Université de Montréal

Mise en œuvre d'une approche sociotechnique de la vie privée pour les systèmes de paiement et de recommandation en ligne

Par

Ghada El Haddad

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Thèse présentée à la Faculté des Arts et des Sciences

En vue de l'obtention du grade de Philosophiae Doctor (Ph.D.)

En Informatique

Décembre 2019

Université de Montréal

Faculté des Arts et des Sciences

Cette thèse intitulée :

Mise en œuvre d'une approche sociotechnique de la vie privée pour les systèmes de paiement et de recommandation en ligne

Présentée par :

Ghada El Haddad

a été évaluée par un jury composé de :

Claude Frasson, Président du jury

Esma Aïmeur, Directrice de recherche

Gilles Brassard, Membre du jury

Luigi Logrippo, Examinateur externe

Résumé

Depuis ses fondements, le domaine de l'Interaction Homme-Machine (*IHM*) est marqué par le souci constant de concevoir et de produire des systèmes numériques utiles et utilisables, c'est-à-dire adaptés aux utilisateurs dans leur contexte. Vu le développement exponentiel des recherches dans les IHM, deux états des lieux s'imposent dans les environnements en ligne : le concept de confiance et le comportement de l'usager. Ces deux états ne cessent de proliférer dans la plupart des solutions conçues et sont à la croisée des travaux dans les interfaces de paiements en ligne et dans les systèmes de recommandation. Devant les progrès des solutions conçues, l'objectif de cette recherche réside dans le fait de mieux comprendre les différents enjeux dans ces deux domaines, apporter des améliorations et proposer de nouvelles solutions adéquates aux usagers en matière de perception et de comportement en ligne. Outre l'état de l'art et les problématiques, ce travail est divisé en cinq parties principales, chacune contribue à mieux enrichir l'expérience de l'usager en ligne en matière de paiement et recommandations en ligne :

- **Analyse des multi-craintes en ligne** : nous analysons les différents facteurs des sites de commerce électronique qui influent directement sur le comportement des consommateurs en matière de prise de décision et de craintes en ligne. Nous élaborons une méthodologie pour mesurer avec précision le moment où surviennent la question de la confidentialité, les perceptions en ligne et les craintes de divulgation et de pertes financières.
- **Intégration de personnalisation, contrôle et paiement conditionnel** : nous proposons une nouvelle plateforme de paiement en ligne qui supporte à la fois la personnalisation et les paiements multiples et conditionnels, tout en préservant la vie privée du détenteur de carte.
- **Exploration de l'interaction des usagers en ligne versus la sensibilisation à la cybersécurité** : nous relatons une expérience de magasinage en ligne qui met en relief la perception du risque de cybercriminalité dans les activités en ligne et le comportement des utilisateurs lié à leur préoccupation en matière de confidentialité.

- **Équilibre entre utilité des données et vie privée** : nous proposons un modèle de préservation de vie privée basé sur l'algorithme « *k*-means » et sur le modèle « *k*-coRating » afin de soutenir l'utilité des données dans les recommandations en ligne tout en préservant la vie privée des usagers.
- **Métrique de stabilité des préférences des utilisateurs** : nous ciblons une meilleure méthode de recommandation qui respecte le changement des préférences des usagers par l'intermédiaire d'un réseau neural. Ce qui constitue une amélioration à la fois efficace et performante pour les systèmes de recommandation.

Cette thèse porte essentiellement sur quatre aspects majeurs liés : 1) aux plateformes des paiements en ligne, 2) au comportement de l'usager dans les transactions de paiement en ligne (prise de décision, multi-craintes, cybersécurité, perception du risque), 3) à la stabilité de ses préférences dans les recommandations en ligne, 4) à l'équilibre entre vie privée et utilité des données en ligne pour les systèmes de recommandation.

Mots-clés : vie privée, paiements en ligne, protocole, protection des données, contrôle, système de recommandation, cyber sécurité, filtrage collaboratif.

