendre la composition de chaque type de vin. Par exemple le pH décrit l'acidité ou l'alcalinité d'un vin sur une échelle allant de 0 (très acide) à 14 (très alcalin), la plupart des vins se situent entre 3 et 4 sur l'échelle du pH. Le chlorure est la quantité de sel dans le vin. L'alcool est le pourcentage de la teneur en alcool du vin, etc. L'objectif de ce jeu de données est de prédire la note qu'un expert attribuera à un échantillon de vin, en utilisant une série de propriétés physico-chimiques, telles que l'acidité et la composition alcoolique. Pour

1. <https://archive.ics.uci.edu/ml/datasets/wine+quality>

des raisons de confidentialité et de logistique, seules les variables physicochimiques (les entrées) et sensorielles (les sorties) sont disponibles (par exemple, il n’y a pas de données sur les types de raisins, la marque de vin, le prix de vente du vin, etc.) [EA16].

Le tableau 4.2 et le tableau 4.3 présentent ces propriétés physicochimiques différentes et les statistiques des données liées de vin blanc et de vin rouge, respectivement [EA16].

| Les attributs | Min | Max | Moyenne |
|-------------------------|-------|-------|---------|
| Acidité fixe | 3,800 | 14,20 | 6,855 |
| Acidité volatile | 0,080 | 1,100 | 0,278 |
| Acide citrique | 0,000 | 1,660 | 0,334 |
| Sucre résiduel | 0,600 | 65,80 | 6,391 |
| Chlorures | 0,009 | 0,346 | 0,046 |
| Dioxyde de soufre libre | 2,000 | 289,0 | 35,31 |
| Dioxyde de soufre total | 9,000 | 440,0 | 138,4 |
| Densité | 0,987 | 1,039 | 0,994 |
| pH | 2,720 | 3,820 | 3,188 |
| Sulfates | 0,220 | 1,080 | 0,490 |
| Alcool | 8,000 | 14,20 | 10,51 |

TABLEAU 4.2 – Les statistiques des données physico-chimiques du vin blanc

| Les attributs | Min | Max | Moyenne |
|-------------------------|-------|-------|---------|
| Acidité fixe | 4,600 | 15,90 | 8,320 |
| Acidité volatile | 0,120 | 1,580 | 0,528 |
| Acide citrique | 0,000 | 1,000 | 0,271 |
| Sucre résiduel | 0,900 | 15,50 | 2,539 |
| Chlorures | 0,012 | 0,611 | 0,087 |
| Dioxyde de soufre libre | 1,000 | 72,00 | 15,87 |
| Dioxyde de soufre total | 6,000 | 289,0 | 46,47 |
| Densité | 0,990 | 1,004 | 0,997 |
| pH | 2,740 | 4,010 | 3,311 |
| Sulfates | 0,330 | 2,000 | 0,658 |
| Alcool | 8,400 | 14,90 | 10,42 |

TABLEAU 4.3 – Les statistiques des données physico-chimiques du vin rouge

Ces valeurs ont été normalisées avant d’utiliser la base de données afin d’obtenir des scores compris entre 0 et 1 compatibles avec la méthode de calcul Q-learning.

4.4.2 Résultats

Il y a 12 attributs dans la base de données. 11 attributs qui décrivent les caractéristiques chimiques et sont utilisés pour le calcul de la similarité et donc le clustering

des données, et l'attribut de la qualité qui est utilisé pour entraîner le système et pour tester la précision de la prédiction de la fonction Q . Des expériences ont été menées pour vérifier si le système calcule correctement le poids des différents clusters en fonction des préférences d'un sommelier expert. Ainsi, si la prédiction est bien faite, les recommandations seront bien adaptées aux goûts de l'utilisateur. Nous avons entraîné le système avec une partie des notes des experts et nous avons essayé de prédire les notes pour les données restantes, si les notes calculées étaient plus ou moins proches des notes originales des experts, le système pourrait bien connaître les préférences du sommelier expert. Par conséquent, la prochaine fois, il recommandera les produits ayant les notes prédites les plus élevées. L'idée était donc de calculer le taux d'erreur des résultats de la prédiction. Notre objectif étant de prédire les notes des experts, nous avons dû utiliser des récompenses données pour calculer les poids des clusters ($\gamma = 0,1$), c'est-à-dire l'exploitation des notes des experts. En diminuant α (le taux d'apprentissage), le système met doucement à jour les poids des clusters, et donc il apprend mieux.

| Id | Valeur originale de qualité | Valeur prédite de qualité |
|------|-----------------------------|---------------------------|
| 1 | 0,56 | 0,54 |
| 106 | 0,56 | 0,53 |
| 469 | 0,67 | 0,61 |
| 738 | 0,56 | 0,45 |
| 1306 | 0,67 | 0,53 |
| 1570 | 0,78 | 0,61 |
| 1658 | 0,44 | 0,25 |
| 2055 | 0,56 | 0,35 |
| 2365 | 0,67 | 0,44 |
| 2901 | 0,89 | 0,61 |
| 5663 | 0,44 | 0,44 |
| 5786 | 0,44 | 0,45 |
| 5950 | 0,56 | 0,6 |

TABLEAU 4.4 – Prédiction de la valeur de la qualité du vin

Le tableau 4.4 représente les valeurs prédictives de la qualité du vin en comparaison avec les valeurs originales. Il n'est pas possible d'afficher les résultats pour toutes les données, donc les résultats sont affichés de manière aléatoire pour quelques lignes de la base de données. Les résultats montrent que la différence entre les valeurs n'est pas trop grande et donc nous pouvons dire que l'algorithme est capable de prédire les notes (qualité) du vin en utilisant une petite partie de la base de données.

Le tableau 4.5 représente le taux d'erreur des résultats calculés à l'aide de la formule

de l'erreur quadratique moyenne (RMSE), où y_i représente les valeurs prédites, x_i les valeurs originales et N le nombre d'observations.

$$RMSE = \sqrt{\sum_{i=1}^N \frac{(y_i - x_i)^2}{N}} \quad (4.3)$$

D'après les résultats, on constate que les taux d'erreur les plus faibles ont été obtenus

| % Train | Bonnes qualités | Mauvaises qualités | Fusion des deux qualités |
|---------|-----------------|--------------------|--------------------------|
| 5% | 25,64 | 25,51 | 30,57 |
| 10% | 19,91 | 19,41 | 26,40 |
| 15% | 18,59 | 16,5 | 20,54 |

TABLEAU 4.5 – Taux d'erreur des valeurs de prédiction

avec l'utilisation des qualités les plus basses du vin. Il serait peut-être préférable de savoir ce que l'utilisateur n'aime pas. Cette méthode peut aider à limiter encore mieux l'espace de recherche, car lorsqu'il y a un retour positif d'un utilisateur que le système ne connaît pas, il l'utilisera (exploitation) pour recommander des produits similaires et il continuera à chercher (exploration) dans d'autres catégories pour collecter encore plus d'informations sur le profil. Mais si le système reçoit une évaluation négative, il va exploiter ce feedback pour éviter toute la catégorie de produits similaires à ce produit et peut-être tout un cluster ou plus, et explorer l'autre partie de la base, ce qui limite bien l'espace de recherche et permet des résultats plus précis puisque la recherche sera plus orientée.

4.5 Conclusion

Le domaine de la recommandation s'est développé ces dernières années, ce qui nécessite une croissance dans ce secteur, et surtout dans le domaine de la vente dans les sites et les applications. Par conséquent, les chercheurs dans ce domaine ont concentré leurs travaux sur le développement de nouvelles approches pour améliorer la recommandation et la vente. Ces techniques sont utilisées dans plusieurs domaines d'application. Dans ce travail, nous avons modélisé le problème des systèmes de recommandation comme un problème de décision de Markov et nous avons proposé une solution hybride qui combine une technique particulière de regroupement hiérarchique et un algorithme d'apprentissage par renforcement approprié. L'utilisation de la technique du clustering nous a permis de répondre aux premier et troisième besoins de l'entreprise O°Code. D'une part, grâce

à cette technique, nous avons regroupé les données produits par cluster, et nous avons fait la recommandation en fonction des attributs de chaque produit sans toucher aux données utilisateurs. D'autre part, cette technique nous a permis d'avoir des descriptions des clusters obtenus, ce qui permet d'expliquer les recommandations. Ensuite, l'algorithme d'apprentissage par renforcement que nous avons utilisé a permis à notre système de parcourir différents produits, d'exploiter et d'explorer l'environnement, ce qui nous fournit de nouvelles recommandations qui évoluent avec les profils des utilisateurs. Par conséquent, nous avons pu répondre au deuxième besoin de O°Code.

Les résultats des tests sont prometteurs avec un taux d'erreur de seulement 16,5 %. Dans le futur, nous souhaitons comparer plusieurs méthodes de clustering, utiliser des ensembles de données plus importants disponibles dans la littérature afin de pouvoir comparer notre approche aux approches existantes. De plus, nous voulons étudier la notion de recommandation de groupe, c'est-à-dire l'étude des liens entre les profils pour extraire un goût commun pour un groupe d'utilisateurs. Enfin, nous voulons explorer d'autres techniques pour fournir des recommandations pertinentes et explicables. D'un autre côté, le problème de gestion des changements dans les profils des utilisateurs est toujours persistant. Il faut toujours assurer la confiance et l'adapter au comportement de l'utilisateur. Et donc il faut traiter les exigences liés aux besoins de l'utilisateur. De plus, le manque d'expliquabilité des recommandations nous ramène à la question comment on fait confiance aux recommandations d'un tel système ? Et enfin, ces systèmes rassemblent une collection massives de données qui peut atteindre la vie privée des utilisateurs. Et donc il faut savoir comment modéliser et assurer la confiance en respectant les données personnelles et en se basant sur les besoins et les comportements des utilisateurs.



Chapitre 5

Un cadre unifié pour la gestion de la confiance

Sommaire

| | | |
|------------|--|------------|
| 5.1 | Introduction | 98 |
| 5.2 | Définitions et Propriétés | 99 |
| 5.2.1 | Confiance | 100 |
| 5.2.1.1 | Contexte | 101 |
| 5.2.1.2 | Transitivité | 102 |
| 5.2.1.3 | Groupe | 102 |
| 5.2.1.4 | Distributivité | 103 |
| 5.2.2 | Réputation | 103 |
| 5.2.3 | Mesures de la confiance et de la réputation | 105 |
| 5.3 | Modèles computationnels | 106 |
| 5.4 | Les besoins métiers liés à la confiance | 109 |
| 5.5 | Analyse des modèles computationnels selon les besoins métiers | 112 |
| 5.5.1 | Modèle bayésien | 112 |
| 5.5.2 | Modèles basés sur les croyances | 113 |
| 5.5.3 | Modèles à valeur discrète | 113 |
| 5.5.4 | Modèles flous | 113 |
| 5.5.5 | Modèles de flux | 114 |
| 5.5.6 | Synthèse | 115 |
| 5.6 | Expérimentations et Résultats | 116 |

| | | |
|------------|---|------------|
| 5.6.1 | Besoin B_1 : « Bon utilisateur vs. Mauvais utilisateur » | 116 |
| 5.6.2 | Besoin B_2 : « Un nouvel utilisateur vs. un utilisateur avec comportement mi-positif mi-négatif » | 116 |
| 5.6.3 | Besoin B_3 : « Le système se souvient des fraudes » | 117 |
| 5.6.4 | Besoin B_4 : « Récidivisme » | 117 |
| 5.6.5 | Besoin B_5 : « Droit à l'erreur » | 119 |
| 5.6.6 | Besoin B_6 : « Vol d'identité » | 119 |
| 5.7 | Conclusion | 121 |

5.1 Introduction

Les concepts de confiance et de réputation sont d'une importance capitale dans les sociétés humaines. Plusieurs disciplines ont recours à leur utilisation de différentes manières selon leurs propres visions et perspectives. Historiquement, ces deux concepts ont émergé dans le domaine de la psychologie et se sont ensuite rapidement étendus à toutes les disciplines liées aux sciences humaines. Dans ce travail, nous mettons en évidence l'utilisation de ces concepts dans un domaine qui devient omniprésent dans nos vies, à savoir le système informatique.

Les travaux de Marsh [Mar94] sont considérés comme les premiers à avoir introduit la notion de confiance dans les systèmes informatiques. Aujourd'hui, de très nombreux systèmes et applications informatiques très connus reposent sur cette notion. Nous pouvons citer le système de réputation présent sur les sites E-commerce Ebay¹ et Amazon² ainsi que les systèmes de notation de plateformes comme Tripadvisor³ ou Goodreads⁴.

Des travaux de recherche ont proposé des modèles théoriques et pratiques pour appréhender la notion de confiance et améliorer les systèmes existants. C'est un domaine de recherche très actif avec de nombreuses propositions récentes [Jia+19; YK20; Moh+19].

. En étudiant les travaux de la littérature sur la confiance, nous avons constaté qu'il existe de nombreuses définitions de la confiance et des notions associées. De plus, contrairement à d'autres domaines comme la conception de programme informatique ou de bases

1. <https://www.ebay.fr/>
2. <https://www.amazon.fr/>
3. <https://www.tripadvisor.fr/>
4. <https://www.goodreads.com/>

de données, il n'existe pas de formalisme graphique pour représenter cette notion et concevoir un système informatique qui s'appuie sur celle-ci.

D'autre part, concernant les modèles computationnels, nous avons constaté qu'il n'est pas aisé de comprendre la sémantique et l'intuition derrière les calculs effectués par ces modèles pour calculer et propager la confiance au sein d'un réseau d'utilisateur. Ceci est un frein pour une société comme O°Code qui souhaite choisir un modèle computationnel qui soit adapté aux besoins applicatifs et cohérent avec les valeurs de l'entreprise.

Pour répondre à ces limites, nous commençons par proposer dans ce chapitre une unification des définitions liées à la confiance et aux notions associées. Nous proposons une formalisation de ces concepts associée à des représentations graphiques. Dans un second temps, nous proposons une étude permettant de comprendre le comportement et l'intuition des modèles computationnels les plus fréquemment utilisés. Nous proposons différents critères qui permettent de caractériser ces modèles afin de faciliter leur comparaison. Ce travail a été publié dans l'article [Sel+21] qui a été présenté à la conférence internationale sur les défis de la recherche en sciences de l'information.

Le reste du document est composé comme suit : la section 5.2 présente les définitions et les propriétés liées à la confiance et à la réputation. Cette section introduit également notre première contribution, qui est la formalisation graphique et textuelle des principes de confiance et de réputation. La section 5.3 décrit les différents types de modèles informatiques de confiance et de réputation. La section 5.4 représente certaines exigences tirées des besoins de l'entreprise pour le choix d'un modèle computationnel. Notre deuxième contribution est présentée dans la section 5.5 concernant le comportement des modèles computationnels. Pour valider notre proposition, une étude expérimentale est présentée dans la section 5.6. Enfin, les points à retenir et les perspectives sont présentés dans la section 5.7.

5.2 Définitions et Propriétés

Dans cette section, nous commençons par donner les différentes définitions de la notion de confiance et des concepts associés issues de la littérature. Nous proposons ensuite notre définition unifiée ainsi qu'une représentation graphique de ce concept et de ceux qui lui sont liés.

Notons tout d'abord que la réputation peut être vue comme un signal visant à réduire l'incertitude des actions et comportements futurs d'un acteur dans une situation de choix. Si, par exemple, un acheteur dispose de moins d'informations sur un produit qu'il souhaite acheter, la « bonne » réputation du vendeur peut être un signal pour le rassurer sur son achat. La réputation est donc une information qui réduit l'incertitude d'un acteur. Elle est construite à partir d'informations sur les comportements passés (dans notre exemple, ceux du vendeur ou de sa marque), et devient potentiellement un facteur de confiance. On peut donc déduire de cette description que la réputation est une relation entre l'utilisateur et le système alors que la confiance est une relation entre deux utilisateurs.

Nous allons détailler toutes les notions liées à ces concepts dans cette section. Commençons par la description de la confiance, entre utilisateurs et avec un groupe d'utilisateurs. Cet échange a évidemment lieu dans un contexte bien défini. D'autres aspects, tels que la transitivité, la distributivité et la réputation, peuvent également affecter le concept de la confiance. Enfin, nous devons mesurer ces concepts afin de les rendre plus simples pour les utilisateurs. Pour cela, nous avons besoin de modèles de calcul qui fondent initialement leurs estimations sur l'historique des transactions des utilisateurs.

5.2.1 Confiance

La confiance est un concept que nous appliquons quotidiennement. Nous faisons confiance à ce matériel ou à cette personne pour mener à bien certaines actions. Malheureusement, la confiance souffre d'un problème de définition, en l'absence d'une définition précise couramment utilisée dans la littérature. Selon [LB+96], il est possible de classer les perspectives de la confiance en trois catégories : (i) celle des théoriciens de la personnalité qui conceptualisent la confiance comme une croyance, une attente ou un sentiment profondément ancré dans la personnalité ; (ii) celle des sociologues, centrée sur la compréhension du lien social ; (iii) celle des psychosociologues qui définissent la confiance en termes d'espoir et de consentement d'un tiers qui s'engage dans une transaction.

Comme on peut le constater, différentes définitions de la confiance ont été proposées. On peut généralement dire que la confiance est une relation entre deux personnes : « un trustor : l'utilisateur qui fait confiance » et « un trustee : l'utilisateur à qui on fait

confiance ».

La relation de confiance peut donc être modélisée comme dans la figure 5.1, où l'utilisateur U_1 (Trustor) fait confiance à un autre utilisateur U_2 (Trustee) avec une valeur X :

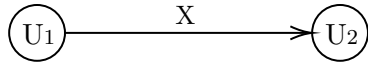


FIGURE 5.1 – Notation graphique de la confiance

$$C(U_1, U_2) = X$$

FIGURE 5.2 – Notation textuelle de la confiance

La fonction $C(U_1, U_2)$ a deux arguments : le trustor « U_1 » et le trustee « U_2 », le résultat de cette fonction est X « la valeur du trust ».

C est la fonction mathématique utilisée par le modèle computationnel de la confiance. Les valeurs possibles de C seront décrites ultérieurement.

5.2.1.1 Contexte

Selon [Vu10], pour définir la confiance, le contexte est un facteur important. Il indique la situation dans laquelle la relation est établie. En dehors de ce contexte, la relation peut ne plus être affirmée. Par exemple : « Alice peut faire confiance à Bob pour lui enseigner les mathématiques, mais elle ne peut pas lui faire confiance pour cuisiner ». Pour représenter le contexte associé à la notion de confiance, nous proposons la notation graphique présentée sur la figure 5.3. La confiance de U_1 en U_2 dans un contexte c est de X , on note :

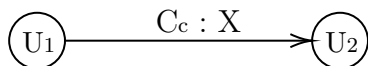


FIGURE 5.3 – Notation graphique du contexte

$$C_c(U_1, U_2) = X$$

FIGURE 5.4 – Notation textuelle du contexte

Considérant que c est une représentation du contexte qui peut être défini plus ou moins précisément selon les besoins applicatifs. Ainsi, le contexte peut être défini uniquement par un mot quand c'est suffisant (par exemple, « Mathématiques » ou « Cuisine ») ou de manière plus précise par un modèle dédié si c'est nécessaire.

5.2.1.2 Transitivité

Ainsi, une fois que la notion de confiance est évoquée, la question de savoir si la relation de confiance est transitive se pose. C'est-à-dire que si U_1 fait confiance à U_2 et que U_2 fait confiance à U_3 , est-ce que U_1 fait confiance à U_3 ? Une notation graphique de la transitivité est donnée dans la Figure 5.5. La plupart des chercheurs dans le domaine de la confiance parviennent à un consensus : la confiance n'est pas complètement transitive entre les acteurs, c'est à dire que la relation de confiance n'est pas transitive globalement mais qu'elle peut l'être pour un sous-ensemble du réseau d'utilisateur. Nous avons donc besoin d'une notation quand c'est le cas. Si U_1 fait confiance à U_2 et que U_2 fait confiance à U_3 , alors U_1 fait confiance à U_3 , on note :

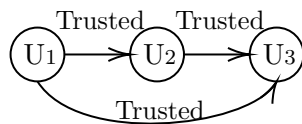


FIGURE 5.5 – Notation graphique de la transitivité

$$C(U_1, U_2) = x \wedge C(U_2, U_3) = y \Rightarrow \exists f / f(x, y) = z.$$

FIGURE 5.6 – Notation textuelle de la transitivité

Comme Josang et Pope le prouvent dans [JP05], la transitivité n'est possible que dans certains cas. Cependant, dans le cas de la transitivité, lorsque le nombre de recommandations augmente, le niveau de confiance est susceptible de diminuer. Par exemple, si Bob demande à Alice de lui recommander un dentiste. Alice répond : « Ma sœur m'a parlé d'un dentiste que son amie lui a recommandé de la part d'un ami de confiance ». Le niveau de confiance de Bob dans cette recommandation est moins élevé que s'il s'agissait d'un dentiste qu'Alice avait vu directement.

5.2.1.3 Groupe

Un groupe dans le réseau de confiance est un ensemble d'utilisateurs ou de groupes. On peut voir sur la figure 5.7 la représentation graphique d'un groupe, la lettre G ; avec l'identifiant reflète le nom du groupe, P est le propriétaire du groupe (ici nous supposons un seul propriétaire), et on peut trouver d'autres membres, on note alors : $G_i = \{P, U_i, \dots, U_j\}$. Un groupe peut être, par exemple, une marque, une organisation, une association, un groupe d'amis dans un réseau, etc. Dans le contexte des projets O°Code, un groupe est un réseau d'amis qui ont les mêmes préférences et qui se font confiance. En reprenant l'exemple du

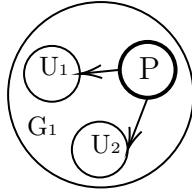


FIGURE 5.7 – Notation graphique d’un groupe

vin évoqué dans le chapitre précédent, un groupe est l’ensemble des utilisateurs qui ont apprécié les mêmes produits.