Abstract

Technologies in Human-Machine Interaction (*HMI*) are playing a vital role across the entire production process to design and deliver advanced digital systems. Given the exponential development of research in this field, two concepts are largely addressed to increase performance and efficiency of online environments: trust and user behavior. These two extents continue to proliferate in most designed solutions and are increasingly enriched by continuous investments in online payments and recommender systems. Along with the trend of digitalization, the objective of this research is to gain a better understanding of the various challenges in these two areas, make improvements and propose solutions more convenient to the users in terms of online perception and user behavior. In addition to the state of the art and challenges, this work is divided into five main parts, each one contributes to better enrich the online user experience in both online payments and system recommendations:

- **Online customer fears**: We analyze different components of the website that may affect customer behavior in decision-making and online fears. We focus on customer perceptions regarding privacy violations and financial loss. We examine the influence on trust and payment security perception as well as their joint effect on three fundamentally important customers' aspects: confidentiality, privacy concerns and financial fear perception.
- **Personalization, control and conditional payment**: we propose a new online payment platform that supports both personalization and conditional multi-payments, while preserving the privacy of the cardholder.
- **Exploring user behavior and cybersecurity knowledge**: we design a new website to conduct an experimental study in online shopping. The results highlight the impact of user's perception in cybersecurity and privacy concerns on his online behavior when dealing with shopping activities.
- **Balance between data utility and user privacy**: we propose a privacy-preserving method based on the "*k*-means" algorithm and the "*k*-coRating" model to support the utility of data in online recommendations while preserving user's privacy.

- **User interest constancy metric**: we propose a neural network to predict the user's interests in recommender systems. Our aim is to provide an efficient method that respects the constancy and variations in user preferences.

In this thesis, we focus on four major contributions related to: 1) online payment platforms, 2) user behavior in online payments regarding decision making, multi-fears and cyber security 3) user interest constancy in online recommendations, 4) balance between privacy and utility of online data in recommender systems.

Keywords: privacy, online payment, payment protocol, data protection, data control, recommender system, cybersecurity, collaborative filtering.

Table des matières

Liste des tableaux

Liste des figures

Liste des algorithmes

Liste des sigles

E-PPSM	E-payment Plan Service Manager Service du plan de paiement électronique
VCC	Virtual Credit Card Carte de Crédit virtuelle
PAYCTRI	PAYment Transactions with Cybersecurity Incidents
CNP	Card not present Carte non présente
PC Engine	Payment Conditional Engine Moteur de paiement conditionnel
UIS	User Interest Stability

Dédicace

À mes chers parents qui ont éclairé ma vie et

à mes précieux enfants qui ont illuminé mes moments

Remerciements

Au terme de ce travail de recherche, je suis convaincue que cette thèse est loin d'être un travail solitaire. Je tiens donc à remercier tous ceux qui, de loin ou de près, ont contribué à la réalisation de cette thèse.

Je remercie infiniment mes parents. Il m'est impossible d'oublier leurs encouragements qui m'ont toujours accompagnée. Une pensée particulière à mon père qui nous a quittés pour un monde meilleur. Ses conseils ont été et restent pour moi les piliers fondateurs de ce que je suis.

Je tiens à exprimer mes plus sincères remerciements à ma directrice de recherche Professeure Esma Aïmeur qui m'a encadrée tout au long de cette thèse et qui m'a orientée vers les bonnes directions. Je la remercie pour la confiance qu'elle m'a toujours accordée, pour son soutien solide dès le premier jour au doctorat et pour ses instructions au cours de l'élaboration de cette thèse. J'ai énormément appris de ses conseils et de ses remarques durant ce long parcours, et ces quelques lignes sont peu de choses par rapport à tout ce qu'elle m'a apporté.