5.2.1.4 Distributivité

La notion de groupe ayant été présentée, la question est maintenant de savoir comment la relation de confiance se propage au sein d’un tel groupe. Nous parlons de la distributivité de la notion de confiance. La distributivité de la confiance est obtenue si un utilisateur a confiance dans un groupe comme dans la figure 5.8. Comme la transitivité, la distributivité dépend du contexte applicatif et notre proposition permet de la représenter quand c’est le cas. Si un utilisateur U_3 fait confiance au groupe G_1 avec une valeur X , cela peut permettre de calculer une valeur de confiance entre l’utilisateur U_3 et les membres du groupe G_1 .

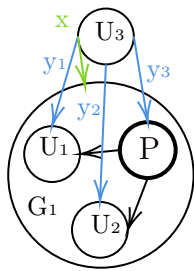


FIGURE 5.8 – Notation graphique de la distributivité

$$C(U_3, G_1) = x ; G_1 = P, U_1 \dots U_n \Rightarrow \exists f / f(x, U_i) = y_i.$$

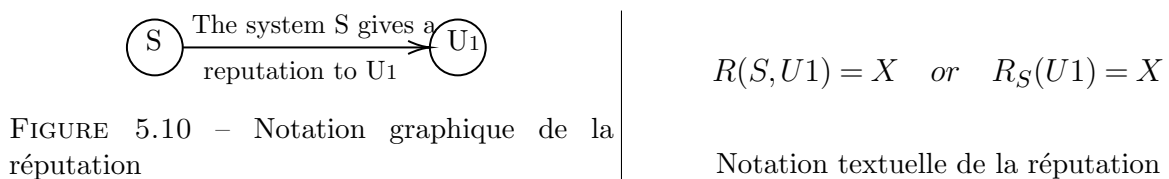
Notation textuelle de la distributivité

5.2.2 Réputation

Le deuxième concept considéré dans ce travail est la réputation. Plusieurs définitions de ce concept peuvent être trouvées dans différents domaines de la littérature. La première est une définition assez générale, à savoir que la réputation peut être considérée comme le sentiment qu’un utilisateur a envers un autre utilisateur [KB16], qui est utilisé pour

décider de coopérer avec lui [PS13]. Selon [Vu10], la réputation est l'opinion d'une communauté sur un individu, un groupe ou une organisation. Jøsang et al [JIB07] considèrent que « la réputation est ce qui est dit ou cru au sujet d'une personne ou des propriétés d'un objet ». Ils pensent également que la réputation est un moyen d'établir la confiance. Dans une communauté, on peut faire confiance à une personne si elle a une bonne réputation. Selon Abdul-Rahman et Hailes [AH00a], la réputation est une estimation du comportement d'une entité dans la communauté, basée sur ses comportements passés. Cette définition prend en compte deux sources principales d'information pour estimer la réputation : les expériences passées avec le sujet et les recommandations d'autres entités dans la communauté. De plus, il est important de dire que la réputation d'un utilisateur n'est pas absolue, mais que sa valeur peut varier selon l'utilisateur qui l'évalue et selon le contexte de l'évaluation.

Les différentes définitions de la réputation font toujours appel à la notion de « communauté ». La réputation est en effet un capital immatériel (une opinion, un sentiment) sur lequel un individu n'a pas un contrôle total puisqu'il émane de la communauté. Ainsi, par instanciation dans le domaine de l'informatique, la réputation est l'opinion d'un système envers une personne ou un groupe. Nous proposons donc de représenter le concept de réputation comme dans la figure 5.10, où le système attribue une note de réputation à un utilisateur ou à un groupe d'utilisateurs, en fonction des opinions de la communauté et de son comportement dans le système. La réputation de U_1 dans le système S est de X .



Comme dans le cas de la confiance, il existe des modèles informatiques de réputation qui représentent une extension du concept de réputation au domaine informatique. Un exemple d'un tel système de réputation est le mécanisme de rétroaction utilisé par eBay. L'application de ces modèles permet un certain degré de contrôle et de surveillance des actions, ce qui est impossible pour un agent humain. En effet, un humain peut être capable de se souvenir des interactions passées. En revanche, il n'est pas capable de les quantifier et d'enregistrer une valeur précise pour ces interactions. Un système informatique peut le faire avec une certaine précision. Il est capable de mesurer les résultats des interactions

précédentes et de les stocker sans interruption. Après l'apparition des sites de vente en ligne, ces systèmes se sont considérablement développés : le donneur de confiance est le site (ou éventuellement un ensemble de sites partenaires), les demandeurs de confiance sont les utilisateurs (clients et vendeurs) et leurs réputations dépendent de la manière dont les achats et les ventes se sont déroulés sur le site. Ceci nous amène à l'importance de pouvoir mesurer la confiance et la réputation dans un système informatique. Nous l'étudions dans la section suivante.

5.2.3 Mesures de la confiance et de la réputation

Afin de quantifier la confiance et la réputation, une mesure appropriée est nécessaire. Quatre types de valeurs d'une telle mesure sont généralement utilisés.

- **Valeur unique ($V \rightarrow \text{Integer}$)** : une valeur unique peut être utilisée pour mesurer la confiance. Cette valeur n'est mentionnée que si l'entité n'inspire pas confiance et ne fait rien dans le cas contraire. Il s'agit de la mesure utilisée pour garantir la qualité des produits dans une chaîne de production. Par exemple, si un article n'est pas conforme aux exigences de fabrication, il est retiré de la chaîne et rien n'est signalé par ailleurs.
- **Valeurs binaires ($V \rightarrow \{0,1\}$)** : les valeurs binaires sont utilisées pour faire la distinction entre une entité fiable et une entité non fiable. Les valeurs binaires ne permettent pas de distinguer un utilisateur avec lequel on a déjà un historique de coopération. Par exemple, si on fait confiance à un utilisateur, on lui attribue une note de 1, et 0 sinon.
- **Valeurs multiples ($V \rightarrow \text{tf, f, m, e, te}$)** : permettent de prendre en compte l'historique de la coopération entre deux entités. Par exemple, les valeurs possibles sont les niveaux de confiance « très faible, faible, moyen, élevé et très élevé ».
- **Valeurs continues ($V \in [0,1]$)** : les valeurs générées sont des valeurs discrètes. Les valeurs continues donnent un plus large éventail de valeurs possibles du niveau de confiance. Généralement, cette valeur varie dans l'intervalle $[0,1]$; elle mesure la confiance sous forme de probabilité avec un seuil définissant la valeur minimale pour qu'une entité soit considérée comme une entité digne de confiance.

Pour mesurer le degré de confiance et la réputation sous la forme d'une valeur quelconque,

les systèmes informatiques se sont appuyés sur des modèles de confiance utilisant différents procédés selon les besoins. Maintenant que nous avons vu différentes manières de quantifier la confiance et la réputation au sein d'un système informatique, la question est de savoir comment ces valeurs sont calculées et comment elles évoluent en fonction des actions des utilisateurs. Pour répondre à ces questions, différents modèles computationnels ont été proposés dans la littérature. Nous les abordons dans la section suivante.

5.3 Modèles computationnels

Les systèmes basés sur la confiance et la réputation doivent disposer d'une méthode de calcul du degré de ces deux concepts. En effet, le processus de calcul doit permettre de prendre une décision. Par exemple, un degré élevé de confiance dans une entité permet de juger cette entité comme étant fiable et de prendre la décision de lui faire confiance. Il en va de même pour la réputation. Différents modèles ont été proposés pour représenter et calculer la confiance et la réputation dans les systèmes, comme indiqué dans le chapitre de l'état de l'art. Ces modèles peuvent être classés comme suit : modèles bayésiens, modèles basés sur les croyances, modèles à valeurs discrètes, modèles flous et modèles de flux.

Un bref résumé de ces modèles sera donné dans cette section.

- **Les modèles bayésiens** : ces modèles prennent des scores d'entrée binaires (c'est-à-dire positifs ou négatifs), et sont basés sur le calcul de scores de confiance et de réputation par la mise à jour statistique de fonctions de distribution de probabilité [JIB07]. Formellement, un réseau bayésien est défini comme un graphe orienté acyclique noté $G = (V, E)$ où V est l'ensemble des variables aléatoires (nœuds) et E est l'ensemble des arcs représentant les liens de causalité entre les variables. Parmi les modèles de la littérature utilisés pour l'étude comparative de ce document, on peut citer quatre modèles utilisant ce type de modèle (c'est-à-dire des modèles bayésiens) pour calculer et représenter les valeurs de confiance et de réputation [AA14 ; LDR13 ; Wie+13 ; AA16b].
- **Les modèles basés sur les croyances** : le modèle de croyance peut être un système lié à l'hypothèse de probabilité, mais où la totalité des probabilités sur tous les résultats concevables n'est pas fondamentalement élevée à 1. La probabilité restante se traduit par une incertitude. Les travaux qui sont basés sur ce type de

modèle, ont non seulement calculé une valeur de confiance ou de réputation, mais ont également souligné qu'un utilisateur dans une telle situation peut ne pas être en mesure de juger ou d'évaluer un autre utilisateur, surtout s'il n'y a pas eu d'interactions entre les deux. En observant les modèles de la littérature revue, nous pouvons trouver quelques modèles qui ont considéré cette notion d'incertitude ou d'incrédulité : [LDR13 ; AXJ15 ; ŠHZ16 ; Zho+14].

- **Les modèles à valeurs discrètes** : les humains sont souvent plus capables d'évaluer les performances sous la forme de déclarations verbales discrètes que de mesures continues. Cela est également vrai pour déterminer les mesures de confiance, et certains auteurs ont proposé un modèle de confiance discret. L'inconvénient des mesures discrètes est qu'elles ne se prêtent pas facilement à la manipulation informatique. Ce que l'on constate dans la littérature, c'est qu'il n'y a pas beaucoup de modèles qui ont utilisé ce type de données. Parmi ceux qui ont été étudiés, il existe deux modèles de calcul [AH00a] et [Lin+15] qui ont évalué la confiance et la réputation sous la forme de déclarations verbales discrètes.
- **Les modèles flous** : la confiance et la réputation peuvent être considérées comme des concepts linguistiques flous, où les fonctions d'appartenance décrivent la mesure dans laquelle un acteur peut être décrit, par exemple, comme : « digne de confiance » ou « indigne de confiance ». Les modèles flous ne sont pas des outils de calcul, mais aident à représenter la confiance et la réputation de manière qualitative à partir de valeurs numériques. Certains modèles de la littérature appartiennent à cette catégorie de modèles : [TMP15 ; CSS16 ; AA16a].
- **Les modèles de flux** : les systèmes qui calculent la confiance ou la réputation par itérations transitives à travers des chaînes en boucle ou arbitrairement longues sont appelés modèles de flux [JIB07]. Quelques modèles de flux supposent un poids constant de confiance/réputation pour la communauté dans son ensemble, et ce poids peut être transmis entre les membres de la communauté. Les participants ne peuvent augmenter leur confiance/réputation qu'au détriment des autres. Le PageRank de Google et le système de réputation d'Advogato appartiennent à cette catégorie. En général, la réputation d'un utilisateur augmente avec le flux entrant et diminue avec le flux sortant. Pour ce type de modèle, on peut citer le modèle Flow-Based Reputation with Uncertainty présenté dans [ŠHZ16], et le modèle Ei-

genTrust développé au départ en 2000 dans [DFM01], puis une version dynamique de ce dernier a été implémentée en 2016 dans [LWL16].

Pour comparer ces différents modèles, un des caractéristiques qu'il faut prendre en compte pour répondre aux besoins de O°Code, est les sources d'information utilisées par les modèles pour calculer les valeurs de confiance. Ces informations peuvent provenir de différentes sources, soit de transactions directes entre utilisateurs, soit en utilisant les transactions et les opinions des autres utilisateurs de la communauté, soit en se référant aux relations sociales des utilisateurs, soit en formant des préjugés sur un utilisateur à partir d'autres utilisateurs qui lui sont similaires.

Un autre phénomène qu'il faut prendre en considération, c'est le problème de démarrage à froid. C'est le phénomène qui se produit au début de l'utilisation du système, dans des situations critiques où le système manque de données pour effectuer un filtrage personnalisé de bonne qualité. Dans les modèles de confiance et de réputation, ce problème se produit lorsqu'un nouvel utilisateur interagit avec le système pour la première fois, le système ne dispose d'aucun historique de transaction ou d'avis sur cet utilisateur pour évaluer sa réputation ou pour aider les autres à décider s'ils peuvent lui faire confiance ou non. Le problème du démarrage à froid est toujours présent dans presque tous les systèmes d'information qui interagissent avec les utilisateurs ou les produits. Dans la littérature sur les modèles de confiance computationnels, et surtout parmi les modèles discutés dans l'étude de ce travail, il a été noté qu'il y a six modèles qui ont mis en évidence ce problème et ont essayé de le résoudre.

Dans cet section, nous avons présenté les différents types des modèles computationnels de confiance. Nous avons donné à titre d'exemple les modèles les plus connus et cité dans la littérature. Nous avons essayé de faire une comparaison entre ces modèles (Tableau 5.1). Nous avons basé notre recherche sur les principales caractéristiques qui distinguent un modèle d'un autre. Par la suite, nous sommes arrivés à une interprétation, qui est que pour comprendre pleinement le fonctionnement d'un modèle basé sur la confiance et la réputation, il est principalement nécessaire de comprendre le type de représentation et de modélisation utilisé par chaque système, les entrées de son modèle, la procédure de calcul qu'il suit et s'il aborde le problème du démarrage à froid ou non. Nous constatons de même qu'il est difficile même avec cette comparaison de comprendre l'intuition derrière ces modèles et si ils répondent aux besoins applicatifs de l'entreprise O°Code.

TABLEAU 5.1 – Comparaison des différents modèles

| Modèle Computational | Type du modèle computationnel | Fonction Mathématique | Source d'informations | Démarrage à froid |
|---------------------------------|---|---|----------------------------------|----------------------|
| Ashtiani and Azgomi [AA14] | Modèle Bayésien | Distribution de probabilités/ Fonctions de statistique | TD ^a / A ^b | Non |
| Liu et al. [LDR13] | Modèle Bayésien Modèle basés sur les croyances | Distribution de probabilités/ Fonctions de statistique | DT / O / P ^c | Oui |
| Wierzbicki et al. [Wie+13] | Modèle Bayésien | Distribution de probabilités Fonctions de statistique | A | Non |
| Ashtiani and Azgomi [AA16b] | Modèle Bayésien | Distribution de probabilités | TD/A | Non |
| Abdel-Hafez et al. [AXJ15] | Modèle Bayésien Modèle basés sur les croyances | Distribution de probabilités/ Fonctions de statistique | A | Non |
| Škorić et al. [SHZ16] | Modèle basés sur les croyances Modèle de flux | Logique probabiliste | TD/A | Non |
| Zhong et al. [Zho+14] | N/A | Différents | TD | Non |
| Abdul-rahman and Hailas [AH00b] | Modèle à valeurs discrètes | Fonctions de statistique | TD/A | Non |
| Lin et al. [Lin+15] | Modèle à valeurs discrètes | Fonctions de statistique | DT | Non |
| Tormo et al. [TMP15] | Modèles flous | Différents | TD/A | Oui |
| Chandran et al. [CSS16] | Modèles flous | Fonctions de statistique | TD/A | Non |
| Ashtiani and Azgomi [AA16a] | Modèles flous | Fonctions de statistique | TD/A/RS ^d | Non |
| Dingledine et al. [DFM00] | Modèles de flux | Fonctions de statistique | TD | Non |
| Lu et al. [LWL16] | Modèles de flux | Fonctions de statistique | TD | Non |

- a. TD : Transactions Directes
- b. A : Avis d'autres utilisateurs
- c. P : Préjugés
- d. RS : Relations sociales

Nous illustrons ce problème en présentant différents besoins applicatifs sur la confiance identifiés au sein de O°Code. Nous proposerons ensuite une étude pour montrer comment les principaux modèles computationnels se comportent par rapport à ces besoins.

5.4 Les besoins métiers liés à la confiance

Différents systèmes utilisent les modèles présentés ci-dessus. Bien entendu, ils ne peuvent pas tous être utilisés en même temps. Il faut choisir le modèle qui correspond le mieux aux exigences du système souhaité. Nous discutons ci-dessous de certaines exigences qui semblent critiques pour l'entreprise O°Code lors du choix d'un modèle de confiance et de réputation.

Premier Besoin (B_1)

« Bon utilisateur vs mauvais utilisateur »

Un besoin applicatif de l'entreprise O°Code est de pouvoir distinguer les bons utilisateur, c'est-à-dire ceux qui ne font que des bonnes actions, des mauvais utilisateurs qui font plus ou moins de mauvaises actions sur le système.

Les bonnes actions augmentent de plus en plus la confiance et les mauvaises actions

la diminuent de plus en plus. Pour O°Code, la valeur de confiance d'un utilisateur qui ne fait que des bonnes actions (six actions positives) devrait être plus élevée que la valeur de confiance d'un utilisateur qui a fait à la fois des bonnes actions (deux actions positives) et des mauvaises actions (quatre actions négatives).

Deuxième Besoin (B_2)

« *Un nouvel utilisateur vs un utilisateur au comportement mi-positif mi-négatif* »
Un besoin applicatif de l'entreprise O°Code est de donner plus de confiance à un nouvel utilisateur qu'à un utilisateur ayant fait autant de bonnes actions que de mauvaises actions.

Pour O°Code, un nouvel utilisateur a une confiance neutre et un utilisateur ayant un comportement mi-positif et mi-négatif devrait avoir une confiance inférieure à la confiance neutre. Par conséquent, un nouvel utilisateur doit avoir une confiance de départ plus élevée qu'un utilisateur qui a effectué quatre actions positives et quatre négatives.

Troisième Besoin (B_3)

« *Le système se souvient des fraudes* »
Un besoin applicatif de l'entreprise O°Code est de prendre en compte les mauvaises actions même si de nombreuses bonnes actions sont effectuées par la suite.

Pour O°Code, si un utilisateur effectue beaucoup de bonnes actions et quelques autres mauvaises, il doit avoir moins de confiance qu'un utilisateur qui n'a jamais fraudé et dont le nombre d'actions positives est inférieur au premier.

Quatrième Besoin (B_4)

« *Droit à l'erreur* »
Un besoin applicatif de l'entreprise O°Code est de permettre à un utilisateur de regagner sa confiance après avoir fait une mauvaise action.

Si un utilisateur qui a un comportement positif fait une mauvaise action, il peut regagner une partie de sa confiance en faisant de bonnes actions. Par exemple, nous supposons que l'utilisateur fait de bonnes actions (10 actions positives) puis fait une mauvaise action

et ensuite il recommence à faire de bonnes actions (trois actions positives). Pour O°Code, le modèle de calcul doit réagir à ce scénario avec un faible impact « récupération partielle de la confiance ».

Ce besoin peut sembler, à juste titre, contradictoire avec le précédent (B_3). Puisque O°Code est impliqué dans différents contextes applicatifs (Vins, Vélo, etc.) qui n'ont pas les mêmes exigences en terme de propagation de la confiance. Cette section énumère les besoins de différents cadres applicatifs (d'où les contradictions possibles entre les besoins).

Cinquième Besoin (B_5)

« *Récidive* »

Un besoin applicatif de l'entreprise O°Code est de baisser fortement la confiance d'un utilisateur qui fait régulièrement des mauvaises actions malgré le fait qu'il puisse en faire de bonnes entre temps.

Pour O°Code, le fait de refaire les mêmes erreurs est la récidive. Nous supposons que l'utilisateur effectue une bonne action, puis une mauvaise action et qu'il répète plusieurs fois cette séquence d'actions.

Sixième Besoin (B_6)

« *Vol d'identité* »

Un besoin applicatif de l'entreprise O°Code est d'identifier les potentiels vols d'identité qui engendrent un comportement inhabituel qui doit être immédiatement répercuté en baissant fortement la confiance de l'utilisateur concerné.

Un bon système de confiance devrait remarquer les comportements inhabituels ou anormaux de ses utilisateurs. Pour O°Code, si l'utilisateur a déjà fait beaucoup de bonnes actions, il doit perdre complètement sa confiance s'il fait plusieurs mauvaises actions successives (une possibilité d'usurpation d'identité). Le système doit être punitif dans ce cas.

Maintenant que nous avons défini différents critères que nous avons identifiés dans plusieurs contextes applicatifs de l'entreprise O°Code, nous constatons qu'il est difficile de savoir quel est le ou les modèles computationnels les plus adaptés pour répondre à ces besoins. Comme première proposition pour répondre à ce besoin, nous proposons dans la section suivante une analyse des modèles computationnels.

5.5 Analyse des modèles computationnels selon les besoins métiers

L'analyse des modèles computationnels permet de choisir les modèles adaptés aux besoins du système. Cette étude est basée sur des scénarios d'utilisation qui simulent les critères d'évaluation spécifiés dans la section précédente. Dans cette section, pour chaque modèle computationnel, nous précisons sa sémantique et son intuition en étudiant les propriétés de sa fonction de calcul. Ceci permettra la mise en œuvre de scénarios d'action et la différenciation des modèles en fonction de leur comportement.

5.5.1 Modèle bayésien

Comme mentionné précédemment, les modèles bayésiens utilisent les fonctions de distribution de probabilité pour estimer les valeurs de confiance et de réputation. La fonction de distribution d'une variable aléatoire réelle X est la fonction F_X qui, à tout réel x , associe la probabilité d'obtenir une valeur telle que :

$$F_X(x) = \mathbb{P}(X \leq x). \quad (5.1)$$

La fonction F_X dépend de la loi utilisée par le modèle de calcul, comme par exemple la distribution bêta, la distribution empirique, la distribution normale, la distribution multinomiale, la distribution de Dirichlet [Fis94], la probablistique quantique, le vecteur de distribution, etc. Cette valeur de probabilité est généralement normalisée pour appartenir à l'intervalle $[-1,1]$, afin de représenter les bons comportements par des valeurs positives, et les mauvais comportements par des valeurs négatives. Par conséquent, une valeur neutre de la confiance ou de la réputation est égale à zéro.

Dans la théorie des probabilités, la procédure de la machine doit être répétée de nombreuses fois afin de prendre une décision finale. Cette approche induit une évolution lente des valeurs attendues. Par conséquent, pour obtenir de bons taux de confiance et de réputation, il est important d'effectuer de nombreuses transactions. Cette stratégie est bénéfique dans le sens où elle donne à un consommateur qui a effectué une mauvaise transaction la possibilité de regagner sa crédibilité, en diminuant progressivement ses qualités. Mais à terme, elle le punira. L'inconvénient est que le modèle ne peut pas le détecter ex-

plicitement en cas d'utilisation malveillante de l'appareil. Il faut plusieurs tentatives de fraude pour réduire la crédibilité de l'utilisateur concerné.

5.5.2 Modèles basés sur les croyances

Comme les modèles bayésiens, la théorie de la croyance est liée à la théorie des probabilités, la différence étant que la somme des probabilités sur tous les résultats possibles n'est pas nécessairement égale à 1, et la probabilité restante est interprétée comme une incertitude. À l'initialisation du modèle, la valeur de l'incertitude est égale à 1, et les valeurs de confiance positive et négative sont égales à zéro. Cette catégorie de modèle se comporte à peu près de la même manière que le modèle bayésien. Sauf que, pour un utilisateur qui n'est pas sûr de la valeur de confiance à donner après une interaction avec un autre utilisateur, il lui donne le droit de fixer la valeur d'incertitude.

5.5.3 Modèles à valeur discrète

Les modèles de valeurs discrètes permettent, comme mentionné ci-dessus, d'évaluer les performances sous la forme de déclarations verbales discrètes au lieu de mesures continues. Ce modèle de calcul utilise quatre degrés de confiance verbaux : « très douteux (td), douteux (d), fiable (f), très fiable (tf) ». L'utilisateur U_1 fait confiance à l'utilisateur U_2 avec une valeur :

$$C(U_1, U_2) = f(nb_{td}, nb_d, nb_f, nb_{tf}) \quad (5.2)$$

La valeur de confiance d'un nouvel utilisateur est égale à zéro. Comme ce modèle n'utilise pas de fonction de probabilité spécifique, le choix de la fonction appropriée dépend des besoins du système. Deux types de fonctions, soit une fonction maximale ou minimale, sont généralement utilisées dans cette situation. Par exemple, lorsque les besoins exigent un système pénalisant, si $nb_{td} = nb_f$, on prend le degré le plus bas (très douteux), et vice versa. Donc pour utiliser ce modèle, il faut le paramétrer en fonction de nos besoins (c'est-à-dire si on veut un système optimiste (tolérant) ou pessimiste (punitif)).

5.5.4 Modèles flous

Les modèles flous représentent la confiance ou la réputation comme des concepts linguistiques flous. Ils décrivent la fiabilité d'un utilisateur en formalisant des règles basées

sur des mesures floues. Dans ce type de modèles, la réputation est un concept multidimensionnel. Elle accepte une dimension individuelle, sociale et ontologique. Dans l'environnement, les utilisateurs peuvent coopérer, être en concurrence ou échanger.

- **Dimension individuelle** : il s'agit de l'expérience directe entre deux utilisateurs. Par exemple, un contrat entre deux utilisateurs est défini par le prix, la qualité et la date de livraison d'un produit. La confiance est modélisée en fonction de la différence entre le contrat initial et les résultats de la vente. Cette différence va permettre de classer l'utilisateur cible dans une catégorie, par exemple, la catégorie « Livre en retard ».
- **Dimension sociale** : l'utilisateur utilise des cookies qui ont déjà un score de réputation pour l'utilisateur cible ou ses voisins. Cette dimension utilise des règles floues. En fonction de la relation du témoin avec la cible et du degré de cette relation, l'utilisateur attribue un degré de croyance à l'information fournie par le témoin ou le voisin. Par exemple, si le témoin coopère fortement avec l'utilisateur cible, alors l'information du témoin est très mauvaise.
- **Dimension ontologique** : combine la réputation de différents aspects afin de calculer une réputation complexe. Par exemple, placer l'utilisateur cible dans une nouvelle catégorie qui est une combinaison de deux catégories.

Ce type de modèle de calcul ne peut pas être utilisé avec les scénarios mentionnés ci-dessus. Puisqu'il s'agit plutôt d'un modèle de représentation et non d'une méthode de calcul.

5.5.5 Modèles de flux

Les modèles de flux calculent les valeurs de confiance ou de réputation par itérations transitives à travers des chaînes en boucle. Les valeurs résultant de la procédure de calcul de ces modèles appartiennent à l'intervalle $[0,1]$. Ce modèle n'a pas d'incidence sur la valeur initiale pour les nouveaux utilisateurs, comme dans le système PageRank de Google. Pour construire une réputation solide, il faut commencer à détecter les flux de confiance entrants. L'avantage ici est que les méthodes d'estimation des flux de données mettent rapidement à jour les valeurs estimées à chaque fois qu'un nouveau flux est détecté. Dans le cas de la fraude, la machine détecte explicitement une série d'actions malveillants. Cette

forme de méthode punitive aide au contrôle de la fraude. La limite de cette technique est qu'une valeur neutre de confiance ou de réputation est égale à zéro, ce qui peut être considéré comme pénalisant.

5.5.6 Synthèse

TABLEAU 5.2 – Synthèse de notre analyse

| Type du modèle Computationnel | Fonction Mathématique | Tolérant | Punitif |
|----------------------------------|--------------------------|----------|---------|
| Modèles Bayésiens | Probabilité | ✓ | |
| Modèles basés sur les croyances | Probabilité | ✓ | |
| Modèles à valeur discrète | Maximum / Minimum | ✓ | ✓ |
| Modèles flous | N/A | N/A | N/A |
| Modèles de flux | Itérations transitives | | ✓ |

Dans cette section, nous avons étudié les modèles computationnels de confiance pour comprendre l'intuition derrière chaque modèle, c'est-à-dire comment le modèle se comporte face aux actions malveillantes des utilisateurs, est-il punitif ou tolérant (voir Tableau 5.2). Cela nous permettra de choisir le modèle le plus adéquat en fonction des besoins de notre application décrits dans la section 5.4.

Dans les systèmes informatiques d'aujourd'hui, la confiance et la réputation sont deux principes qui sont devenus très importants. Comme il y a beaucoup de travaux qui ont discuté de ces concepts dans la littérature, cela conduit à une variété de descriptions. D'une part, pour ces définitions, nous avons proposé une formalisation globale graphique et textuelle. D'autre part, à notre connaissance, il existe peu de travaux qui clarifient le type de modélisation de la confiance et de la réputation qu'ils utilisent. Cela rend leur utilisation dans les applications compliquée. C'est pourquoi il sera plus facile de choisir le modèle à adapter, si nous définissons les spécifications du système dès le début.

Pour aller plus loin dans l'analyse des modèles computationnels par rapport aux besoins applicatifs identifiés, nous proposons dans la section suivante une mise en oeuvre expérimentale.

5.6 Expérimentations et Résultats

Comme mentionné ci-dessus, ce travail est réalisé dans le but d'évaluer les situations problématiques existantes dans le domaine de l'informatique, en particulier en ce qui concerne les problèmes liés aux modèles de confiance et de réputation computationnels. Il convient de mentionner que, depuis l'apparition de ce domaine, plusieurs travaux ont été développés pour proposer des solutions aux difficultés rencontrées. Dans cette section, nous avons essayé d'appliquer les différents exigences décrits dans la section 5.4 aux différents types de modèles computationnels. L'objectif de ces expériences est de valider les descriptions fournies dans la section 5.5 pour le choix des modèles. Pour chaque modèle, l'idée est de faire plusieurs types de transactions et d'essayer de voir comment il peut réagir. Nous symbolisons les bonnes transactions par la lettre B, et les mauvaises ou malveillantes par la lettre M.

5.6.1 Besoin B_1 : « Bon utilisateur vs. Mauvais utilisateur »

La première expérience a été réalisée afin d'observer l'effet des bons et mauvais comportements sur l'évolution de la confiance. Nous constatons sur la figure 5.12 que pour tous les modèles testés, ce critère est confirmé. Il est tout à fait raisonnable. Une bonne crédibilité se gagne par de bonnes pratiques, comme dans la vie réelle, et se perd par des actions inappropriées.

5.6.2 Besoin B_2 : « Un nouvel utilisateur vs. un utilisateur avec comportement mi-positif mi-négatif »

Le deuxième scénario, mentionné précédemment, consiste à observer comment le système se comporte avec un nouvel utilisateur et un autre qui a un équilibre entre ses transactions positives et négatives, comme le montre la figure 5.13. On constate qu'il n'y a pas de différence entre les deux utilisateurs pour le modèle bayésien et le modèle basé sur les croyances, ce qui n'est pas avantageux. On peut remarquer que cela dépend de la loi de distribution de probabilité utilisée. Nous avons expérimenté ici le modèle de Josang [CJI02] qui utilise la loi de distribution bêta. Cette loi calcule la différence entre le nombre d'actions positives et négatives. Elle tend vers zéro lorsque les deux nombres sont égaux. Les modèles de flux, quant à eux, prennent en compte ce scénario. Car dans ce modèle, un

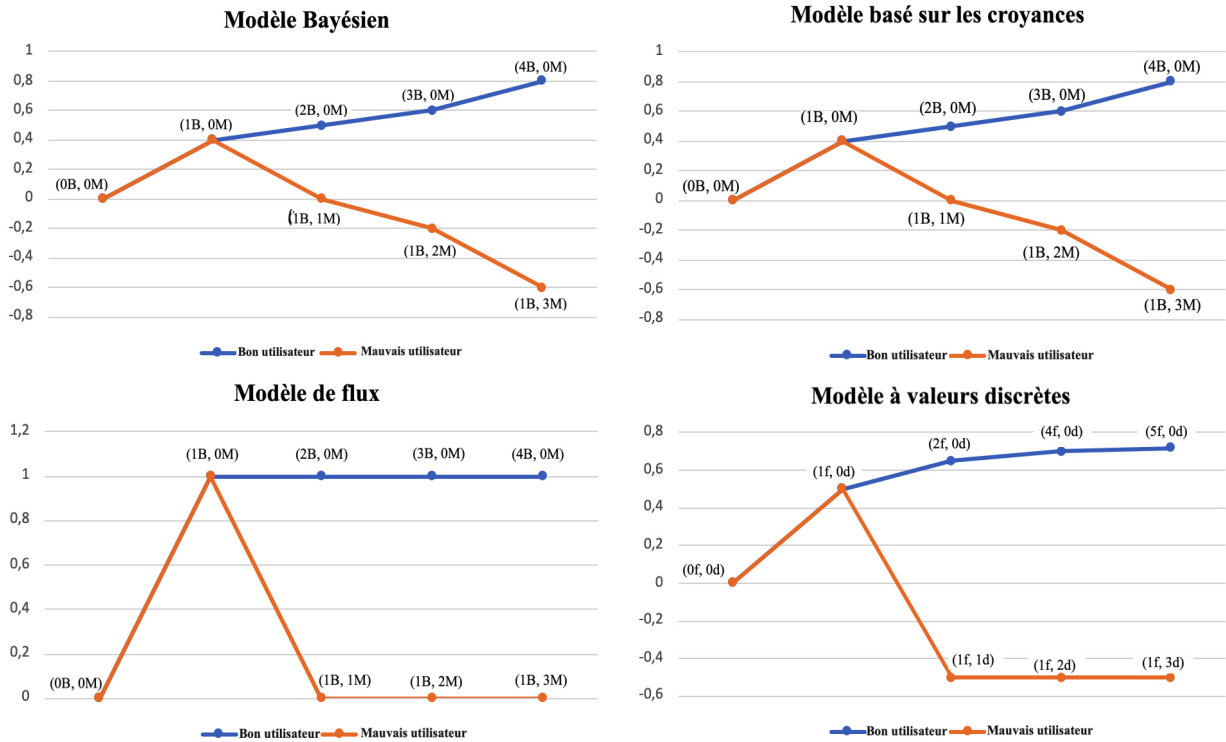


FIGURE 5.12 – Bon utilisateur vs. Mauvais utilisateur

nouvel utilisateur ne peut avoir une valeur de réputation avant d'avoir obtenu au moins un flux entrant. C'est le cas pour le modèle à valeur discrète. Ce critère peut être résolu avec une confiance neutre pour un nouvel utilisateur et la possibilité de mesurer une confiance inférieure à zéro pour un autre utilisateur.

5.6.3 Besoin B_3 : « Le système se souvient des fraudes »

Un bon modèle computationnel doit faire la distinction entre deux utilisateurs qui ont le même nombre d'actions. Le premier n'a que de bonnes actions, tandis que le second a quelques mauvaises actions. Ce critère est pris en compte par le modèle à valeurs discrètes et un peu moins par le modèle de flux, comme le montre la figure 5.14. Cela est dû aux processus utilisés pour modifier les valeurs ainsi qu'à la possibilité que les mauvaises actions soient prises en compte dans les fonctions de calcul.

5.6.4 Besoin B_4 : « Récidivisme »

La récidive doit être abordée avec un paradigme fort de confiance et de réputation. Si un utilisateur fait une bonne action, puis une mauvaise action, puis une bonne action, il

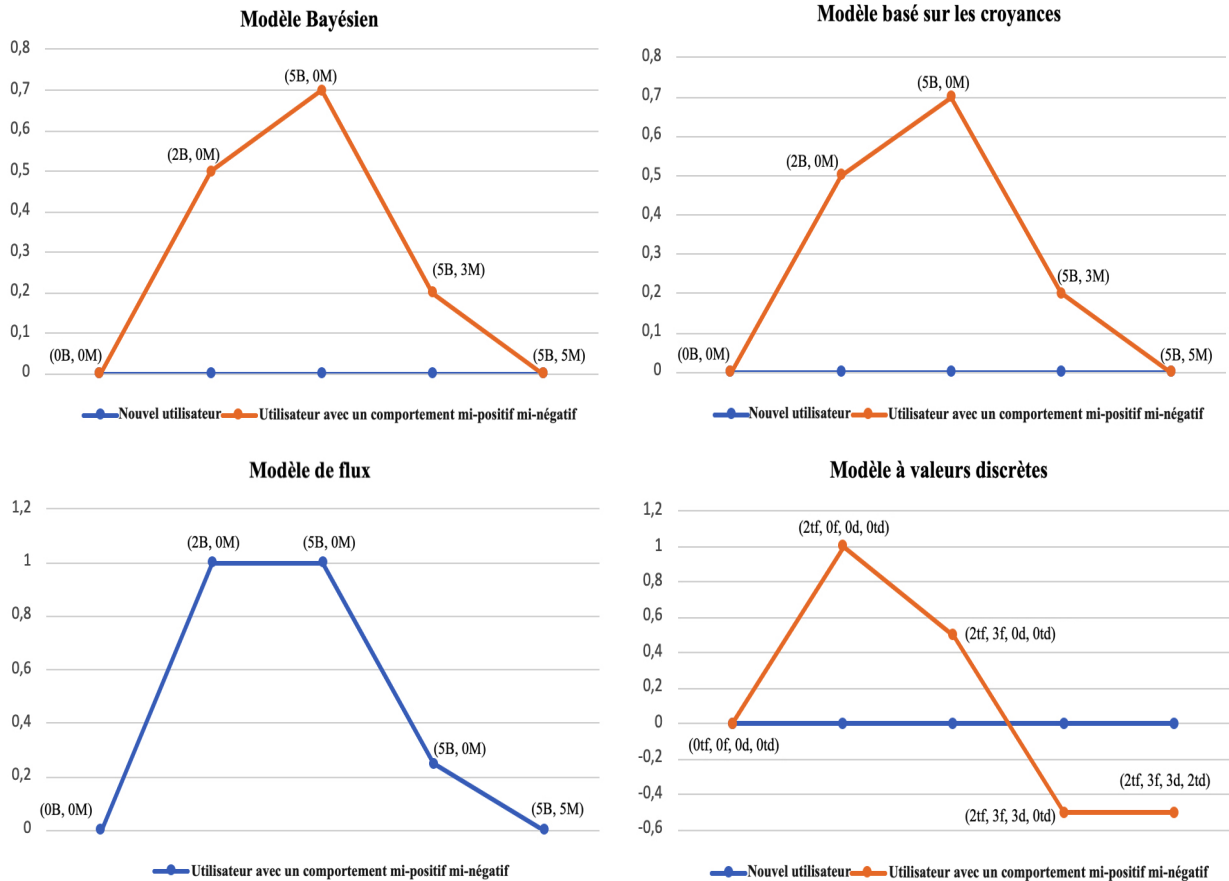


FIGURE 5.13 – Un nouvel utilisateur vs. un utilisateur avec comportement mi-positif mi-négatif

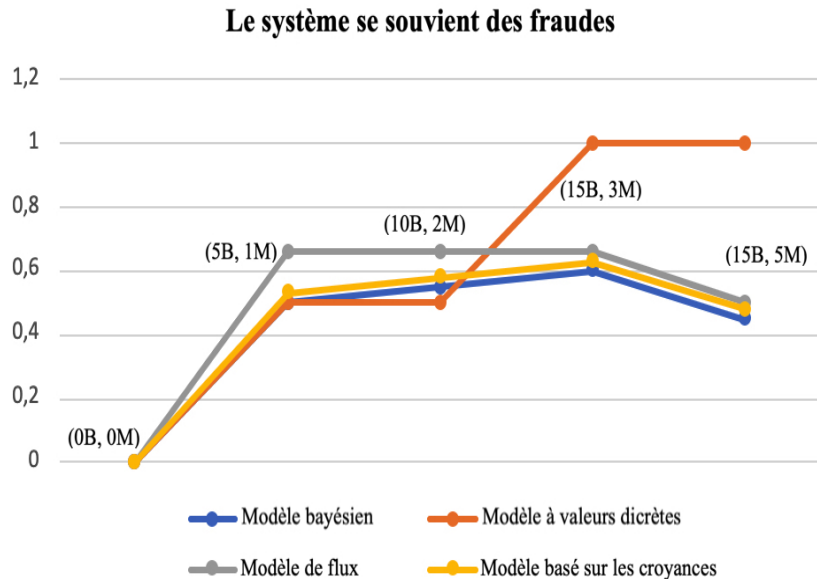


FIGURE 5.14 – Le système se souvient des fraudes

recupérera une partie, mais pas la totalité, de sa réputation. Il doit perdre une partie de sa fiabilité chaque fois qu'il répète cette série d'actions. Tous les modèles, à l'exception

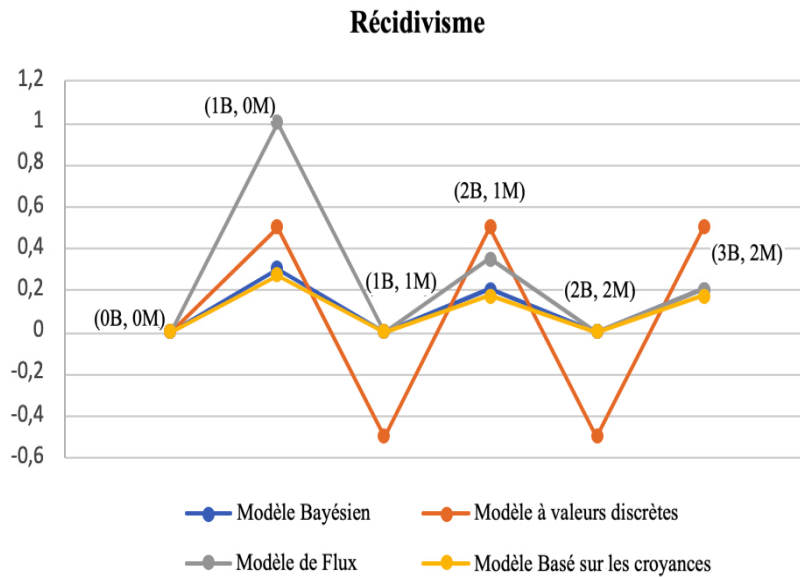


FIGURE 5.15 – Récidivisme

du modèle à valeur discrète, valident ce scénario comme le montre la figure 5.15.

5.6.5 Besoin B_5 : « Droit à l'erreur »

Il arrive que dans ses interactions, un utilisateur fasse une erreur. Les modèles qui utilisent des fonctions de probabilité et de récursivité sont capables de gérer ce problème. Comme le montre la figure 5.16, le raffinement des valeurs déterminées après une ou un maximum de deux erreurs aidera l'utilisateur à récupérer la confiance perdue. Comme les fonctions de calcul maximum et minimum sont utilisées par les systèmes de valeurs discrètes, cela ne peut pas être très utile pour récupérer les taux perdus.

5.6.6 Besoin B_6 : « Vol d'identité »

Comme nous pouvons le voir sur la figure 5.17, seul le modèle de flux peut bien réagir à une fraude impliquant un vol d'identité. Cela est dû aux fonctions de récursion utilisées pour chaque détection de flux, qui permettent de réévaluer rapidement les taux de valeur de confiance et de réputation. Le modèle bayésien et le modèle basé sur les croyances sont également disposés, mais après de nombreuses opérations de mise à jour, à détecter les cas de vol ou de fraude. Nous pouvons remarquer que le modèle bayésien et le modèle basé sur les croyances se comportent presque de la même manière. La distinction réside dans la forme du calcul, qui prend trois paramètres au lieu de deux pour le deuxième modèle.