Mes remerciements s'adressent également aux membres du jury qui ont accepté d'évaluer ce travail, Professeur Claude Frasson et Professeur Gilles Brassard. En particulier, je tiens à remercier sincèrement Professeur Luigi Logrippo pour le temps qu'il a consacré à la lecture de cette thèse.

J'adresse mes remerciements à mes collègues du laboratoire HERON pour les suggestions inspirantes tout au long de ces années de travail. Je les remercie pour toutes nos discussions intéressantes et les travaux en commun qui ont été et resteront des motivations pour mes projets professionnels.

Je remercie très chaleureusement mes sœurs qui m'ont encouragé depuis la maitrise à continuer mon parcours académique pendant plusieurs discussions téléphoniques.

Ces remerciements seraient incomplets si je n'en adressais pas à ma famille qui connait très bien rendre les moments agréables. Leur bonne humeur et leur enthousiasme m'ont permis d'écarter les doutes et d'aller en avant dans ce travail de thèse.

Chapitre 1 : Introduction

De nos jours, les services en ligne sont de plus en plus nombreux et disponibles à travers des sites diversifiés (Woo & Liu, 2019). Les activités telles que la collecte des données, la négociation, l'achat et la vente, le financement des projets, la prise de décision en groupe, l'entrepreneuriat, l'établissement des planifications, la publicité, l'initiation d'un partenariat et d'une alliance, la fabrication, le marketing, la distribution, la prestation des services, et la maintenance à distance sont de plus en plus tributaires d'Internet (Heath, 2017). Ces dernières années, avec le développement du Web et plus particulièrement des plateformes en commerce électronique, l'intérêt pour les systèmes de recommandation et les systèmes de paiement en ligne a considérablement augmenté (Adomavicius*, et al.*, 2017). Au cours de la dernière décennie, ces deux domaines ont subi une évolution dans nos usages en termes de services en ligne ce qui constitue le point de départ de notre thèse.

Prenons l'exemple de Bob, un client en ligne, qui effectue des recherches afin de trouver une imprimante pour son bureau. Bob n'est pas à l'aise. Il n'est ni confiant, ni satisfait de la transaction qu'il voulait effectuer sur un des sites d'un fournisseur. Le site apparait mal organisé, il n'y a pas de signes de sécurité sur la page de paiement. De multiples craintes l'envahissent, et peuvent affecter son attitude, sa perception du risque et son expérience en ligne. De plus, Bob n'a pas de contrôle sur les paiements exécutés ni sur les données échangées, ce qui expose sa vie privée à des menaces et à des risques de divulgation. Ce qui l'intrigue le plus, c'est que le système lui propose à plusieurs reprises des produits non satisfaisants sans tenir compte de la possibilité qu'il puisse changer d'avis.

À un degré moindre, il est nécessaire de trouver des solutions centrées sur l'utilisateur qui permettront à Bob d'être plus exigeant en matière de vie privée, plus conscient des risques et plus satisfait des recommandations fournies en ligne.

1.1 Contexte

Ce travail trouve ses origines dans les domaines des paiements en ligne et des systèmes de recommandation.

D’une part, les systèmes de paiement ont beaucoup évolué lors des quarante dernières années avec l’apparition des cartes bancaires et des moyens de paiement électronique. Le paiement en ligne est très répandu du fait de la démocratisation d’Internet et des paiements via l’ordinateur. De nombreux utilisateurs ont recours à cette forme de paiement qui ne demande aucun investissement majeur d’équipement ou de mise en place. Avec la dématérialisation et l'introduction de la carte de crédit, l'évolution des moyens de paiement s’est plus récemment alignée sur celle des technologies numériques.