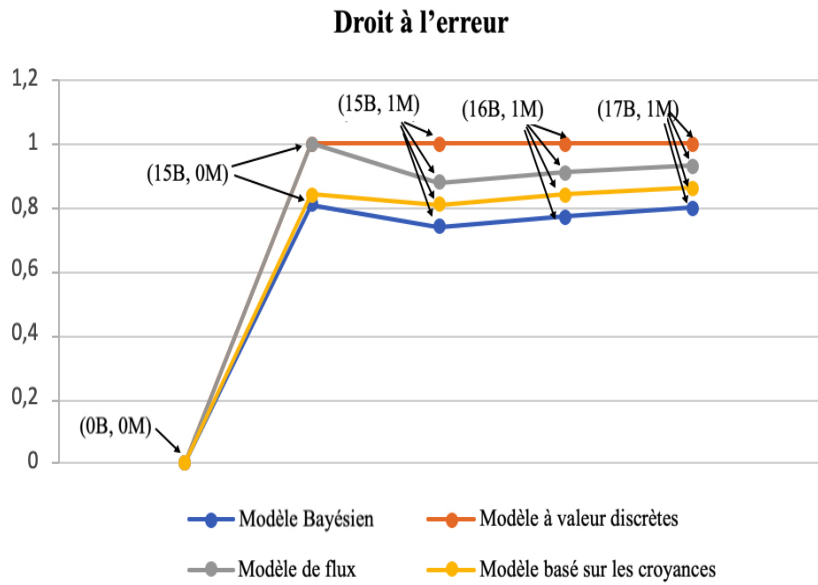


FIGURE 5.16 – Droit à l'erreur

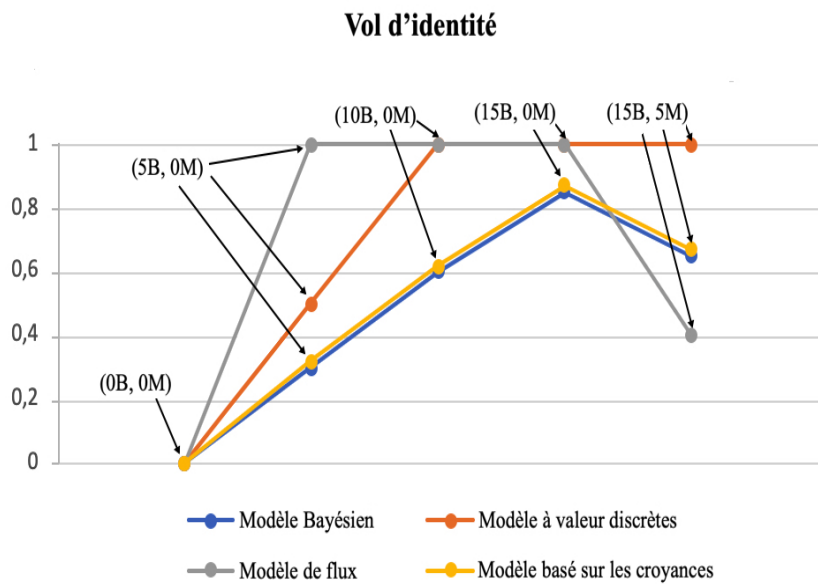


FIGURE 5.17 – Vol d'identité

Cela laisse le choix à l'utilisateur de montrer son incertitude, comme le montre le tableau 5.3. Dans le tableau 5.4, un résumé de tous ces résultats est donné.

TABLEAU 5.3 – Incertitude dans le modèle basé sur les croyances

| | 0B,0M | 5B,0M | 10B,0M | 15B,0M | 15B,5M |
|--------------------|-------|-------|--------|--------|--------|
| Confiance positive | 0 | 0,3 | 0,6 | 0,85 | 0,65 |
| Confiance négative | 0 | 0 | 0 | 0 | 0,2 |
| Incertitude | 1 | 0,7 | 0,4 | 0,15 | 0,15 |

| Type du modèle | B_1 | B_2 | B_3 | B_4 | B_5 | B_6 |
|---------------------------------|-------|-------|-------|-------|-------|-------|
| Modèles Bayésiens | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Modèles basés sur les croyances | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| Modèles à valeurs discrètes | ✓✓ | ✓ | × | × | × | × |
| Modèles flous | × | × | × | × | × | × |
| Modèles de flux | ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ ✓ |

TABLEAU 5.4 – Résumé des comportements des modèles computationnels

L'analyse expérimentale que nous avons faite permet donc de savoir quels modèles computationnels respectent les critères applicatifs que nous avons définis. Nous irons plus loin dans le chapitre suivant car le problème est que les critères applicatifs évoluent avec les nouveaux besoins et marchés de l'entreprise. Cette analyse n'est donc pas suffisante.

5.7 Conclusion

Dans ce chapitre, nous avons abordé le problème des modèles computationnels de la confiance et de la réputation. En raison des nombreuses études réalisées dans la littérature sur ces deux concepts, nous avons proposé une formalisation unifiée de ces derniers pour les besoins de la recommandation. En particulier, nous avons révisé leurs définitions et reformulé leurs propriétés de base. Cela permet de comprendre le comportement et l'intuition derrière chaque modèle de calcul. Un ensemble d'exigences a été établi pour rendre le choix du modèle plus pratique et plus intelligent, dans le sens où il répond aux besoins souhaités. Il faut noter que ce sont nos propositions d'exigences d'application que nous avons mis selon les besoins de l'entreprise et avons vu qu'elles sont indispensables pour chaque système. Elles peuvent varier d'un système à l'autre et nous pouvons recréer les spécifications associées pour chaque application. Notre idée était de comparer et de proposer une nouvelle

classification des types de modèles de calcul existant dans la littérature. Cela permet de sélectionner le modèle de calcul approprié pour une application si nécessaire. Cette idée nous ramène à chercher les exigences liés à la confiance dans la littérature, comment les modéliser pour comprendre le comportement des utilisateurs et comment recommander le modèle computationnel le plus adéquat selon les besoins de l'application. Les expériences réalisées montrent que notre proposition d'exigences aide à différencier les différents modèles et à sélectionner les plus appropriés en fonction des besoins. Ce travail constitue notre premier pas vers un nouveau modèle général de confiance/réputation qui peut s'adapter au contexte de chaque application. Cependant, cette étude n'est pas suffisante puisque les besoins de l'entreprise peut évoluer selon les nouveaux marchés obtenus. En plus de la comparaison « statique » des modèles computationnels que nous avons proposée dans cette section, nous avons besoin de pouvoir comparer « dynamiquement » ces systèmes en fonction de besoin définie à la volée par un concepteur d'application. Le prochain chapitre présente notre proposition pour répondre à cette problématique.

Chapitre 6

Recommandation du modèle computationnel de confiance : une approche guidée par les besoins métiers

Sommaire

| | | |
|------------|---|------------|
| 6.1 | Introduction | 124 |
| 6.2 | Exemple pour illustrer la contribution | 125 |
| 6.3 | Analyse de l'état de l'art par rapport aux besoins métiers | 126 |
| 6.3.1 | Analyse des travaux d'évaluation des modèles computationnels | 126 |
| 6.3.2 | Analyse des besoins applicatifs pour l'évaluation des modèles computationnels | 127 |
| 6.4 | Approche de sélection du modèle computationnel | 128 |
| 6.4.1 | Modélisation des exigences de l'application | 129 |
| 6.4.2 | Modélisation des exigences sur l'évolution de la confiance | 132 |
| 6.4.2.1 | Formalisme graphique et textuelle | 134 |
| 6.4.2.2 | Opérateurs de décomposition | 135 |
| 6.4.2.3 | Contraintes | 136 |
| 6.4.2.4 | Instanciation des exigences de la confiance | 136 |
| 6.4.3 | Recommandation du modèle computationnel de la confiance | 139 |
| 6.5 | Étude de cas | 140 |
| 6.5.1 | Exigences pour l'application de covoiturage | 140 |
| 6.5.2 | Exigences de confiance pour le covoiturage | 141 |

| | | |
|------------|--|------------|
| 6.5.3 | Recommandation du modèle computationnel de confiance . . . | 143 |
| 6.6 | Conclusion et Perspectives | 145 |

6.1 Introduction

Dans le chapitre précédent, nous avons proposé une définition et formalisation des concepts liés à la notion de confiance. Cette formalisation nous a permis d'analyser et de comprendre l'intuition derrière chaque modèle. Cette intuition est liée à un ensemble d'exigences qui décrivent les besoins de chaque application. L'analyse et la modélisation de ses besoins permettent de les lier aux modèles computationnels étudiés et de recommander le modèle le plus approprié selon chaque application communautaire.

L'étude proposée dans le chapitre précédent s'est basée sur des besoins en terme d'évolution de la confiance définis par l'entreprise O°Code. Cependant, ces besoins peuvent être amenés à évoluer, d'une part, et, l'entreprise O°Code prévoit d'étendre son activité à de nouveaux domaines pour lesquels de nouveaux besoins pourront apparaître, d'autre part. Il est nécessaire d'aller plus loin dans ce que nous avons proposé pour sélectionner un modèle computationnel.

Nous proposons donc, dans ce chapitre, une approche permettant de modéliser les besoins en terme d'évolution de la confiance et de sélectionner un modèle computationnel répondant à ces besoins. L'approche présentée dans le chapitre précédent peut donc être vue comme une approche statique de sélection d'un modèle computationnel quand les besoins sont connus et non évolutifs. L'approche proposée dans ce chapitre est dynamique, puisqu'elle est basée sur des besoins définis à la volée par le concepteur d'une application.

Notre contribution est divisée en trois étapes. La première étape de notre approche vise à aider l'utilisateur à définir les attentes de son système cible, et à être capable de modéliser ces exigences. La deuxième étape se concentre sur la modélisation de la séquence des actions de l'utilisateur au sein du système et sur la manière dont l'utilisateur souhaite que la confiance évolue dans le système. Quant à la troisième étape de ce travail, et à partir des résultats des deux premières étapes, elle traite la question liée à la sélection du modèle computationnel le plus adéquat en fonction des exigences de l'utilisateur.

Nous avons publié ce travail dans l'article [Sel+22] qui a été présenté à la conférence internationale sur les défis de la recherche en sciences de l'information.

Le reste du chapitre est composé comme suit : la section 6.2 présente un exemple motivant tiré d'applications du monde réel qui sera utilisé tout au long du travail. La section 6.3 décrit brièvement l'état de l'art qui contextualise notre travail. La section 6.4 discute des différentes étapes de notre approche pour la modélisation des exigences de confiance afin d'aider l'utilisateur de systèmes basés sur la confiance à choisir le modèle computationnel le plus adapté à ses besoins. Pour valider notre proposition, nous fournissons dans la section 6.5 une étude de cas complète avec des exemples concrets, couvrant tous les aspects de la contribution et montrant sa faisabilité technique. Enfin, les points à retenir et les perspectives sont présentés dans la section 6.6.

6.2 Exemple pour illustrer la contribution

Dans cette section, nous présentons un exemple d'application basée sur la confiance que nous utilisons tout au long du chapitre. Plusieurs systèmes basés sur la confiance ont été développés. Il existe des systèmes de location de logements, des systèmes de covoiturage, des systèmes d'échange de biens et de services, etc.

Pour illustrer nos idées, prenons l'exemple d'un système de covoiturage, inspiré du système Blablacar¹. Des systèmes dans d'autres domaines pourraient être considérés et la même approche s'appliquerait. Le principe du covoiturage est de partager un trajet entre un conducteur qui dispose de places libres avec des passagers qui se rendent à la même destination et qui ne se connaissent pas. Il y a donc deux types de membres dans ce type d'application : le conducteur et les passagers. Après avoir effectué le voyage, les membres peuvent laisser des notes. Le principe de la notation consiste à évaluer la performance sous forme d'énoncés verbaux discrets (Excellent, Bon, Correct, Décevant, Très décevant). Le conducteur peut noter le passager pour l'évaluer et le recommander à la communauté de l'application. Le passager peut également noter le conducteur pour évaluer son expérience de covoiturage avec lui et le recommander aussi. Un passager ne peut pas noter un autre passager. Ce principe introduit le concept de confiance qui est l'un des piliers de la communauté de covoiturage. Cela permet à un membre de la communauté de décider de covoiturer avec une personne qu'il ne connaît pas.

À partir des avis laissés pour chaque profil, les membres sont en mesure d'accumuler un

1. <https://www.blablacar.fr/>

« capital confiance », qui résulte de la combinaison des différentes évaluations données au cours de la séquence d'interactions. Ce capital peut augmenter si l'évaluation est positive ou diminuer si elle est négative [Maz15].

Par conséquent, la première priorité est de savoir comment calculer la valeur actuelle de ce capital ? En général, les systèmes basés sur la confiance ne divulguent pas les algorithmes utilisés et leurs méthodes de calcul. Mais comme ils évaluent la confiance qui peut être accordé à chaque utilisateur, on peut supposer qu'il existe des modèles computationnels pour faire cette évaluation. Nous considérons le cas où le concepteur d'une application de covoiturage doit choisir un modèle computationnel existant.

Prenons l'exemple d'un concepteur d'applications qui souhaite que la confiance dans son système soit calculée selon un certain nombre de principes (par exemple, « évolution douce »). Il est alors confronté à un grand nombre de modèles computationnels possibles. Choisir le ou les modèles adéquats selon ses besoins applicatifs est une tâche difficile qui nécessite de maîtriser chacun des modèles computationnels. Dans le cadre industriel de cette thèse, nous considérons que cette hypothèse ne peut pas être faite. Il est donc nécessaire d'aider le concepteur d'une application à définir ses besoins applicatifs en terme d'évolution de la confiance et à sélectionner le ou les modèles computationnels adaptés à ces besoins. C'est ce type de questions que nous abordons dans ce chapitre. Commençons par discuter de l'état de l'art lié à notre travail dans la section suivante.

6.3 Analyse de l'état de l'art par rapport aux besoins métiers

Dans cette section, nous présentons quelques travaux de recherche qui ont été effectués dans le contexte de l'évaluation des modèles de confiance informatiques. Un ensemble de critères a été proposé dans la littérature qu'un bon système de confiance devrait satisfaire.

6.3.1 Analyse des travaux d'évaluation des modèles computationnels

De nombreux chercheurs ont proposé des modèles pour représenter et calculer la confiance dans les systèmes informatiques [Bra+18]. Ces modèles peuvent être classés en cinq catégories : modèles bayésiens, modèles basés sur les croyances, modèles à valeurs discrètes, modèles flous et modèles de flux.

Cependant, le choix du modèle computationnel qui répond le mieux aux exigences de l'utilisateur est difficile en raison de la variété des modèles computationnels disponibles dans la littérature.

Certains travaux ont été proposés pour évaluer et comparer les modèles computationnels, voir par exemple [KT15; Ora01]. Dans [KT15], les auteurs ont inspecté de manière approfondie les composants d'évaluation accessibles dans la littérature. L'objectif de cet article est de fournir aux analystes des pistes pour choisir un mécanisme d'évaluation et un outil de simulation raisonnables, d'une part, et pour élaborer un système d'évaluation commun, d'autre part.

6.3.2 Analyse des besoins applicatifs pour l'évaluation des modèles computationnels

Le travail de [Ora01] présente une série de critères auxquels un bon système d'évaluation devrait répondre.

- *Précis pour la performance à long terme*, c'est-à-dire que le système peut faire la différence entre une substance inutilisée de qualité inconnue et une substance ayant une mauvaise performance à long terme.
- *Pondéré en fonction du comportement actuel*, c'est-à-dire que le système reconnaît et reflète les tendances ultérieures de la performance de la substance.
- *Efficace*, c'est-à-dire qu'il est pratique dans le cas où le système peut recalculer un score rapidement.
- *Robuste contre les attaques*, c'est-à-dire que le système devrait résister aux tentatives de toute substance d'influencer les scores autrement qu'en étant plus honnête ou en ayant une meilleure réputation.
- *Apte à l'évaluation statistique*, c'est-à-dire qu'il doit être simple de découvrir les exceptions et autres composants qui peuvent faire que le système évalue les scores d'une manière inattendue.
- *Confidentiel*, c'est-à-dire que personne ne devrait pouvoir mémoriser la façon dont un évaluateur donné a évalué une substance, sauf l'évaluateur lui-même.
- *Flexible*, c'est-à-dire que l'inclusion d'une seule note d'évaluation ne fait pas trop varier le score.

-
- *Compréhensible*, c'est-à-dire qu'il doit être simple de clarifier pour les utilisateurs qui se servent de ces modèles ce qui signifient les scores données.
 - *Vérifiable*, c'est-à-dire qu'une note inférieure au débat peut être étayée par des informations.

Un bon système de notation devrait répondre aux qualités mentionnées ci-dessus. Contrairement à ces études, notre objectif dans ce travail est de proposer une approche pour savoir quels modèles computationnels remplissent un ensemble d'exigences liées au calcul de la confiance. Les études existantes peuvent être considérées comme une comparaison statique des modèles computationnels alors que l'approche que nous proposons fait une comparaison dynamique dirigée par les exigences du concepteur.

6.4 Approche de sélection du modèle computationnel

Afin de gérer et de calculer la confiance, les systèmes informatiques utilisent des modèles de calcul appelés des modèles computationnels. Dans ce travail, notre objectif est de fournir une approche pour modéliser les exigences de confiance afin d'aider les utilisateurs de ces systèmes à choisir le modèle computationnel le plus adéquat pour leurs besoins. Notre approche consiste en trois étapes, comme le montre la Figure 6.1.

- La première étape consiste à construire un modèle pour exprimer les exigences de l'application du système cible. Dans le cadre de ce travail, nous avons pris le covoiturage comme exemple d'exigence applicative. Cela nous permettra de classer les différents types d'actions qui peuvent être effectuées par les utilisateurs au sein du système.
- La deuxième étape porte sur le modèle des exigences de confiance. Cela nous permettra de modéliser la chaîne des actions définies et d'appliquer des contraintes sur la valeur de confiance souhaitée. Par exemple, après un seul covoiturage, un souhait souhaitable est l'évolution douce de la confiance c'est-à-dire que la valeur de confiance évolue de manière graduelle.
- La troisième étape consiste à évaluer un modèle computationnel de la confiance par rapport aux deux modèles définis aux étapes 1 et 2. Les modèles computationnels seront utilisés pour calculer le score, le comparer aux contraintes définies et recommander le modèle le mieux adapté aux exigences.

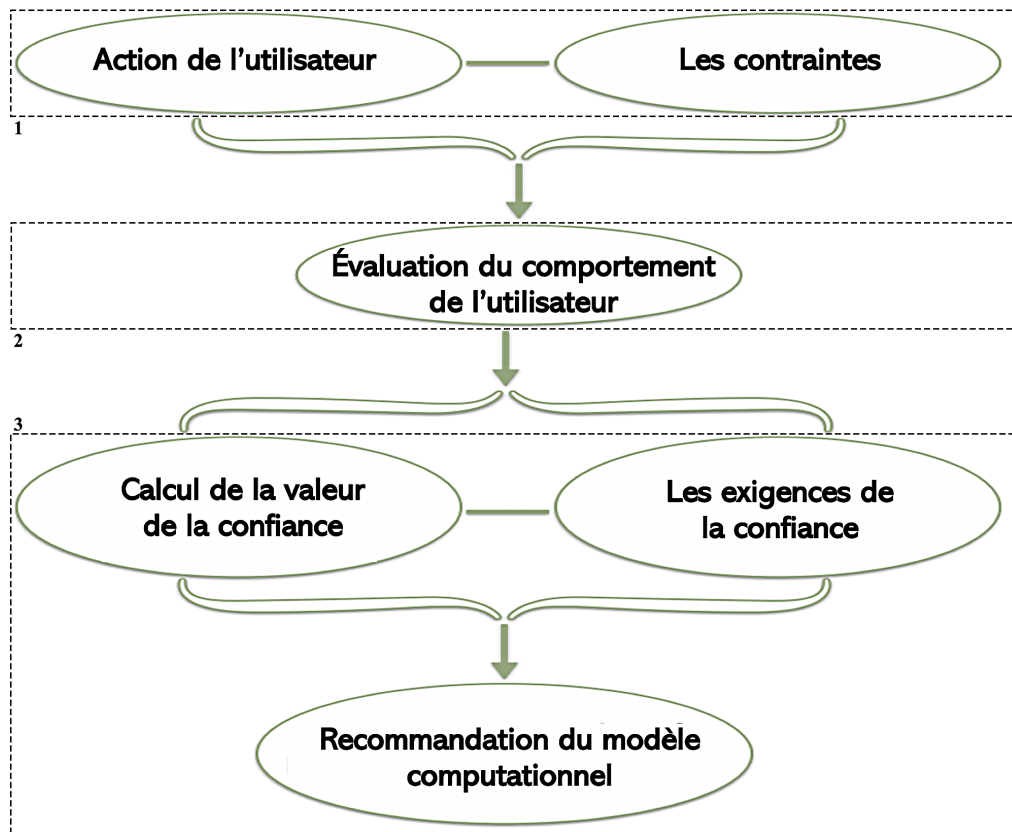


FIGURE 6.1 – La méthodologie de notre approche

L'exemple défini dans la section 6.2 sera utilisé dans cette section pour illustrer nos contributions, mais une expérimentation plus complète sera faite dans la section 6.5.

6.4.1 Modélisation des exigences de l'application

Dans cette section, nous aborderons la première étape de notre approche, qui définit les différents types d'actions d'un système en fonction des exigences de l'application.

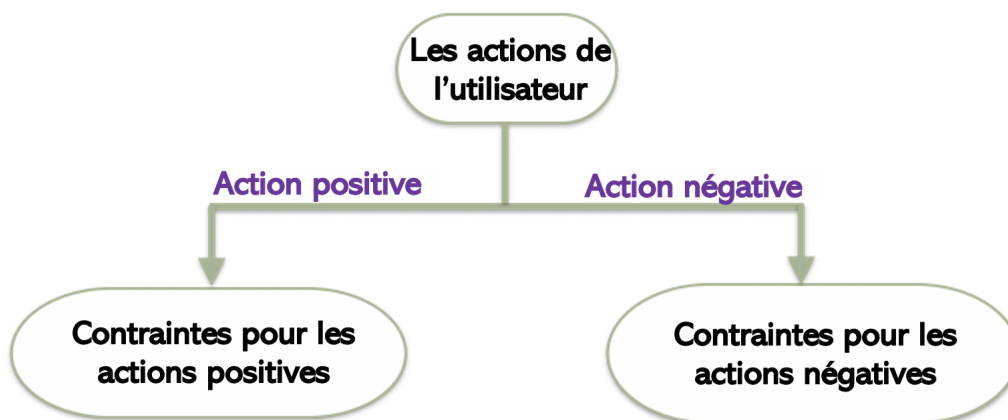


FIGURE 6.2 – Modélisation des actions de l'utilisateur

La priorité des systèmes basés sur la confiance est d'assurer la sécurité de l'utilisateur qui interagit avec le système. Par conséquent, chaque utilisateur est caractérisé par une

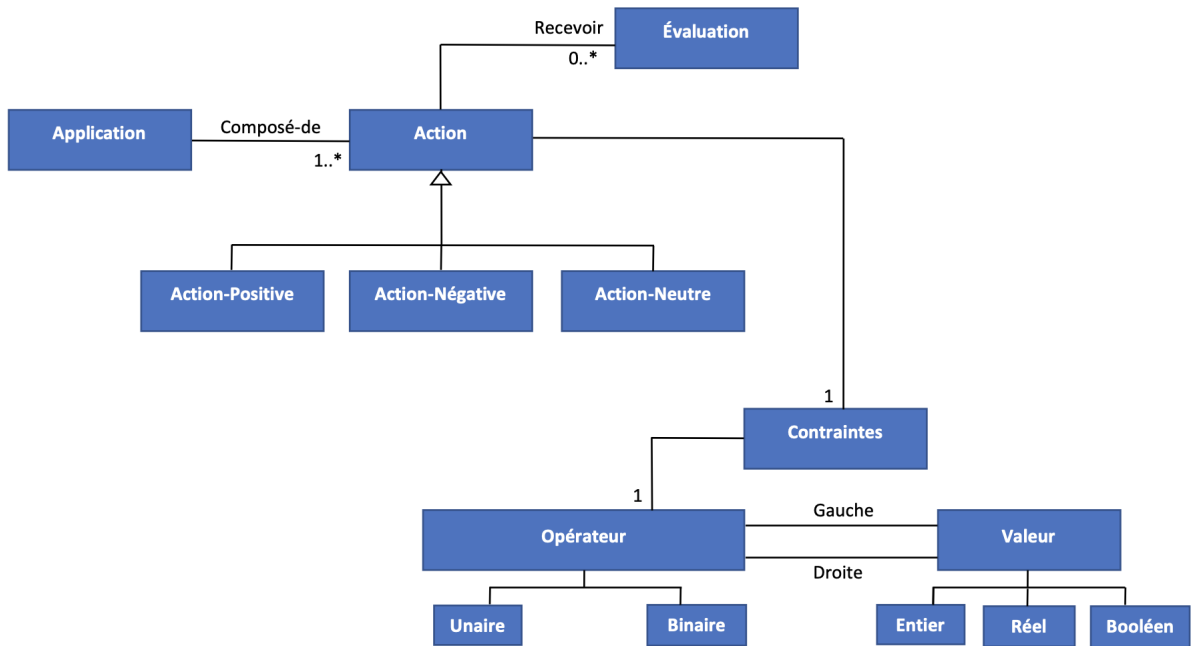


FIGURE 6.3 – Modélisation des exigences de l’application

estimation de sa réputation sur laquelle sont basés les choix de coopération. Cette estimation est calculée à partir des actions effectuées par l’utilisateur. Un utilisateur ayant un bon comportement aura une bonne valeur de réputation. Alors qu’un utilisateur nocif aura une mauvaise valeur de réputation. Par conséquent, afin de reconnaître un bon utilisateur d’un mauvais, il est important de reconnaître dès le départ les différents types d’actions qu’ils peuvent faire. Le premier objectif consiste à déterminer si une action est positive ou négative. Pour donner une description plus précise de ces deux types d’action, la figure 6.2 montre le résumé de cette étape. Si l’action effectuée par l’utilisateur satisfait aux contraintes définies pour les actions positives, le système considère que cet utilisateur a effectué un bon comportement. En contrepartie, une action qui satisfait les contraintes d’une action négative, permet au système d’enregistrer un comportement négatif.

Comme nous pouvons le voir sur la Figure 6.3, chaque action dans le système est liée à une évaluation à partir de laquelle nous pouvons connaître le type d’action. En fait, chaque action dans le système est évaluée par les autres utilisateurs impliqués dans l’interaction. En fonction de la valeur de cette évaluation, le système peut distinguer si l’utilisateur a fait une action positive pour augmenter sa valeur de réputation, ou une action négative pour la diminuer. Un utilisateur peut également effectuer des actions neutres qui n’ont pas d’impact sur la valeur de sa réputation (par exemple, s’inscrire, naviguer dans le système, etc.). En général, ces actions dépendent du contexte dans lequel elles ont été effectuées.

TABLEAU 6.1 – Association des valeurs continues aux évaluations.

| Très décevant | Décevant | Correct | Bon | Excellent |
|---------------|----------|---------|-----|-----------|
| -1 | -0,5 | 0 | 0,5 | 1 |

Ce contexte représente les exigences de l'application du système.

Prenons l'exemple décrit dans la section 6.2. Dans un système de covoiturage, après avoir effectué un trajet, les membres participants sont invités à formuler des commentaires pour évaluer l'expérience. L'évaluateur peut choisir entre différents niveaux d'évaluation. S'il trouve que le voyage s'est bien passé et recommande cet utilisateur à la communauté du système, il peut donner un avis entre « Bon » et « Excellent ». En conséquence, le système considère que l'utilisateur évalué a fait une action positive. Dans le cas contraire, l'évaluateur peut donner un avis « Décevant » ou « Très décevant », s'il n'est pas satisfait de l'expérience. Dans ce cas, le système note que l'utilisateur évalué a effectué une action négative.

Comme nous pouvons le constater, ces systèmes utilisent des énoncés linguistiques. Afin de modéliser cet exemple avec notre proposition de modélisation, nous devons nous appuyer sur des évaluations continues. Une idée est d'associer des valeurs continues à ces évaluations afin qu'elles puissent également être utilisées ultérieurement avec les modèles computationnels.

Comme le montre le tableau 6.1, le système utilise quatre niveaux de confiance : « Excellent, Bon, Correct, Décevant, Très décevant » qui pourrait correspondre à « 1, 0,5, 0, -0,5, -1 ».

Pour instancier notre modèle, nous prenons l'exemple décrit dans la section 6.2 :

#1 = *Application* ('Blablacar')

#2 = *Action* ('Covoiturage')

#3 = *Évaluation* (0.5)

#4 = *Action – Positive* ('Évaluation > 0')

#5 = *Action – Négative* ('Évaluation < 0')

#6 = *Action – Neutre* ('Évaluation = 0')

#7 = *Contraintes* ((#3, #10, #12))

#8 = *Opérateur* ((#9, #10))

#9 = *Unaire* ('+', '-')

#10 = *Binnaire* ('<', '>', '=', '<=', '>=')

#11 = *Valeur* ((#12, #13, #14))

#12 = *Valeur* (0)

#13 = *Valeur* (*Réel*)

#14 = *Valeur* (*Booléenne*)

Comme nous pouvons le voir, un utilisateur a fait une expérience de covoiturage et a reçu une évaluation qui est égale à 0,5 (avec le vocabulaire de l'application, cette expérience est considérée comme « Bonne »). Le système va comparer cette évaluation à une valeur exacte qui est zéro « 0 ». Et comme l'évaluation donnée est supérieure à 0, le système va classer cette action comme positive.

À cette étape, notre modèle permet de savoir au sein de l'application quel type d'actions sont réalisées par les utilisateurs. Il permet également de catégoriser ces actions en deux types (bonnes ou mauvaises) en définissant l'interprétation de ces deux notions dans le cadre applicatif considéré. Cependant, cette étape ne prend pas en compte l'enchaînement des actions et ne permet pas de décrire ce qui est attendu du modèle computationnel, c'est-à-dire qu'elle ne permet pas d'indiquer des exigences sur l'évolution du score de confiance. Par exemple, le concepteur de l'application pourrait vouloir spécifier comment le score de confiance doit évoluer après 5 covoiturations.

Afin de pouvoir sélectionner le modèle correct selon les besoins du concepteur de l'application, il est essentiel de pouvoir décrire et modéliser la façon dont la confiance doit évoluer en fonction du comportement de l'utilisateur. C'est la deuxième partie de notre approche qui est présentée dans la section suivante.

6.4.2 Modélisation des exigences sur l'évolution de la confiance

Dans la section précédente, notre modèle proposé nous a permis d'identifier les types d'action (positive, négative...) qui peuvent être effectuées par les utilisateurs d'un système suite aux évaluations données. À ce stade, on ne parle que des actions individuelles. Autrement dit, on ne peut pas avoir d'informations sur la réputation d'un utilisateur, puisqu'on n'a pas d'informations sur l'enchaînement de ses actions. Par conséquent, il faut lier ces actions pour enrichir notre modèle, comprendre le comportement des utilisateurs et pouvoir l'utiliser avec les modèles computationnels de confiance.

Comme précisé précédemment, l'objectif de cette section est de pouvoir modéliser ce qu'on attend de l'évolution de la confiance au sein d'un système par rapport aux actions communiquées dans le modèle précédent. C'est pourquoi nous avons proposés un deuxième modèle pour traiter cette question.

Afin d'exprimer l'enchaînement d'actions, il existe plusieurs formalismes dans les systèmes de communication homme-machine qui permettent aux utilisateurs de définir les attentes de leur système, par exemple : Business Process Model and Notation (BPMN) [Whi04], Unified Modeling Language(UML) [JBR96], BPEL (Business Process Execution Language) [And+03]. Les modèles de tâches [LV04] présentent un grand intérêt pour l'activité des utilisateurs de systèmes et visent à produire une liste de tâches, une description des tâches et de leurs interactions. Différents modèles de tâches ont été développés dans la littérature, voir (CTT [PMM97], GTA [VLB96], MAD [SP89], N-MDA (K-MAD) [Luc05], UAN [HSH90], etc). Cependant, toutes ces méthodes de modélisation n'ont pas été développées pour traiter le sujet de la confiance. C'est la première fois que de telles méthodes sont utilisées pour traiter et modéliser les exigences des systèmes basés sur la confiance.

Afin de présenter l'enchaînement d'actions, nous optons pour l'utilisation des modèles de tâches puisque nous nous intéressons à l'activité des utilisateurs du système. Le but de l'analyse des tâches avec ces modèles est de produire une liste de tâches et une description des tâches et de leurs interactions. Dans les modèles de tâche, une tâche fait référence à un ensemble d'activités cohérentes qui sont réalisées pour atteindre un objectif dans un domaine donné [MH89].

- Une tâche a un début et une fin bien définis. Elle est exécutée dans un intervalle de temps relativement court. C'est la contrainte par défaut de ce qui doit être considéré comme une tâche.
- Une tâche décrit une partie spécifique et indépendante du travail. Cette indépendance ne signifie pas que la tâche est toujours exécutée dans un contexte isolé. Les sous-tâches n'ont généralement de sens que dans le contexte de leur super-tâche. Ce que cette propriété indique, c'est que les énoncés de tâches doivent fournir une description complète de la tâche correspondante.
- Une tâche commence par un indice observable. Cela signifie qu'il doit y avoir un moyen de décider quand une tâche est ou peut être commencée.

Les modèles de tâches sont des modèles dans lesquels l'activité est décrite en procédant par décomposition hiérarchique des tâches.

De nombreux modèles de tâches ont été développés, ces modèles permettent d'exprimer plusieurs caractéristiques sur les tâches, mais ce qui nous intéresse dans notre travail est :

- la décomposition d'une tâche en sous-tâches ;
- les relations d'ordre temporel des sous-tâches (séquence, alternative, parallélisme, etc.).

Par conséquent, ces modèles nous permettent d'exprimer l'enchaînement d'actions, les contraintes, ainsi qu'une présentation graphique et visuelle des exigences. C'est pour cette raison que nous avons choisi de les exploiter pour représenter les comportements des utilisateurs afin d'avoir une vue sur l'enchaînement de leurs actions. En revanche, la limite de ces modèles est qu'ils ne permettent pas d'indiquer des contraintes sur l'évolution du score de confiance. Cela est dû au fait que ces modèles n'ont pas été développés dans le cadre des systèmes de confiance. En conséquence, nous proposons d'utiliser des caractéristiques des modèles de tâches et de les adapter aux spécificités des systèmes basés sur la notion de confiance.

6.4.2.1 Formalisme graphique et textuelle

Nous proposons une extension des modèles de tâches dans la figure 6.4. Cette extension comprend notre proposition de représentation graphique des exigences de confiance en utilisant le principe des modèles de tâches qui nous permettent d'avoir des tâches décomposées en sous-tâches avec un opérateur de temps séquentiel et des informations sur la cardinalité des tâches.

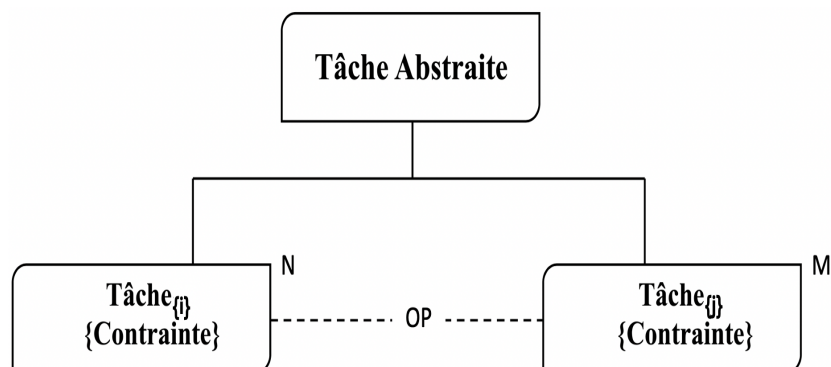


FIGURE 6.4 – Un exemple qui montre notre proposition graphique via le principe des modèles de tâches.

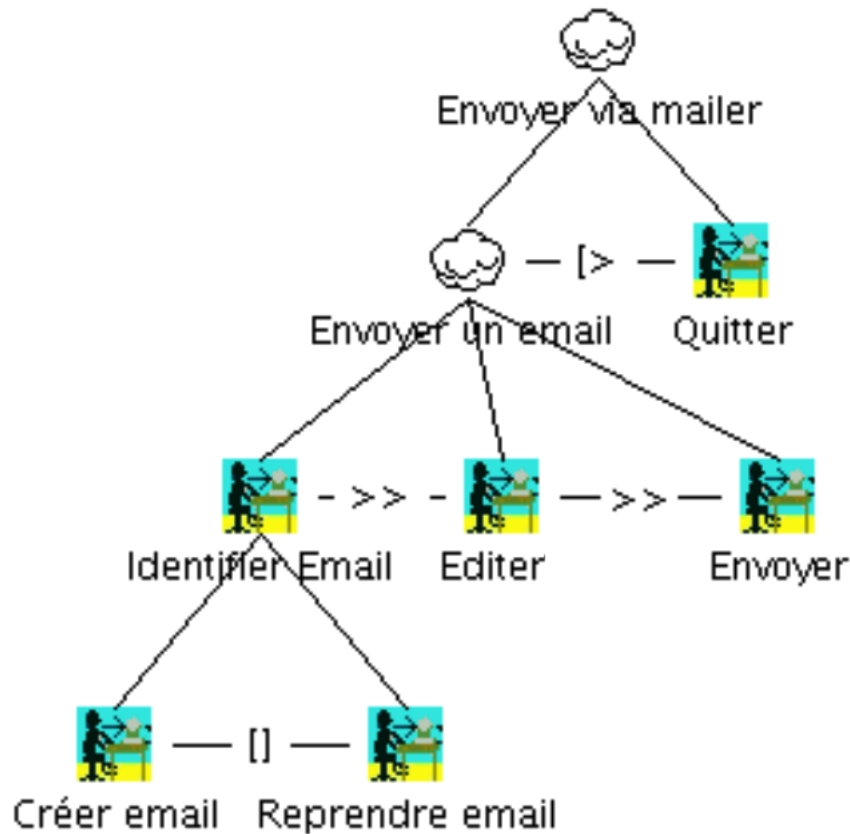


FIGURE 6.5 – Exemple de décomposition de tâches

Pour comprendre l'idée, cette proposition graphique peut être expliquée avec notre deuxième proposition qui est une expression textuelle des activités de l'utilisateur.

$$(Exigence) \gg [(T\grave{a}che_{\{i\}}\{Contrainte\})^N OP (T\grave{a}che_{\{j\}}\{Contrainte\})^M] \quad (6.1)$$

Dans les deux propositions Figure 6.4 et Equation(6.1), pour décrire les exigences de confiance et les tâches qui les composent, nous utilisons le concept de contraintes.

6.4.2.2 Opérateurs de décomposition

Dans les modèles de tâches, chaque tâche décrit l'ordonnancement de ses sous-tâches en utilisant des opérateurs de décomposition. Enfin, chaque tâche décomposée indique comment ses sous-tâches sont temporellement organisées à l'aide d'opérateurs de décomposition (séquence (\gg), parallèle ($| = |$), choix ($[]$, interruption ($[>$) [Caf09]. Ces opérateurs s'appliquent entre deux tâches sœurs, c'est-à-dire du même niveau hiérarchique.

La figure 6.5 montre un exemple de modélisation de la tâche d'envoi d'un e-mail. La tâche racine de l'activité est composée d'une tâche «Envoyer un mail» qui peut être

interrompue par une tâche «Quitter» qui met fin à l'activité modélisée. L'envoi d'un mail est composé d'une première tâche «Identifier le mail» qui est exécutée en choisissant entre deux tâches, soit en créant un nouveau mail «Créer le mail», soit en reprenant un mail déjà écrit sauvegardé dans les brouillons «Reprendre le mail». Une fois l'e-mail identifié, il est suivi séquentiellement par une tâche d'édition «Editer». Une fois l'e-mail édité, cette tâche peut être suivie en séquence par une tâche «Envoyer».

6.4.2.3 Contraintes

Afin de décrire de manière précise chaque tâche, des contraintes peuvent y être associées. Dans les modèles de tâches, ces contraintes sont appelées des pré-conditions et des post-conditions. La pré-condition est la contrainte appliquée au début de la tâche et permettant d'en valider le résultat. Alors que la post-condition c'est la condition qui doit toujours être vrai juste après l'exécution d'une tâche.

Prenons l'exemple de covoiturage. Pour que le système puisse punir un utilisateur malveillant, cet utilisateur doit au début exécuter des actions. Dans des telles applications, le système doit enregistrer au moins trois actions de l'utilisateur pour pouvoir commencer à appliquer les règles de punition. Dans ce cas, la pré-condition de la punition c'est l'enregistrement de trois actions. L'idée derrière cette procédure, est de pouvoir comprendre le comportement de l'utilisateur et laisser l'opportunité à un nouvel utilisateur de découvrir le fonctionnement du système avant de commencer de le punir suite à des actions négatives. Après trois actions, le système détecte que cet utilisateurs a fait deux mauvaises actions. Dans ce cas, il décide de suspendre son activité temporairement. Ici on parle de la post-condition (suspendre l'activité après un mauvais comportement).

6.4.2.4 Instanciation des exigences de la confiance

Dans ce travail, la contrainte est un prédicat booléen qui permet de définir un intervalle dans lequel la valeur de la confiance doit être incluse. Ici, nous ne traitons que les contraintes simples basées sur des valeurs exactes et des pourcentages. Un pourcentage s'appuie sur une valeur de confiance précédente pour exprimer son évolution. Les entiers N et M utilisés fournissent des informations sur l'itération des tâches (c'est-à-dire le nombre de fois qu'une tâche peut se produire). Enfin, « OP » est un opérateur temporel permettant de lier les différentes tâches. Actuellement, seul l'opérateur de séquence est géré,

car il est déterministe et permet de produire une seule sortie en passant par les mêmes tâches. D'autres opérateurs sont fournis, mais ils sont non déterministes (par exemple, choix, interruption, parallèle, etc.) et permettent plusieurs sorties.

Sur la base des modèles de tâches, nous sommes en mesure de définir de nouveaux concepts qui nous permettent d'exprimer des contraintes sur les exigences de confiance et de suivre l'enchaînement des actions de l'utilisateur. Cette proposition nous permettra d'enrichir notre modèle de la Figure 6.2 pour avoir un modèle plus riche qui aide l'utilisateur à la fois à décrire la séquence d'activité humaine se déroulant sur son système, à spécifier le type d'action effectuée et à indiquer des exigences sur l'évolution du score de confiance.

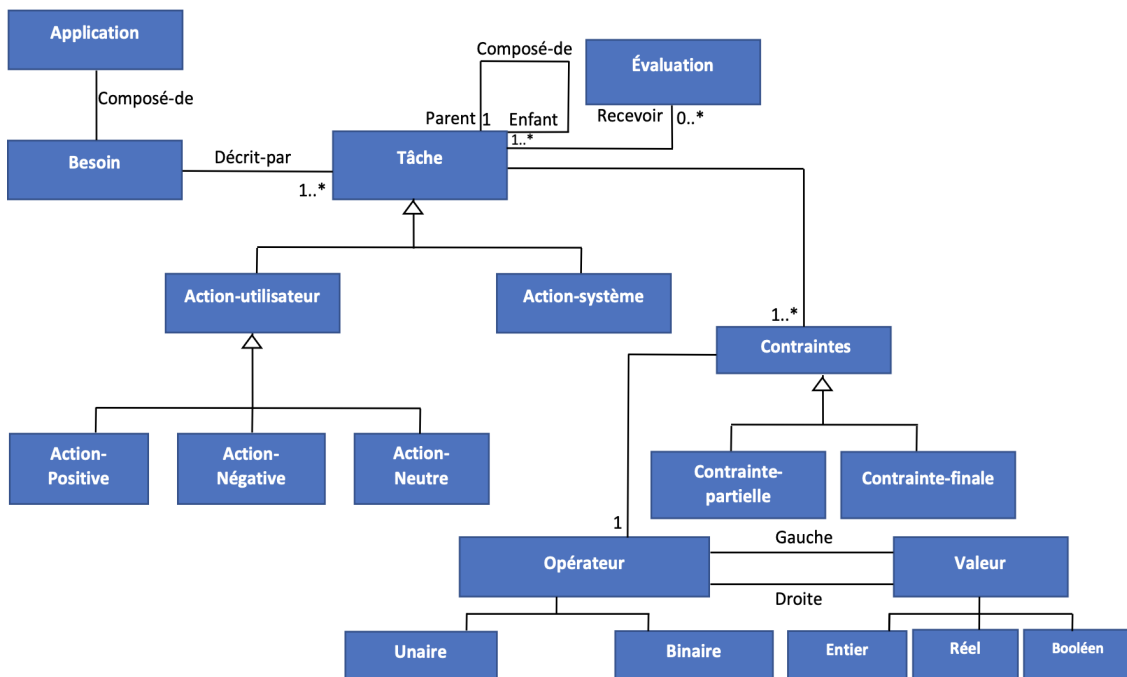


FIGURE 6.6 – Modélisation des exigences de confiance

Comme on peut le voir sur la Figure 6.6, à partir du modèle proposé, chaque exigence de confiance peut être décrite par une tâche. Le système effectue des tâches pour calculer le score, surveiller le comportement, etc. L'utilisateur peut effectuer différents types d'actions que nous avons décrites précédemment. De plus, le principe des sous-tâches dans les modèles de tâches nous permet de spécifier des contraintes partielles pour chaque sous-tâche, ainsi qu'une contrainte finale sur la tâche pour répondre à l'exigence souhaitée. La contrainte partielle fournit des informations sur l'évolution de la valeur de confiance après chaque sous-tâche. Alors que la contrainte finale est utilisée pour spécifier la valeur de

confiance finale souhaitée vers la fin de la tâche.