D’autre part, le but des systèmes de recommandation est de prédire l’affinité entre un utilisateur et un article, en se fondant sur un ensemble d’informations déjà acquises sur cet utilisateur et sur d’autres usagers, ainsi que sur cet article et sur d’autres items. Il est possible de classer les systèmes de recommandation de différentes manières. La classification la plus connue est basée selon trois approches : la recommandation basée sur le *contenu*, la recommandation par *filtrage collaboratif* et la recommandation *hybride* (H. Wang*, et al.*, 2015). Par exemple, dans une plateforme de magasinage, un feedback peut consister en des notes ou avis que les clients peuvent attribuer aux contenus. Toutes les actions et les feedbacks des utilisateurs peuvent être enregistrés dans la base de données du système de recommandation, et être utilisés par la suite pour générer de nouvelles recommandations.

Cette thèse porte essentiellement sur quatre aspects majeurs liés : 1) aux plateformes des paiements en ligne, 2) au comportement de l’usager dans les transactions de paiement en ligne (prise de décision, multi-craintes, cybersécurité, et perception du risque, 3) à la stabilité de ses préférences dans les recommandations en ligne, 4) à l’équilibre entre vie privée et utilité des données en ligne pour les systèmes de recommandation.

1.2 Motivations

Il est primordial de noter que, dans notre vie quotidienne, indépendamment de notre attitude envers la technologie, nous avons forcément divulgué des renseignements personnels en ligne soit en remplissant une demande d'emploi, en obtenant une carte de fidélité en magasin, ou encore en utilisant une carte de crédit sur un site pour la première fois. Ces informations peuvent être mal utilisées comme dans la publicité non sollicitée, la

discrimination, les vols d'identité ou même le harcèlement criminel (Bettini & Riboni, 2015).

Une réflexion sur le déroulement de la transaction en ligne vis-à-vis des **recommandations** et **paiements** nous a menés à vouloir analyser différents aspects et à trouver des solutions ou des méthodes qui peuvent contribuer à apporter des améliorations aux deux domaines. D'une part, la perception de la vie privée, les craintes en ligne ainsi que le domaine de la cybersécurité engendrent des impacts significatifs sur le comportement de l'utilisateur en ligne. D'autre part, l'utilisateur parcourt les recommandations, fournit un feedback implicite ou explicite, change potentiellement son avis de multiples fois et met sa vie privée en péril (préférences, choix, historiques de ses activités). Par conséquent, il est nécessaire de trouver des solutions de paiement en ligne centrées sur l'utilisateur ainsi que des améliorations dans les systèmes de recommandation. C'est ce qui nous amène à formuler les cinq objectifs de notre thèse.

1.3 Objectifs de recherche

Dans la section précédente, nous avons exprimé nos motivations de recherche selon trois sujets : les paiements en ligne, le comportement des utilisateurs en ligne ainsi que les systèmes de recommandation. Nous nous proposons de réaliser les objectifs suivants :

Dans un premier temps, nous présentons les diverses craintes des usagers dans les paiements en ligne et les exigences de protection de vie privée ainsi que les données financières, lesquelles suscitent beaucoup de réflexions et méritent que nous nous y attardions. Cet objectif aide à analyser les préoccupations des clients et à examiner les facteurs par rapport à la confiance, à la perception de la sécurité des paiements ainsi qu'à leur effet conjoint. Nous nous efforçons dans notre recherche de répondre aux questions suivantes : (1) quels sont les facteurs qui accroissent les craintes des utilisateurs en ligne ? (2) Quels sont les facteurs qui mènent à une prise de décision ? (3) Comment renforcer la confiance ainsi que la satisfaction du consommateur ? (4) Comment éviter les sentiments de craintes et favoriser le sentiment de quiétude chez l'utilisateur durant une transaction en ligne ?

Dans un deuxième temps, nous proposons une nouvelle plateforme de paiement en ligne dont l'objectif vise à fournir un environnement de paiement en ligne incluant toutes les étapes qui mènent à conclure une transaction de paiement.

Dans un troisième temps, nous abordons le sujet de la cybersécurité, dans le contexte d'une expérience en ligne. Pour cet objectif, nous soulignons l'importance de sensibiliser les personnes à la cybersécurité à travers un questionnaire en ligne. Nos constatations mènent à deux ensembles d'actions : réduire le risque perçu de cybercriminalité dans les activités en ligne tout en augmentant le niveau de connaissance en cybersécurité.