Comme mentionné dans la section 6.3, certains travaux de recherche ont proposé des critères pour l'évolution de la confiance afin d'évaluer les modèles computationnels de confiance [Ora01]. Un exemple est le critère « La pondération vers le comportement actuel » que nous nommerons « WTCB (Weighted toward current behavior) ». Pour simuler ce critère, on suppose que l'utilisateur effectue des actions positives (dix actions positives) puis commence à effectuer des actions négatives (quatre actions négatives). Tant que l'utilisateur a déjà fait beaucoup d'actions positives, il y a un grand impact sur sa valeur de confiance s'il fait plusieurs actions négatives. Comme on peut le voir dans l'équation 6.2, chaque bonne action permet à l'utilisateur d'augmenter sa valeur de confiance (+20%). Dès qu'il commence à faire des actions négatives, cette valeur doit commencer à diminuer (-15%). Dans le contexte du covoiturage, un utilisateur avec une bonne réputation qui reçoit des évaluations positives après chaque voyage, et qui commence à recevoir des évaluations négatives, doit perdre un pourcentage significatif de sa valeur de confiance. En utilisant la définition des contraintes que nous proposons, nous obtenons :

$$(WTCB) : [(PT_1\{S + 20\%\})^{10} \gg (NT_2\{S < -15\%\})^4] \quad (6.2)$$

Cette notation nous permet d'obtenir une séquence d'actions, 10 actions positives suivies de 4 actions négatives, comme montré dans l'équation 6.3 :

$$(WTCB) : [PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg PT_1 \gg NT_2 \gg NT_2 \gg NT_2 \gg NT_2] \quad (6.3)$$

Les deux modèles proposés peuvent être instanciés pour définir pour chaque système, d'une part, les types d'actions qui peuvent être réalisées en fonction des exigences de l'application, et d'autre part, l'enchaînement de ces actions pour pouvoir suivre l'évolution de la confiance et appliquer des exigences qui répondent aux besoins du système. En utilisant ces deux modèles, nous pouvons passer à la dernière étape de notre approche, qui consiste à choisir le modèle computationnel le plus approprié en fonction des exigences de l'utilisateur.

6.4.3 Recommandation du modèle computationnel de la confiance

Dans la section 6.4.1, nous avons défini les différents types d'actions d'un système en fonction des exigences de l'application. À la fin de cette première étape, notre modèle permet de savoir au sein de l'application quel type d'actions sont réalisées par les utilisateurs. Cependant, cette étape ne prend pas en compte l'enchaînement des actions et ne permet pas de décrire ce qui est attendu du modèle computationnel de la confiance, c'est-à-dire qu'elle ne permet pas d'indiquer des exigences sur le score de confiance. Par conséquent, dans la section 6.4.2, l'idée du deuxième modèle est d'étudier la séquence des actions de l'utilisateur pour comprendre son comportement, avoir une idée sur l'enchaînement de ses actions, pouvoir appliquer les pré-conditions avant chaque action et la lier à l'action suivante en utilisant les post-conditions. Ce deuxième modèle enrichi va nous permettre d'utiliser les modèles computationnels pour calculer des valeurs de confiance pour chaque utilisateur en fonction de son comportement. Dans les applications communautaires, ce sont ces valeurs qui décrivent la réputation de l'utilisateur et aident les autres utilisateurs à prendre la décision de coopérer en ayant une idée de la fiabilité des profils sur la base des actions précédentes.

Un système basé sur la confiance doit, comme mentionné ci-dessus, avoir une stratégie pour calculer la valeur de la confiance. En effet, le calcul de la confiance doit permettre de faire un choix, par exemple, un haut degré de confiance dans une entité permet de la juger fiable et de faire le choix de lui faire confiance [Gai11]. De nombreux auteurs ont proposé des modèles pour représenter et calculer la confiance dans les systèmes. Ces modèles sont classés en modèles bayésiens, modèles à valeurs discrètes, modèles à base de croyances, modèles flous et modèles de flux.

Afin d'évaluer ces modèles, ce chapitre se concentre sur les critères qui permettent d'observer le comportement de l'être humain au sein du système suivi de l'évolution du score de confiance. L'idée derrière cette partie de l'approche est de générer un scénario que l'utilisateur peut faire dans le système, de mettre des contraintes sur la façon dont le score de la confiance évolue (par exemple, une évolution progressive), et de calculer la valeur du score en utilisant des modèles computationnels développés dans la littérature.

Comme résultat de ce modèle, nous aurons une estimation de la correspondance entre les contraintes fixées et les valeurs obtenues. Cela facilitera la recommandation du modèle computationnel le plus approprié pour chaque exigence. Une démonstration plus complète

avec des résultats sera illustrée dans la section suivante.

6.5 Étude de cas

Pour valider notre approche, nous présentons dans cette section une étude de cas plus complète basée sur l'exemple motivant de la section 6.2 qui permet de couvrir tous les aspects de la contribution, d'expliquer le processus complet et de montrer la faisabilité technique de notre travail. Pour pouvoir montrer les résultats de notre approche, un développement a été fait dans lequel les deux modèles et les principaux modèles computationnels ont été mis en œuvre.

L'objectif est de fournir un outil, appelé TME (Trust Model Evaluation), qui peut évaluer automatiquement les modèles computationnels par rapport aux exigences exprimées. En ce qui concerne l'environnement technique, nous avons utilisé Java comme langage de programmation avec une approche dirigée par les tests pour valider notre travail. La machine utilisée pour les tests est un ordinateur macOS avec un processeur Intel Core i7 6-core à 2.6 GHz. Actuellement, le code source est disponible sur la forge du laboratoire².

6.5.1 Exigences pour l'application de covoiturage

La première partie de notre approche consiste à définir les types d'actions qu'un utilisateur peut effectuer pour contrôler ensuite leur enchaînement, demander des préférences sur l'évolution de cette valeur, calculer une valeur de confiance et choisir le modèle computationnel approprié.

Pour ce faire, dans notre exemple, si l'utilisateur reçoit une note « Décevant ou Très décevant », le système considère cela comme une action négative. S'il reçoit une évaluation « Excellent ou Bon », alors il a effectué une action positive. Et si l'utilisateur reçoit une évaluation « Correct », alors il a effectué une action neutre. Afin de pouvoir classer le type d'action effectuée par l'utilisateur, nous devons associer des valeurs continues à ces évaluations discrètes pour comprendre le comportement de l'utilisateur et l'évaluation du score comme le montre le tableau 6.2.

2. <https://forge.lias-lab.fr/projects/trustmodelevaluation>

TABLEAU 6.2 – Discrétisation des degrés d'évaluation.

| | | | | |
|---------------|----------|---------|-----|-----------|
| Très décevant | Décevant | Correct | Bon | Excellent |
| 0 | 1 | 2 | 3 | 4 |

Ainsi, ces valeurs nous permettent de mettre des contraintes sur les évaluations. Chaque utilisateur peut donner une *notation* $\in [-1;1]$. Si la *notation* > 0 , l'action est positive. Si la *notation* < 0 , l'action est négative. Si la *notation* $= 0$, l'action est neutre.

Nous considérons dans la suite de ce chapitre l'exemple d'un passager qui a effectué 10 voyages et a été évalué après chaque expérience comme indiqué dans le tableau 6.3.

TABLEAU 6.3 – Exemple de comportement de l'utilisateur et de ses évaluations dans le système.

| Actions | Voyage 1 | Voyage 2 | Voyage 3 | Voyage 4 | Voyage 5 | Voyage 6 | Voyage 7 |
|-------------|------------|------------|------------|------------|------------|------------|------------|
| Evaluation | Bon | Bon | Excellent | Décevant | Bon | Décevant | Décevant |
| Contraintes | $note > 0$ | $note > 0$ | $note > 0$ | $note > 0$ | $note < 0$ | $note > 0$ | $note < 0$ |
| Type | Positive | Positive | Positive | Positive | Négative | Positive | Négative |

6.5.2 Exigences de confiance pour le covoiturage

À ce stade, notre premier modèle est capable de définir les types d'actions qu'un utilisateur peut effectuer. La deuxième étape est de pouvoir modéliser ce comportement et d'exiger des contraintes sur le score de confiance. L'objectif de cette partie de l'approche est de pouvoir modéliser ce que l'on attend de l'évolution de la confiance dans le système par rapport aux actions exprimées dans le modèle précédent.

Prenons l'exemple de trois formes d'évolution de la confiance parmi les critères mentionnés dans la section 6.3. La première est « Pondération vers le comportement actuel (WTCB) » : Si l'utilisateur a une bonne réputation, c'est-à-dire qu'il a fait plusieurs actions positives (PT), et qu'il commence à faire des actions négatives (NT), le système devrait montrer un fort impact sur le score de confiance (S). Pour ce critère, les systèmes existants commencent à surveiller le score de l'utilisateur généralement à partir de la troisième action, afin de donner à un nouvel utilisateur la possibilité de comprendre le fonctionnement du système et d'acquérir une première réputation. Après la première étape de modélisation, nous pouvons définir l'ensemble des actions de l'utilisateur et ainsi avoir

TABLEAU 6.4 – Contraintes appliquées au score de confiance souhaité pour le critère WTCB.

| Actions | P | P | P | P | P | P | P | N | N | N | N |
|-------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|-------|-------|
| Contraintes | S > 22 | S > 24 | S > 26 | S > 28 | S > 30 | S > 33 | S < 36 | S < 23 | S < 14 | S < 9 | S < 5 |

une séquence d'actions :

$$(WTCB) : [(PT_1\{S > +10\%\})^7 \gg (NT_2\{S < -35\%\})^4] \quad (6.4)$$

Le deuxième critère est « Efficace » : Si l'utilisateur a une bonne réputation, c'est-à-dire qu'il a fait plusieurs actions positives, et qu'il fait une action négative, cet utilisateur peut alors récupérer partiellement sa confiance s'il fait une action positive. Pour modéliser ce critère, supposons qu'un utilisateur a reçu ces évaluations : (Bon, Bon, Excellent, Excellent, Décevant, Bon, Bon, Décevant, Bon). A partir du premier modèle, nous pouvons définir toutes ses actions et ainsi avoir une chaîne d'actions :

$$(Efficace) : [(PT_1\{Score > +10\%\})^4 \gg (NT_2\{Score < -25\%\}) \gg (PT_3\{S > +20\%\})^2 \gg (NT_4\{S < -25\%\})] \quad (6.5)$$

TABLEAU 6.5 – Contraintes appliquées au score de confiance souhaité pour le critère Efficace.

| Actions | P | P | P | P | N | P | P | N |
|-------------|--------|--------|--------|--------|--------|--------|--------|--------|
| Contraintes | S > 22 | S > 24 | S > 26 | S > 28 | S < 21 | S > 25 | S > 30 | S < 22 |

Le troisième critère est « Flexible » : Pour chaque action positive, le système devrait augmenter légèrement le score de l'utilisateur. Lorsque l'utilisateur fait une seule action négative, le système devrait diminuer légèrement le score. En appliquant le même modèle que les deux premiers critères, nous obtenons :

$$(Flexible) : [(PT_1\{S > +10\%\})^5 \gg (NT_2\{S < -10\%\}) \gg (PT_3\{S > +10\%\})^5 \gg (NT_4\{S < -20\%\})^6] \quad (6.6)$$

TABLEAU 6.6 – Contraintes appliquées au score de confiance souhaité pour le critère Flexible.

| | | | | | | | | | |
|-------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| Actions | P | P | P | P | P | N | P | P | P |
| Contraintes | $S > 22$ | $S > 24$ | $S > 26$ | $S > 28$ | $S > 30$ | $S < 27$ | $S > 29$ | $S > 31$ | $S > 34$ |
| Actions | P | P | N | N | N | N | N | N | |
| Contraintes | $S > 37$ | $S > 40$ | $S < 32$ | $S < 25$ | $S < 20$ | $S < 16$ | $S < 12$ | $S < 9$ | |

6.5.3 Recommandation du modèle computationnel de confiance

Dans cet exemple, nous avons proposé des contraintes pour satisfaire les trois critères que nous avons considérés. Pour ces contraintes, nous avons mis l'accent sur le fait que l'évolution du score de confiance est progressive, pour satisfaire le critère « flexible ». Par la suite, ces contraintes doivent prendre en compte le fait que si l'utilisateur se comporte bien après une action négative, il a le droit de récupérer une partie de son score de confiance (critère d'efficacité). Mais s'il continue à mal se comporter, il doit perdre sa réputation (critères pondérés vers le comportement actuel).

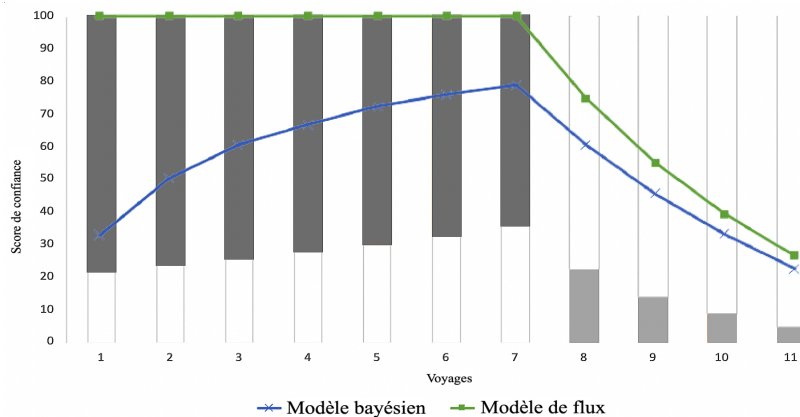


FIGURE 6.7 – Compatibilité des modèles computationnels pour le critère WTCB

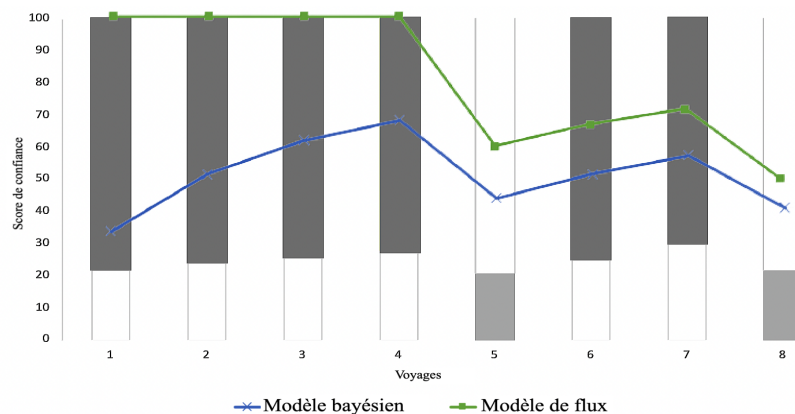


FIGURE 6.8 – Compatibilité des modèles computationnels pour le critère Efficace

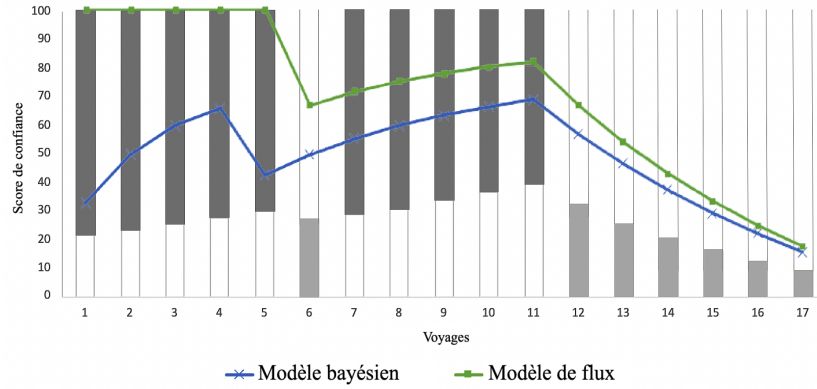


FIGURE 6.9 – Compatibilité des modèles computationnels pour le critère Flexible

Les figures 6.7, 6.8, 6.9 montre les résultats obtenus par notre modèle implémenté. Comme nous pouvons le voir, notre modèle permet d’exprimer des préférences sur la valeur du score de confiance désiré pour l’utilisateur (U), qui peut être vu sous la forme de barres dans la figure, et de tester les modèles computationnels existants dans la littérature afin de connaître par la suite le modèle le plus adéquat. Il existe plusieurs modèles computationnels de confiance dans la littérature. Nous avons choisi de prendre deux modèles comme exemples pour montrer les résultats et la faisabilité de notre approche. Le premier modèle choisi est un modèle bayésien [CJI02] qui utilise la fonction(6.7) pour obtenir un score de confiance et le second est un modèle de flux [KSG03] avec la fonction(6.8).

$$Score\{U\} = \frac{P - N}{P + N + 2} \quad (6.7) \quad Score\{U\} = \frac{\max(P - N, 0)}{P + N} \quad (6.8)$$

La figure 6.10 montre les résultats de la compatibilité des valeurs obtenues à l’aide des modèles computationnels avec les valeurs souhaitées en fonction des contraintes fixées par l’utilisateur. Cette méthode nous permet de recommander le modèle computationnel le plus approprié en fonction des exigences. Par exemple, pour un utilisateur qui recherche un système lui permettant de mettre à jour progressivement le score de confiance, il sera préférable de baser son calcul sur le modèle bayésien qui s’est avéré plus performant pour ce critère.

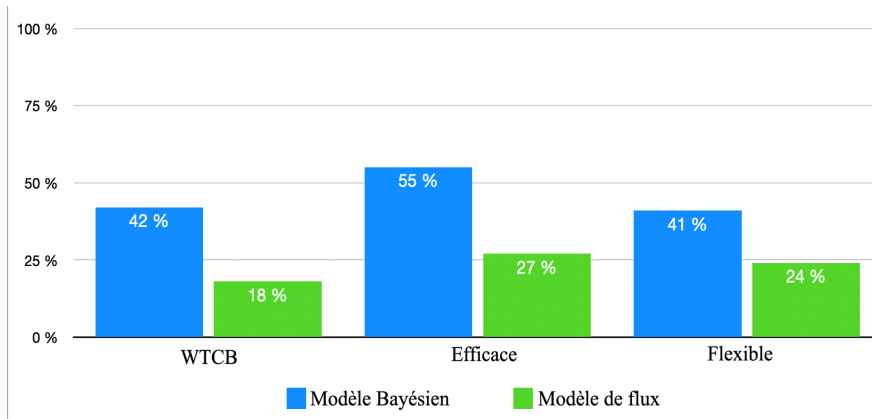


FIGURE 6.10 – Pourcentage de compatibilité des modèles computationnels pour chaque critère

6.6 Conclusion et Perspectives

Dans ce chapitre, nous avons abordé le problème de l'évaluation des systèmes basés sur la confiance et du choix du modèle le plus approprié aux exigences de l'application.

Nous avons proposé une approche qui aide l'utilisateur à sélectionner le modèle le plus adapté à son système. Nous avons défini et implémenté une étude de cas complète. Cette dernière montre que notre approche peut être utilisée pour modéliser différentes exigences, trouvées dans la littérature, sur le calcul de la confiance. De plus, notre approche et l'outil associé comparent les différents modèles computationnels sur la base d'un ensemble d'exigences afin de sélectionner le plus approprié. Ce travail peut être étendu de différentes manières. Dans notre proposition, chaque modèle computationnel est testé et le plus adéquat est proposé au concepteur de l'application. Cependant, une combinaison de ces modèles computationnels pourraient permettre de mieux satisfaire les besoins d'évolution de la confiance. Une perspective consiste donc à considérer des combinaisons de modèles computationnels dans notre approche.

Une autre perspective concerne la définition des besoins en terme d'évolution de la confiance. Actuellement, notre modèle est capable de représenter différentes enchaînements d'activités tels que la séquence ou l'alternative. Cependant, un concepteur pourrait avoir besoin d'opérateurs plus complexes, tels que des opérateurs temporels (par exemple, des opérateurs de parallélisme ou d'interruption). L'extension de notre modèle avec ce type d'opérateurs est une de nos perspectives immédiates.

Conclusion générale et perspectives

Dans cette thèse, nous nous sommes intéressés aux modèles computationnels des systèmes de confiance pour la recommandation. Ce sujet possède de multiples facettes et a nécessité que nous l'abordions selon trois axes : les systèmes de recommandation ; les systèmes de confiance ; les exigences des systèmes de confiance.

État de l'art

Ainsi, dans la première partie, nous avons dressé un état de l'art de ces trois axes. Avant d'aborder les systèmes de recommandation et les systèmes de confiance, nous avons dû présenter le cadre dans lequel ces systèmes ont émergé, ce sont les réseaux sociaux. Ensuite, nous avons discuté de certains problèmes qui ont surgi avec ces réseaux, en particulier, la collecte de données et la violation de la vie privée.

Ces problèmes ont été traités par l'émergence des réseaux sociaux anonymes. Nous avons brièvement introduit le concept de l'anonymat ainsi que certains systèmes qui l'ont adopté. Ces systèmes deviennent plus tard des outils de cyberintimidation et de fraude, ce qui rend difficile l'établissement de relations au sein de ces systèmes, l'échange d'informations, la recommandation et l'instauration d'un environnement de confiance.

Nous avons ensuite défini le concept de la confiance, les systèmes qui l'utilisent, comment on le calcule en utilisant les modèles computationnels et finalement comment propager l'information de la confiance au sein d'un réseau en se basant sur la recommandation. Ainsi, cette technologie de partage d'informations nous a conduit à développer l'état de l'art des systèmes de recommandation.

Travaux réalisés

Dans la deuxième partie de ce travail, nous avons décrit et détaillé nos trois contributions. Comme nous l'avons expliqué, avec l'émergence des réseaux sociaux, la confiance est devenue l'un des éléments clés qui permettent aux utilisateurs d'interagir en toute sécurité. Ce concept a été développé dans plusieurs travaux afin de produire des systèmes de recommandation à base de confiance.

Systemes de recommandations

Certains systèmes de recommandation posent encore plusieurs problèmes tels que : la difficulté à gérer les profils atypiques, la difficulté à traiter les changements de profils des utilisateurs, le manque de diversité des recommandations, le manque d'explication des recommandations, etc. Pour résoudre certains de ces problèmes, de nouvelles approches basées sur des techniques d'Intelligence Artificielle émergent. Dans un premier temps, nous avons modélisé le besoin de recommandation comme un problème de décision de Markov (MDP) et l'avons traité via une solution d'apprentissage par renforcement. Cependant, les systèmes de recommandation par renforcement existants présentent deux problèmes majeurs : (1) ils doivent traverser un grand nombre d'états, ce qui augmente la complexité algorithmique et (2) il est difficile d'expliquer les résultats. Dans ce travail, nous proposons une méthode hybride pour résoudre ces problèmes. Nous utilisons une technique de clustering hiérarchique qui permet de réduire l'espace des états et des actions et donc d'améliorer la complexité algorithmique. L'utilisation du clustering hiérarchique ne permet pas seulement de réduire l'espace, mais peut également contribuer à améliorer la qualité des recommandations et à renforcer l'explicabilité.

Systemes de confiance

Par la suite, dans un second temps, nous avons abordé le problème de la confiance, de la réputation des utilisateurs et de leur modèles computationnels. En raison des nombreuses études réalisées dans la littérature sur ces concepts, nous avons tenté de proposer une formalisation unifiée de ces derniers pour les besoins de la recommandation. En particulier, nous avons révisé leurs définitions et reformulé leurs propriétés de base. Ce qui permet de bien comprendre le comportement et l'intuition derrière chaque modèle computationnel.

Un ensemble d'exigences a été établi pour rendre le choix du modèle plus pratique et plus intelligent, dans le sens où il répond effectivement aux besoins souhaités. Il faut noter que les propositions d'exigences d'application que nous avons établies sont en accord avec les besoins de l'entreprise O°Code. Elles peuvent varier d'un système à l'autre et nous pouvons redéfinir les spécifications associées pour chaque application. Notre idée était de comparer et de proposer une nouvelle classification des types de modèles computationnels existants dans la littérature. Cela permet de sélectionner le modèle de calcul le plus approprié pour une application si nécessaire. Cette idée nous ramène à chercher les exigences liés à la confiance dans la littérature, comment les modéliser pour comprendre le comportement des utilisateurs? et comment recommander le modèle computationnel le plus adéquat selon les besoins de l'application? Les expériences réalisées montrent que notre proposition d'exigences permet de discriminer entre les différents modèles et de sélectionner les plus appropriés en fonction des besoins.

Exigences des systèmes de confiance

Ensuite, dans la dernière partie, nous avons abordé le problème de l'évaluation des systèmes de confiance et du choix du modèle computationnel le plus approprié aux exigences de chaque application. Nous avons tenté de proposer une approche qui aide l'utilisateur à sélectionner le modèle le plus adapté à son système. Nous avons défini et implémenté une étude de cas complète. Cette dernière montre que notre approche peut être utilisée pour modéliser différentes exigences, trouvées dans la littérature, sur le calcul de la confiance. De plus, notre approche et l'outil associé comparent les différents modèles computationnels sur la base d'un ensemble d'exigences afin de sélectionner le modèle le plus approprié.

Perspectives

Vers une recommandation hybride

L'idée est de travailler sur d'autres méthodes de clustering. Nous voulons comparer plusieurs méthodes de clustering et utiliser des jeux de données plus importants disponibles dans la littérature afin de pouvoir comparer notre approche aux approches existantes.

De plus, une extension possible de ce travail est de considérer la notion de recommandation de groupe, c'est-à-dire, l'étude des liens entre les profils pour extraire un goût commun pour un groupe d'utilisateurs. L'explication des résultats est un autre aspect majeur à intégrer dans ce travail afin d'augmenter la confiance dans les recommandations. Par ailleurs, le problème de gestion des changements dans les profils des utilisateurs est toujours persistant. Ce qui nécessite de maintenir la confiance et l'adapter au comportement de l'utilisateur. L'idée serait de traiter les exigences liés aux besoins de l'utilisateur. Ces systèmes collectent des quantités massives de données qui peuvent atteindre la vie privée des utilisateurs. La question comment modéliser et assurer la confiance en respectant les données personnelles et en se basant sur les besoins et les comportements des utilisateurs, se pose également.

Enrichissement du modèle de confiance

Nous avons pu effectuer un premier pas vers un nouveau modèle général de confiance qui peut s'adapter au contexte de chaque application. Notre travail peut être amélioré en ajoutant certaines fonctionnalités comme la construction d'un modèle hybride qui répond au mieux aux différentes exigences de la confiance, par exemple le concepteur désire satisfaire deux exigences en même temps, et que notre approche lui fournit une recommandation différente pour chaque exigence, la fusion des deux modèles computationnels recommandés serait une solution. Actuellement, notre modèle est capable de représenter différentes enchaînements d'activités tels que la séquence ou l'alternative. Cependant, un concepteur pourrait avoir besoin d'opérateurs plus complexes, tels que des opérateurs temporels (par exemple, des opérateurs de parallélisme ou d'interruption). L'extension de notre modèle avec ce type d'opérateurs est aussi une de nos perspectives immédiates. En outre, nous envisageons aborder la question de la vérification de l'expressivité, la complétude et les limitations de notre framework pour modéliser les besoins des systèmes communautaires existants.

Bibliographie

- [DF04] Alain DEGENNE et Michel FORSÉ. *Les réseaux sociaux*. T. 2. Armand Colin Paris, 2004.
- [CC15] Lisa CRÉNO et Béatrice CAHOUR. “Triangulation des méthodes pour une analyse écologique de l’expérience vécue de gestion des emails chez des cadres surchargés”. In : *Activités humaines, Technologies et Bien être* (2015), p. 219.
- [KCS14] Gérald KEMBELLEC, Ghislaine CHARTRON et Imad SALEH. *Les moteurs et systèmes de recommandation*. ISTE Group, 2014.
- [Hay14] Charif Alchiekh HAYDAR. “Les systèmes de recommandation à base de confiance”. Thèse de doct. Université de Lorraine, 2014.
- [Bar69] John A BARNES. “Graph theory and social networks : A technical comment on connectedness and connectivity”. In : *Sociology* 3.2 (1969), p. 215-232.
- [Gon+20] Zaiwu GONG et al. “Measuring trust in social networks based on linear uncertainty theory”. In : *Information Sciences* 508 (2020), p. 154-172.
- [BE07] Danah M BOYD et Nicole B ELLISON. “Social network sites : Definition, history, and scholarship”. In : *Journal of computer-mediated Communication* 13.1 (2007), p. 210-230.
- [HKP12] Julia HEIDEMANN, Mathias KLIER et Florian PROBST. “Online social networks : A survey of a global phenomenon”. In : *Computer networks* 56.18 (2012), p. 3866-3878.
- [Onl22] ONLYSO. “*Les chiffres 2021 des réseaux sociaux*”. <https://www.onlyso.fr/les-chiffres-2021-des-reseaux-sociaux.html>. Mis en ligne le 30 Novembre 2021, Consulté le 08 Mars 2022.

-
- [MK82] Samuel Finley Breese MORSE et William KLOSS. *Samuel FB Morse*. Grey Art Gallery et Study Center, 1982.
- [PS19] Camille PALOQUE-BERGÈS et Valérie SCHAFER. “Arpanet (1969–2019)”. In : *Internet Histories 3.1* (2019), p. 1-14.
- [NSF22] NSF. “*The National Science Foundation*”. https://www.nsf.gov/news/special_reports/nsf-net/textonly/index.jsp. Consulté le 08 Mars 2022.
- [Sha22] Saqib SHAH. “*The history of social networking*”. <https://www.digitaltrends.com/features/the-history-of-social-networking/>. Mis en ligne le 14 Mai 2016, consulté le 08 Mars 2022.
- [Boy04] Danah Michele BOYD. “Friendster and publicly articulated social networking”. In : *CHI’04 extended abstracts on Human factors in computing systems*. 2004, p. 1279-1282.
- [Alb+11] W David ALBRECHT et al. “LinkedIn for accounting and business students”. In : *American Journal of Business Education (AJBE)* 4.10 (2011), p. 39-42.
- [Lin22] LINKEDIN. “*LinkedIn Pressroom*”. <https://news.linkedin.com/about-us#Statistics>. Consulté le 08 Mars 2022.
- [Jon+08] Steve JONES et al. “Whose space is MySpace? A content analysis of MySpace profiles”. In : *First monday* (2008).
- [Brü15] Niels BRÜGGER. “A brief history of Facebook as a media text : The development of an empty structure”. In : *First Monday* (2015).
- [Ass22] Christophe ASSELIN. “*Facebook les chiffres essentiels en 2022 en France et dans le Monde*”. <https://blog.digimind.com/fr/agences/facebook-chiffres-essentiels>. Mise à jour en Février 2022, Consulté le 08 Mars 2022.
- [Mag+12] Gabriel MAGNO et al. “New kid on the block : Exploring the google+ social graph”. In : *Proceedings of the 2012 Internet Measurement Conference*. 2012, p. 159-170.
- [Mar22] Bachelor’s in MARKETING. “*The Evolution of Social Media : How Did It Begin, and Where Could It Go Next?*” <https://online.maryville.edu/blog/evolution-social-media/s>. Consulté le 08 Mars 2022.

-
- [MS16] Maurice MARS et Richard E SCOTT. “Whatsapp in clinical practice : A literature”. In : *The Promise of New Technologies in an Age of New Health Challenges* (2016), p. 82.
- [Pen+18] Sancheng PENG et al. “Influence analysis in social networks : A survey”. In : *Journal of Network and Computer Applications* 106 (2018), p. 17-32.
- [KB18] Joseph KAHNE et Benjamin BOWYER. “The political significance of social media activity and social networks”. In : *Political Communication* 35.3 (2018), p. 470-493.
- [RH09] Vala Ali ROHANI et Ow Siew HOCK. “On social network web sites : definition, features, architectures and analysis tools”. In : *Journal of Computer Engineering* 1 (2009), p. 3-11.
- [CHW06] Chao-Min CHIU, Meng-Hsiang HSU et Eric TG WANG. “Understanding knowledge sharing in virtual communities : An integration of social capital and social cognitive theories”. In : *Decision support systems* 42.3 (2006), p. 1872-1888.
- [SP13] Belinda SHIPPS et Brandis PHILLIPS. “Social networks, interactivity and satisfaction : Assessing socio-technical behavioral factors as an extension to technology acceptance”. In : *Journal of theoretical and applied electronic commerce research* 8.1 (2013), p. 35-52.
- [Wan+14] Gang WANG et al. “Whispers in the dark : analysis of an anonymous social network”. In : *Proceedings of the 2014 conference on internet measurement conference*. 2014, p. 137-150.
- [Wal99] Kathleen A WALLACE. “Anonymity”. In : *Ethics and Information technology* 1.1 (1999), p. 21-31.
- [Fle21] Sean FLEMING. “The Unabomber and the origins of anti-tech radicalism”. In : *Journal of Political Ideologies* (2021), p. 1-19.
- [HO05] Joseph Y HALPERN et Kevin R O’NEILL. “Anonymity and information hiding in multiagent systems”. In : *Journal of Computer Security* 13.3 (2005), p. 483-514.

-
- [CP15] Sudhanshu CHAUHAN et Nutan Kumar PANDA. *Hacking web intelligence : Open source intelligence and web reconnaissance concepts and techniques*. Syngress, 2015.
- [Mat+03] Naohiro MATSUMURA et al. “The Dynamism of 2channel”. In : *SID-2003 : Social Intelligence Design, Royal Holloway University of London at Egham, Surrey* (2003).
- [Gro14] JV GROVE. “Secrets and lies : Whisper and the return of the anonymous app”. In : *CNet News, January* (2014).
- [Nak08] Satoshi NAKAMOTO. “Bitcoin : A peer-to-peer electronic cash system”. In : *Decentralized Business Review* (2008), p. 21260.
- [blo22] BLOCK. “Deloitte”. <https://www2.deloitte.com/>. Consulté le 1er Avril 2022.
- [SP16] Sheryl Gay STOLBERG et Richard PÉREZ-PEÑA. “Wildly popular app kik offers teenagers, and predators, anonymity”. In : *The New York Times* (2016).
- [MFS15] Timothy MOREY, Theodore FORBATH et Allison SCHOOP. “Customer data : Designing for transparency and trust”. In : *Harvard Business Review* 93.5 (2015), p. 96-105.
- [Hay05] Caroline HAYTHORNTHWAITTE. “Social networks and Internet connectivity effects”. In : *Information, Community & Society* 8.2 (2005), p. 125-147.
- [SNP13] Wanita SHERCHAN, Surya NEPAL et Cecile PARIS. “A survey of trust in social networks”. In : *ACM Computing Surveys (CSUR)* 45.4 (2013), p. 1-33.
- [Jae+07] Paul T JAEGER et al. “Community response grids : E-government, social networks, and effective emergency management”. In : *Telecommunications Policy* 31.10-11 (2007), p. 592-604.
- [GA05] Ralph GROSS et Alessandro ACQUISTI. “Information revelation and privacy in online social networks”. In : *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. 2005, p. 71-80.
- [Hel94] Dirk HELBING. “A mathematical model for the behavior of individuals in a social field”. In : *Journal of Mathematical Sociology* 19.3 (1994), p. 189-219.

-
- [Möl01] Guido MÖLLERING. “The nature of trust : From Georg Simmel to a theory of expectation, interpretation and suspension”. In : *Sociology* 35.2 (2001), p. 403-420.
- [Rot67] Julian B ROTTER. “A new scale for the measurement of interpersonal trust 1”. In : *Journal of personality* 35.4 (1967), p. 651-665.
- [Hua07] Fali HUANG. “Building social trust : A human-capital approach”. In : *Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft* (2007), p. 552-573.
- [MTG07] Muthucumaru MAHESWARAN, Hon Cheong TANG et Ahmad GHUNAIM. “Towards a gravity-based trust model for social networking systems”. In : *27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)*. IEEE. 2007, p. 24-24.
- [MQR04] M MOBIUS, Do QUOC-ANH et Tanya S ROSENBLAT. “Social capital in social networks”. In : *Retrieved March 3* (2004), p. 2009.
- [JIB07] Audun JØSANG, Roslan ISMAIL et Colin BOYD. “A survey of trust and reputation systems for online service provision”. In : *Decision support systems* 43.2 (2007), p. 618-644.
- [Vu10] Van-Hoan VU. “Infrastructure de gestion de la confiance sur internet”. Thèse de doct. Ecole Nationale Supérieure des Mines de Saint-Etienne, 2010.
- [AH00a] Alfaraz ABDUL-RAHMAN et Stephen HAILES. “Supporting trust in virtual communities”. In : *Proceedings of the 33rd annual Hawaii international conference on system sciences*. IEEE. 2000, 9-pp.
- [lar22] LAROUSSE. ”*LAROUSSE*”. <https://www.larousse.fr/dictionnaires/francais/capital/12900>. Consulté le 07 Juin 2022.
- [DD03] Wilfred DOLFSMA et Charlie DANNREUTHER. “Subjects and boundaries : Contesting social capital-based policies”. In : *Journal of Economic Issues* 37.2 (2003), p. 405-413.
- [RSS02] Lindon J ROBISON, A Allan SCHMID et Marcelo E SILES. “Is social capital really capital?” In : *Review of social economy* 60.1 (2002), p. 1-21.

-
- [AK02] Paul S ADLER et Seok-Woo KWON. “Social capital : Prospects for a new concept”. In : *Academy of management review* 27.1 (2002), p. 17-40.
- [Cla04] Tristan CLARIDGE. “Social capital and natural resource management”. In : *Unpublished Thesis, University of Queensland, Brisbane, Australia* (2004).
- [Bru09] Aurélie BRUNIE. “Meaningful distinctions within a concept : Relational, collective, and generalized social capital”. In : *Social science research* 38.2 (2009), p. 251-265.
- [NG98] Janine NAHAPIET et Sumantra GHOSHAL. “Social capital, intellectual capital, and the organizational advantage”. In : *Academy of management review* 23.2 (1998), p. 242-266.
- [Col88] James S COLEMAN. “Social capital in the creation of human capital”. In : *American journal of sociology* 94 (1988), S95-S120.
- [Pal00] Martin PALDAM. “Social capital : one or many? Definition and measurement”. In : *Journal of economic surveys* 14.5 (2000), p. 629-653.
- [Put00] Robert D PUTNAM. “Bowling alone : America’s declining social capital”. In : *Culture and politics*. Springer, 2000, p. 223-234.
- [Ora01] Andy ORAM. *Peer-to-Peer : Harnessing the power of disruptive technologies*. ” O’Reilly Media, Inc.”, 2001.
- [AWW02] Donna ANDERT, Robin WAKEFIELD et Joel WEISE. “Trust modeling for security architecture development”. In : *Sun Microsystems BluePrints* (2002).
- [Deu62] Morton DEUTSCH. “Cooperation and trust : Some theoretical notes.” In : (1962).
- [Mar94] Stephen Paul MARSH. “Formalising trust as a computational concept”. In : (1994).
- [AD01] Karl ABERER et Zoran DESPOTOVIC. “Managing trust in a peer-2-peer information system”. In : *Proceedings of the tenth international conference on Information and knowledge management*. 2001, p. 310-317.

-
- [KSG03] Sepandar D KAMVAR, Mario T SCHLOSSER et Hector GARCIA-MOLINA. “The eigentrust algorithm for reputation management in p2p networks”. In : *Proceedings of the 12th international conference on World Wide Web*. 2003, p. 640-651.
- [DSC05] Claudiu DUMA, Nahid SHAHMEHRI et Germano CARONNI. “Dynamic trust metrics for peer-to-peer systems”. In : *16th International Workshop on Database and Expert Systems Applications (DEXA'05)*. IEEE. 2005, p. 776-781.
- [CJI02] Bled Electronic COMMERCE, Audun JØSANG et Roslan ISMAIL. “The beta reputation system”. In : *In proceedings of the 15th bled electronic commerce conference*. Citeseer. 2002.
- [AXJ15] Ahmad ABDEL-HAFEZ, Yue XU et Audun JØSANG. “A normal-distribution based rating aggregation method for generating product reputations”. In : *Web Intelligence*. T. 13. 1. IOS Press. 2015, p. 43-51.
- [Wie+13] Adam WIERZBICKI et al. “Improving computational trust representation based on Internet auction traces”. In : *Decision Support Systems* 54.2 (2013), p. 929-940.
- [Lee+13] Jin Joo LEE et al. “Computationally modeling interpersonal trust”. In : *Frontiers in psychology* 4 (2013), p. 893.
- [AA14] Mehrdad ASHTIANI et Mohammad Abdollahi AZGOMI. “Contextuality, incompatibility and biased inference in a quantum-like formulation of computational trust”. In : *Advances in Complex Systems* 17.05 (2014), p. 1450020.
- [HWA15] Stephan HAMMER, Michael WISSNER et Elisabeth ANDRÉ. “Trust-based decision-making for smart and adaptive environments”. In : *User Modeling and User-Adapted Interaction* 25.3 (2015), p. 267-293.
- [Lin+15] Hui LIN et al. “Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks”. In : *International Journal of Distributed Sensor Networks* 11.10 (2015), p. 674591.
- [Gai11] Emmanuelle GAILLARD. “Les systèmes informatiques fondés sur la confiance : un état de l’art.” Thèse de doct. Loria & Inria Grand Est, 2011.

-
- [ŠHZ16] Boris ŠKORIĆ, Sebastiaan JA de HOOGH et Nicola ZANNONE. “Flow-based reputation with uncertainty : evidence-based subjective logic”. In : *International Journal of Information Security* 15.4 (2016), p. 381-402.
- [MB15] Elham MAJD et Vimala BALAKRISHNAN. “Selecting advisor agents using reliability, reputation and risks”. In : *Journal of Intelligent & Fuzzy Systems* 29.5 (2015), p. 1835-1846.
- [Aca+16] Giovanni ACAMPORA et al. “An interval type-2 fuzzy logic based framework for reputation management in Peer-to-Peer e-commerce”. In : *Information Sciences* 333 (2016), p. 88-107.
- [JT14] David JELENC et Denis TRČEK. “Qualitative trust model with a configurable method to aggregate ordinal data”. In : *Autonomous agents and multi-agent systems* 28.5 (2014), p. 805-835.
- [Trč14] Denis TRČEK. “Computational trust management, QAD, and its applications”. In : *Informatika* 25.1 (2014), p. 139-154.
- [TMP15] Ginés Dólera TORMO, Félix Gómez MÁRMOL et Gregorio Martínez PÉREZ. “Dynamic and flexible selection of a reputation mechanism for heterogeneous environments”. In : *Future Generation Computer Systems* 49 (2015), p. 113-124.
- [AA16a] Mehrdad ASHTIANI et Mohammad Abdollahi AZGOMI. “A hesitant fuzzy model of computational trust considering hesitancy, vagueness and uncertainty”. In : *Applied Soft Computing* 42 (2016), p. 18-37.
- [SS02] Jordi SABATER et Carles SIERRA. “Reputation and social network analysis in multi-agent systems”. In : *Proceedings of the first international joint conference on Autonomous agents and multiagent systems : Part 1*. 2002, p. 475-482.
- [Pag+99] Lawrence PAGE et al. *The PageRank citation ranking : Bringing order to the web*. Rapp. tech. Stanford InfoLab, 1999.
- [Lev09] Raph LEVIEN. “Attack-resistant trust metrics”. In : *Computing with Social Trust*. Springer, 2009, p. 121-132.