Dans un quatrième temps, nous nous intéressons à la vie privée vis-à-vis des systèmes de recommandation qui jouent un rôle essentiel dans les expériences des usagers en ligne. Assurer la protection de la vie privée dans les systèmes de recommandation demeure un défi de recherche, et dans ce document, nous étudions l'équilibre entre la vie privée et l'utilité des informations publiées. Les préoccupations en matière de protection de vie privée sont dues au problème de la recommandation de filtrage collaboratif visant à préserver la vie privée. Pour ce faire, nous proposons une méthode de préservation de vie privée basée sur l'algorithme « *k*-means » et sur le modèle « *k*-coRating » (F. Zhang*, et al.*, 2014; Zhang*, et al.*, 2019).

Toujours dans le cadre des systèmes de recommandation, notre cinquième objectif vise à améliorer une de leurs fonctions, qui est la prédiction pour assurer une affinité entre un utilisateur et un produit. Le but est de fournir à l'utilisateur des suggestions/recommandations en se fondant sur un ensemble d'informations déjà acquises sur cet utilisateur et sur ceux qui lui sont similaires. Pour ce faire, nous proposons un réseau neuronal pour prédire le goût de l'utilisateur en fonction de la séquence des éléments sélectionnés et des caractéristiques des éléments en supposant que le goût de l'utilisateur ne change pas radicalement. La stabilité des préférences des utilisateurs est démontrée dans notre méthode de prédiction qui consiste à générer des recommandations fournissant des éléments innovants et différents aux utilisateurs dont les préférences peuvent changer avec le temps.

1.4 Organisation du document

Cette thèse est organisée en neuf chapitres consignés dans le tableau suivant.

Chapitre	Contenu
Introduction	Introduire les motivations et les objectifs de la thèse.
Vue globale des paiements en ligne	Présenter les fondements théoriques de sécurité, les éléments principaux et leurs fonctions ainsi que les protocoles dans le mécanisme des paiements en ligne.
Problématique de recherche	Présenter les problématiques sur lesquelles porte cette thèse.
Multi-craintes des usagers en ligne	Présenter et discuter des résultats d'une étude empirique afin d'analyser les facteurs de la confiance, de la perception de la sécurité ainsi que leurs effets sur la confidentialité et les craintes financières dans le contexte des paiements en ligne.
Nouvelle plateforme de paiement en ligne	Proposer une nouvelle plateforme de paiement en ligne.
Cybersécurité dans le contexte de paiement en ligne	Présenter et discuter des résultats d'une expérience de magasinage en ligne dans le contexte d'une sensibilisation à la cybersécurité.
Équilibre entre vie privée et utilité dans les systèmes de recommandation	Discuter des principales notions liées aux systèmes de recommandation et proposer un modèle de préservation de la vie privée basé sur l'algorithme *k*-means et le modèle *k*-coRating.
Stabilité des préférences dans les systèmes de recommandation	Proposer un réseau neuronal de prédiction du goût de l'utilisateur dans le contexte des systèmes de recommandation
Conclusions et travaux futurs	Résumer nos contributions ainsi que les travaux futurs envisagés.

Chapitre 2 : Vue globale des paiements en ligne

Au cours des dernières années, l'accroissement des technologies de la communication a mené à la mise en place des transactions électroniques pour échanger, en tout temps, des biens et des services variés en ligne. À travers le service bancaire, les courriels, le commerce et le vote électronique ainsi que les réseaux sociaux, divers domaines ont bénéficié d'importantes innovations. Le marché du paiement en ligne a aussi progressé avec les diverses méthodes de paiements disponibles pour l'usager. Depuis plusieurs décennies, ce domaine était stable avec des participants dont chacun possédait un rôle bien défini (acquéreurs et les émetteurs), des modèles d'affaires rentables (les systèmes de cartes) et un environnement dans lequel les marchands s'occupaient de frais associés aux paiements (Staykova & Damsgaard, 2015).