-
- [DFM01] Roger DINGLELINE, Michael FREEDMAN et David MOLNAR. *Peer-to-peer : Harnessing the power of disruptive technology*. 2001.
- [LWL16] Kun LU, Junlong WANG et Mingchu LI. “An Eigentrust dynamic evolutionary model in P2P file-sharing systems”. In : *Peer-to-Peer Networking and Applications* 9.3 (2016), p. 599-612.
- [KT15] Eleni KOUTROULI et Aphrodite TSALGATIDOU. “Reputation systems evaluation survey”. In : *ACM Computing Surveys (CSUR)* 48.3 (2015), p. 1-28.
- [VD04] Fernanda B VIÉGAS et Judith DONATH. “Social network visualization : Can we go beyond the graph”. In : *Workshop on social networks, CSCW*. T. 4. Citeseer. 2004, p. 6-10.
- [ODo+07] John O’DONOVAN et al. “Extracting and Visualizing Trust Relationships from Online Auction Feedback Comments.” In : *IJCAI*. 2007, p. 2826-2831.
- [GKH09] Annie GUERRIERO, Sylvain KUBICKI et Gilles HALIN. “Trust-oriented multi-visualization of cooperation context”. In : *2009 Second International Conference in Visualisation*. IEEE. 2009, p. 96-101.
- [BMP08] Kamaljit Kaur BIMRAH, Haralambos MOURATIDIS et David PRESTON. “Modelling trust requirements by means of a visualization language”. In : *2008 Requirements Engineering Visualization*. IEEE. 2008, p. 26-30.
- [HS10] Chung-Wei HANG et Munindar P SINGH. “Trust-based recommendation based on graph similarity”. In : *AAMAS Workshop on Trust in Agent Societies (Trust)*. Citeseer. 2010, p. 71-81.
- [MA07] Paolo MASSA et Paolo AVESANI. “Trust-aware recommender systems”. In : *Proceedings of the 2007 ACM conference on Recommender systems*. 2007, p. 17-24.
- [And+08] Reid ANDERSEN et al. “Trust-based recommendation systems : an axiomatic approach”. In : *Proceedings of the 17th international conference on World Wide Web*. 2008, p. 199-208.
- [Hes06] Claudia HESS. “Trust-based recommendations for publications : A multi-layer network approach”. In : *TCDL Bulletin* 2.2 (2006), p. 190-201.

-
- [Sch+07] J Ben SCHAFER et al. “Collaborative filtering recommender systems”. In : *The adaptive web*. Springer, 2007, p. 291-324.
- [OMa+04] Michael O’MAHONY et al. “Collaborative recommendation : A robustness analysis”. In : *ACM Transactions on Internet Technology (TOIT)* 4.4 (2004), p. 344-377.
- [PB07] Michael J PAZZANI et Daniel BILLSUS. “Content-based recommendation systems”. In : *The adaptive web*. Springer, 2007, p. 325-341.
- [Agg16] Charu C AGGARWAL. “Content-based recommender systems”. In : *Recommender systems*. Springer, 2016, p. 139-166.
- [Hua08] Shiu-li HUANG. “Comparision of utility-based recommendation methods”. In : *PACIS 2008 Proceedings* (2008), p. 21.
- [Bur00] Robin BURKE. “Knowledge-based recommender systems”. In : *Encyclopedia of library and information systems* 69.Supplement 32 (2000), p. 175-186.
- [Bur02] Robin BURKE. “Hybrid recommender systems : Survey and experiments”. In : *User modeling and user-adapted interaction* 12.4 (2002), p. 331-370.
- [Cla+99] Mark CLAYPOOL et al. “Combining content-based and collaborative filters in an online newspaper”. In : *Proceedings of ACM SIGIR workshop on recommender systems*. T. 60. Citeseer. 1999, p. 1853-1870.
- [Paz99] Michael J PAZZANI. “A framework for collaborative, content-based and demographic filtering”. In : *Artificial intelligence review* 13.5 (1999), p. 393-408.
- [CS00] Paul COTTER et Barry SMYTH. “Ptv : Intelligent personalised tv guides”. In : *AAAI/IAAI*. 2000, p. 957-964.
- [ZLJ21] Qian ZHANG, Jie LU et Yaochu JIN. “Artificial intelligence in recommender systems”. In : *Complex & Intelligent Systems* 7.1 (2021), p. 439-457.
- [SMH07] Ruslan SALAKHUTDINOV, Andriy MNIH et Geoffrey HINTON. “Restricted Boltzmann machines for collaborative filtering”. In : *Proceedings of the 24th international conference on Machine learning*. 2007, p. 791-798.
- [TPV12] Tran The TRUYEN, Dinh Q PHUNG et Svetha VENKATESH. “Ordinal Boltzmann machines for collaborative filtering”. In : *arXiv preprint arXiv : 1205.2611* (2012).

-
- [LBH15] Yann LECUN, Yoshua BENGIO et Geoffrey HINTON. “Deep learning”. In : *nature* 521.7553 (2015), p. 436-444.
- [Zha+19] Shuai ZHANG et al. “Deep learning based recommender system : A survey and new perspectives”. In : *ACM Computing Surveys (CSUR)* 52.1 (2019), p. 1-38.
- [SLH14] Yue SHI, Martha LARSON et Alan HANJALIC. “Collaborative filtering beyond the user-item matrix : A survey of the state of the art and future challenges”. In : *ACM Computing Surveys (CSUR)* 47.1 (2014), p. 1-45.
- [Can+15] Iván CANTADOR et al. “Cross-domain recommender systems”. In : *Recommender systems handbook*. Springer, 2015, p. 919-959.
- [BF85] Donald A BERRY et Bert FRISTEDT. “Bandit problems : sequential allocation of experiments (Monographs on statistics and applied probability)”. In : *London : Chapman and Hall* 5.71-87 (1985), p. 7-7.
- [Sha+05] Guy SHANI et al. “An MDP-based recommender system.” In : *Journal of Machine Learning Research* 6.9 (2005).
- [WLM18] Romain WARLOP, Alessandro LAZARIC et Jérémie MARY. “Fighting boredom in recommender systems with linear reinforcement learning”. In : *Advances in Neural Information Processing Systems* 31 (2018).
- [Zen+16] Chunqiu ZENG et al. “Online context-aware recommendation with time varying multi-armed bandit”. In : *Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining*. 2016, p. 2025-2034.
- [RSP05] Pornthep ROJANAVASU, Phaitoon SRINIL et Ouen PINNGERN. “New Recommendation System Using Reinforcement Learning”. In : (jan. 2005).
- [HR07] Cheul HWANG et Frank Chung-Hoon RHEE. “Uncertain fuzzy clustering : Interval type-2 fuzzy approach to *c*-means”. In : *IEEE Transactions on fuzzy systems* 15.1 (2007), p. 107-120.
- [Yag03] Ronald R YAGER. “Fuzzy logic methods in recommender systems”. In : *Fuzzy Sets and Systems* 136.2 (2003), p. 133-149.

-
- [ZZN10] Azene ZENEBE, Lina ZHOU et Anthony F NORCIO. “User preferences discovery using fuzzy models”. In : *Fuzzy Sets and Systems* 161.23 (2010), p. 3044-3063.
- [Mao+15] Mingsong MAO et al. “A fuzzy content matching-based e-commerce recommendation approach”. In : *2015 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE. 2015, p. 1-8.
- [WZL14] Dianshuang WU, Guangquan ZHANG et Jie LU. “A fuzzy preference tree-based recommender system for personalized business-to-business e-services”. In : *IEEE Transactions on Fuzzy Systems* 23.1 (2014), p. 29-43.
- [Ngu20] C Thi NGUYEN. “Echo chambers and epistemic bubbles”. In : *Episteme* 17.2 (2020), p. 141-161.
- [Sel+20] Chayma SELLAMI et al. “A Hybrid Learning-Based Model for Wine Recommendation”. In : (2020).
- [LSS14] Elad LIEBMAN, Maytal SAAR-TSECHANSKY et Peter STONE. *DJ-MC : A Reinforcement-Learning Agent for Music Playlist Recommendation*. 2014. arXiv : 1401.1880 [cs.LG].
- [Zha+17] Xiangyu ZHAO et al. *Deep Reinforcement Learning for List-wise Recommendations*. 2017. arXiv : 1801.00209 [cs.LG].
- [RM05] Lior ROKACH et Oded MAIMON. “Clustering methods”. In : (2005), p. 321-352.
- [Joh67] Stephen C JOHNSON. “Hierarchical clustering schemes”. In : *Psychometrika* 32.3 (1967), p. 241-254.
- [SB13] K SASIREKHA et P BABY. “Agglomerative hierarchical clustering algorithm-a”. In : *International Journal of Scientific and Research Publications* 83.3 (2013), p. 83.
- [Sav+02] Sergio M SAVARESI et al. “Cluster selection in divisive clustering algorithms”. In : *Proceedings of the 2002 SIAM International Conference on Data Mining*. SIAM. 2002, p. 299-314.

-
- [LZH08] Peter LANGFELDER, Bin ZHANG et Steve HORVATH. “Defining clusters from a hierarchical cluster tree : the Dynamic Tree Cut package for R”. In : *Bioinformatics* 24.5 (2008), p. 719-720.
- [WD92] Christopher JCH WATKINS et Peter DAYAN. “Q-learning”. In : *Machine learning* 8.3 (1992), p. 279-292.
- [SB+98] Richard S SUTTON, Andrew G BARTO et al. *Introduction to reinforcement learning*. T. 135. MIT press Cambridge, 1998.
- [MC12] Fionn MURTAGH et Pedro CONTRERAS. “Algorithms for hierarchical clustering : an overview”. In : *Wiley Interdisciplinary Reviews : Data Mining and Knowledge Discovery* 2.1 (2012), p. 86-97.
- [RV13] Chandan K REDDY et Bhanukiran VINZAMURI. “A Survey of Partitional and Hierarchical Clustering Algorithms.” In : *Data clustering : Algorithms and applications* 87 (2013).
- [EA16] Yeşim ER et Ayten ATASOY. “The classification of white wine and red wine according to their physicochemical qualities”. In : *International Journal of Intelligent Systems and Applications in Engineering* 4.Special Issue-1 (2016), p. 23-26.
- [Jia+19] Liaoliang JIANG et al. “A trust-based collaborative filtering algorithm for E-commerce recommendation system”. In : *Journal of ambient intelligence and humanized computing* 10.8 (2019), p. 3023-3034.
- [YK20] Tzu-Yu YEH et Rasha KASHEF. “Trust-Based collaborative filtering recommendation systems on the blockchain”. In : *Advances in Internet of Things* 10.4 (2020), p. 37-56.
- [Moh+19] Venus MOHAMMADI et al. “Trust-based recommendation systems in Internet of Things : a systematic literature review”. In : *Human-centric Computing and Information Sciences* 9.1 (2019), p. 1-61.
- [Sel+21] Chayma SELLAMI et al. “Towards a unified framework for computational trust and reputation models for e-commerce applications”. In : *International Conference on Research Challenges in Information Science*. Springer, 2021, p. 616-622.

-
- [LB+96] Roy J LEWICKI, Barbara B BUNKER et al. “Developing and maintaining trust in work relationships”. In : *Trust in organizations : Frontiers of theory and research* 114 (1996), p. 139.
- [JP05] Audun JØSANG et Simon POPE. “Semantic constraints for trust transitivity”. In : *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling- Volume 43*. 2005, p. 59-68.
- [KB16] Kalliopi KRAVARI et Nick BASSILIADES. “DISARM : A social distributed agent reputation model based on defeasible logic”. In : *Journal of Systems and Software* 117 (2016), p. 130-152.
- [PS13] Isaac PINYOL et Jordi SABATER-MIR. “Computational trust and reputation models for open multi-agent systems : a review”. In : *Artificial Intelligence Review* 40.1 (2013), p. 1-25.
- [LDR13] Xin LIU, Anwitaman DATTA et Krzysztof RZADCA. “Trust beyond reputation : A computational trust model based on stereotypes”. In : *Electronic Commerce Research and Applications* 12.1 (2013), p. 24-39.
- [AA16b] Mehrdad ASHTIANI et Mohammad Abdollahi AZGOMI. “A formulation of computational trust based on quantum decision theory”. In : *Information Systems Frontiers* 18.4 (2016), p. 735-764.
- [Zho+14] Yuhui ZHONG et al. “A computational dynamic trust model for user authorization”. In : *IEEE Transactions on Dependable and Secure Computing* 12.1 (2014), p. 1-15.
- [CSS16] Kamalanathan CHANDRAN, Valarmathy SHANMUGASUDARAM et Kirubakaran SUBRAMANI. “Designing a Fuzzy-Logic Based Trust and Reputation Model for Secure Resource Allocation in Cloud Computing.” In : *International Arab Journal of Information Technology (IAJIT)* 13.1 (2016).
- [AH00b] A ABDUL-RAHMAN et S HAILES. “Supporting Trust in Virtual Communities : Proc”. In : *IEEE International Conference on System Sciences*. 2000.
- [DFM00] R DINGLEDINE, M FREEDMAN et D MOLNAR. *Accountability measures for peer-to-peer systems, Peer-to-Peer : Harnessing the Power of Disruptive Technologies*. 2000.

-
- [Fis94] Hans FISCHER. “Dirichlet’s contributions to mathematical probability theory”. In : *Historia mathematica* 21.1 (1994), p. 39-63.
- [Sel+22] Chayma SELLAMI et al. “Trust Model Recommendation Driven by Application Requirements”. In : *International Conference on Research Challenges in Information Science*. Springer. 2022, p. 694-702.
- [Maz15] Frédéric MAZZELLA. “BlaBlaCar et le tourisme collaboratif”. In : *Réalités Industrielles* (2015), p. 54.
- [Bra+18] Diego De Siqueira BRAGA et al. “Survey on computational trust and reputation models”. In : *ACM Computing Surveys (CSUR)* 51.5 (2018), p. 1-40.
- [Whi04] Stephen A WHITE. “Introduction to BPMN”. In : *Ibm Cooperation* 2.0 (2004), p. 0.
- [JBR96] Ivar JACOBSON, Grady BOOCH et James RUMBAUGH. “The Unified Modeling Language”. In : *University Video Communications* (1996).
- [And+03] Tony ANDREWS et al. *Business process execution language for web services*. 2003.
- [LV04] Quentin LIMBOURG et Jean VANDERDONCKT. “Comparing task models for user interface design”. In : *The handbook of task analysis for human-computer interaction* 6 (2004), p. 135-154.
- [PMM97] Fabio PATERNO, Cristiano MANCINI et Silvia MENICONI. “ConcurTaskTrees : A diagrammatic notation for specifying task models”. In : *Human-computer interaction INTERACT’97*. Springer. 1997, p. 362-369.
- [VLB96] Gerrit C VAN DER VEER, Bert F LENTING et Bas AJ BERGEVOET. “GTA : Groupware task analysis—Modeling complexity”. In : *Acta psychologica* 91.3 (1996), p. 297-322.
- [SP89] Dominique SCAPIN et Christine PIERRET-GOLBREICH. “Towards a method for task description : MAD”. In : *Work with display units* 89 (1989), p. 371-380.
- [Luc05] Vincent LUCQUIAUD. “Sémantique et outil pour la modélisation des tâches utilisateur : N-MDA”. Thèse de doct. Poitiers, 2005.

-
- [HSH90] H Rex HARTSON, Antonio C SIOCHI et Deborah HIX. “The UAN : A user-oriented representation for direct manipulation interface designs”. In : *ACM Transactions on Information Systems (TOIS)* 8.3 (1990), p. 181-203.
- [MH89] Karen L MCGRAW et Karen HARBISON-BRIGGS. “Knowledge acquisition : Principles and guidelines”. In : (1989).
- [Caf09] Sybille CAFFIAU. “Approche dirigée par les modèles pour la conception et la validation des applications interactives : une démarche basée sur la modélisation des tâches”. Thèse de doct. ISAE-ENSMA Ecole Nationale Supérieure de Mécanique et d’Aérotechnique-Poitiers, 2009.





Résumé

De nos jours, les réseaux sociaux constituent un élément essentiel de la vie des personnes du monde entier. Le World Wide Web est le principal outil utilisé pour partager des informations et interagir avec d'autres personnes via Internet. Pour s'adapter à l'évolution du Web, les techniques de recherche d'information ont dû intégrer des aspects sociaux et axés sur l'utilisateur et son comportement. Parmi ces techniques, on parle dans ce travail des systèmes de recommandation.

En effet, la majorité de ces réseaux et systèmes n'offrent pas de réelles garanties sur le respect de la vie privée des utilisateurs (c'est-à-dire, ils collectent des données d'identités des consommateurs). Ce travail de thèse s'inscrit dans le cadre de la famille des réseaux dits « anonymes » où l'anonymat des utilisateurs est complètement respecté (non-collecte des informations liées à leurs identités). On peut donc se demander comment les utilisateurs peuvent se faire confiance et se fier aux informations fournies par ces systèmes tout en étant anonymes? Il est donc essentiel d'instaurer un modèle confiance au sein du réseau social. Plusieurs travaux de recherche ont été menés pour développer des réseaux sociaux et des systèmes de recommandation à base de confiance. Ces systèmes utilisent des relations de confiance entre les utilisateurs pour prédire les évaluations de confiance en fonction des expériences et des commentaires.

Bien que l'exploitation de ces relations d'interaction soit souvent efficace pour améliorer les résultats fournis par les systèmes de recommandation, on peut néanmoins noter quelques problèmes. Le premier concerne la nature statique de certains systèmes de recommandation et qui ne s'adaptent donc pas aux changements des comportements des utilisateurs. Le deuxième problème concerne la modélisation de la confiance. Ce concept est utilisé dans plusieurs domaines, cependant, une définition uniforme et consensuelle de ce concept n'existe pas. Le troisième problème a trait à la variation des modèles computationnels dans les systèmes à base de confiance. En fait, les interactions entre les utilisateurs génèrent des nouvelles données ce qui peut mener un utilisateur à changer son comportement et ses activités dans le système. Ce qui va créer des variations dans les profils utilisateurs. Certains utilisateurs ont des comportements corrects dans le système, d'autres peuvent faire des activités malveillantes. D'autres utilisateurs font confiance rapidement, d'autres sont méfiants à l'égard des inconnus, etc. Tous ces comportements doivent conduire à un (re)calcul de la valeur de la confiance selon différents modèles computationnels.

Dans le cadre de cette thèse, dans un premier temps, un travail sur les systèmes de recommandation a été réalisé afin de trouver une solution pour la nature statique de ces systèmes. Cette solution utilise des techniques issues de l'apprentissage par renforcement. Dans un second temps, nous avons proposé un cadre unifié de gestion de la confiance tant au niveau sémantique qu'au niveau calculatoire. Une analyse approfondie pour comprendre l'intuition derrière chaque modèle computationnel a également été introduite. Enfin, la question de la sélection d'un modèle computationnel le plus approprié, selon la nature des besoins des utilisateurs, a aussi été abordée.

Mots-clés : Réseaux sociaux, Anonymat, Capital social, Confiance, Systèmes de Recommandation, Apprentissage, Modèles Computationnels

Abstract

Today, social networking is an essential part of the lives of people around the world. The World Wide Web is the primary tool used to share information and interact with others via the Internet. To adapt to the evolution of the Web, information retrieval techniques have had to incorporate social and user-centered aspects and behavior. Among these techniques, we talk in this work about recommendation systems.

However, the majority of these networks and systems do not offer real guarantees on the respect of the users' privacy (i.e., they collect consumers' identity data). This thesis is part of the family of so-called "anonymous" networks where the anonymity of users is completely respected (no collection of information related to their identities). We can therefore ask ourselves how users can trust and rely on the information provided by these systems while being anonymous? It is therefore essential to establish a trust model within the social network. Several research works have been conducted to develop trust-based social networks and recommendation systems. These systems use trust relationships between users to predict trust ratings based on experiences and comments.

Although the exploitation of these interaction relationships is often effective in improving the results provided by recommender systems, there are a few problems that can be noted. The first one concerns the static nature of some recommender systems, which do not adapt to changes in user behavior. The second problem concerns the modeling of trust. This concept is used in several domains, however, a uniform and consensual definition of this concept does not exist. The third problem relates to the variation of computational models in trust-based systems. In fact, interactions between users generate new data which can lead a user to change his behavior and activities in the system. This will create variations in user profiles. Some users behave correctly in the system, others may do malicious activities. Other users are quick to trust, others are suspicious of strangers, etc. All these behaviors must lead to a (re)calculation of the value of trust according to different computational models.

In the context of this thesis, in a first step, a work on recommender systems has been done in order to find a solution for the static nature of these systems. This solution uses techniques from reinforcement learning. In a second step, we proposed a unified framework for trust management at both the semantic and computational levels. An in-depth analysis to understand the intuition behind each computational model has also been introduced. Finally, the issue of selecting the most appropriate computational model, depending on the nature of the users' needs, has also been addressed.

Keywords : Social networks, Anonymity, Social capital, Trust, Recommendation systems, Learning, Computational models.