Dans ce chapitre, nous allons aborder le processus du paiement avec toutes les exigences demandées pour assurer une transaction électronique sécurisée. Nous accordons une attention particulière aux différents protocoles qui la supportent.

2.1 Aperçu de base

Depuis quelques décennies, le marché de paiement a bénéficié d'une croissance rapide due à la progression des systèmes de paiements électroniques. Plusieurs solutions de paiement ont été déployées (Ashrafi & Ng, 2009; X. Chen*, et al.*, 2014; Mazumdar & Giri, 2012; S. Roy & Venkateswaran, 2014; J.-h. Wang*, et al.*, 2009). Monnaies électroniques (*E-Cash*), cartes prépayées, cartes de crédit, cartes de débit et chèques électroniques sont largement utilisées dans des environnements de commerce électronique. Nous les décrivons comme suit :

- **Monnaies électroniques** (E-Cash) : Les clients peuvent régler leurs transactions par l'intermédiaire d'un échange de monnaie électronique.

- **Cartes prépayées** : Le client inscrit un numéro de carte unique sur le site du marchand. Ce numéro est lié à une carte prépayée pour une durée spécifiée. Le montant versé au marchand est déduit de la valeur de la carte.
- **Cartes de crédit** : Le client est authentifié avant tout achat. Une vérification est effectuée par un serveur avec la banque si des fonds suffisants sont disponibles. Les frais de la transaction sont validés avec le compte du client ; et le client paiera le solde de la facture à la banque.
- **Cartes de débit** : Le client conserve un solde positif dans son compte, la transaction, les frais seront déduits du compte immédiatement.
- **Chèques électroniques** : Une institution financière règle électroniquement les transactions entre la banque de l'acheteur et la banque du vendeur sous forme d'un chèque électronique.

Après avoir cité les différentes méthodes de paiement, nous nous concentrons dans la prochaine section sur les méthodes de paiement basées sur la carte de crédit en développant les différentes entités qui y participent.

2.2 Entités principales

Malgré la multitude de solutions de paiement, les systèmes basés sur la carte restent les plus courants. Prenons la méthode de paiement en ligne par l'intermédiaire de la carte de crédit. Dans ce contexte, la transaction se déroule dans un milieu de confiance envers le fournisseur du service par lequel les informations bancaires du client transitent (Mazumdar & Giri, 2012; Omariba*, et al.*, 2012). Ceci s'établit aussi dans un environnement sécurisé selon un protocole tel que SSL/TLS (Secure Sockets Layers/Transport Layer Security). De tels protocoles permettent de sécuriser la transaction entre le client et le fournisseur de service, mais ne fournissent pas de véritable authentification du client.

Le schéma, illustré dans la Figure 1, présente les étapes du paiement consécutives et interactives. Comme cela est indiqué, différentes entités sont impliquées dans une transaction de paiement électronique (Gómez*, et al.*, 2018; Gommans*, et al.*, 2015). Chacun

possède un rôle défini et bien précis. Nous citons : le client, le marchand, la banque du client et la banque du marchand. Leurs rôles peuvent être décrits comme suit :

- Le client est l'entité qui réalise la commande sur les sites d'achats. Une fois décidé, il procède à la prochaine étape pour accomplir le paiement avec le marchand.
- Le marchand est l'entité qui offre les articles ou les services sur le Web et les rend disponibles pour le client afin de satisfaire son achat.
- La banque du client ou l'émetteur de la carte du client : son rôle est d'authentifier le client, de valider les informations bancaires reçues et d'effectuer le retrait de la transaction du paiement effectuée.
- La banque du marchand ou l'acquéreur est l'entité qui s'occupe de recevoir les données du client et les envoie à l'émetteur pour les valider. Il possède les comptes du marchand et est capable de les valider.

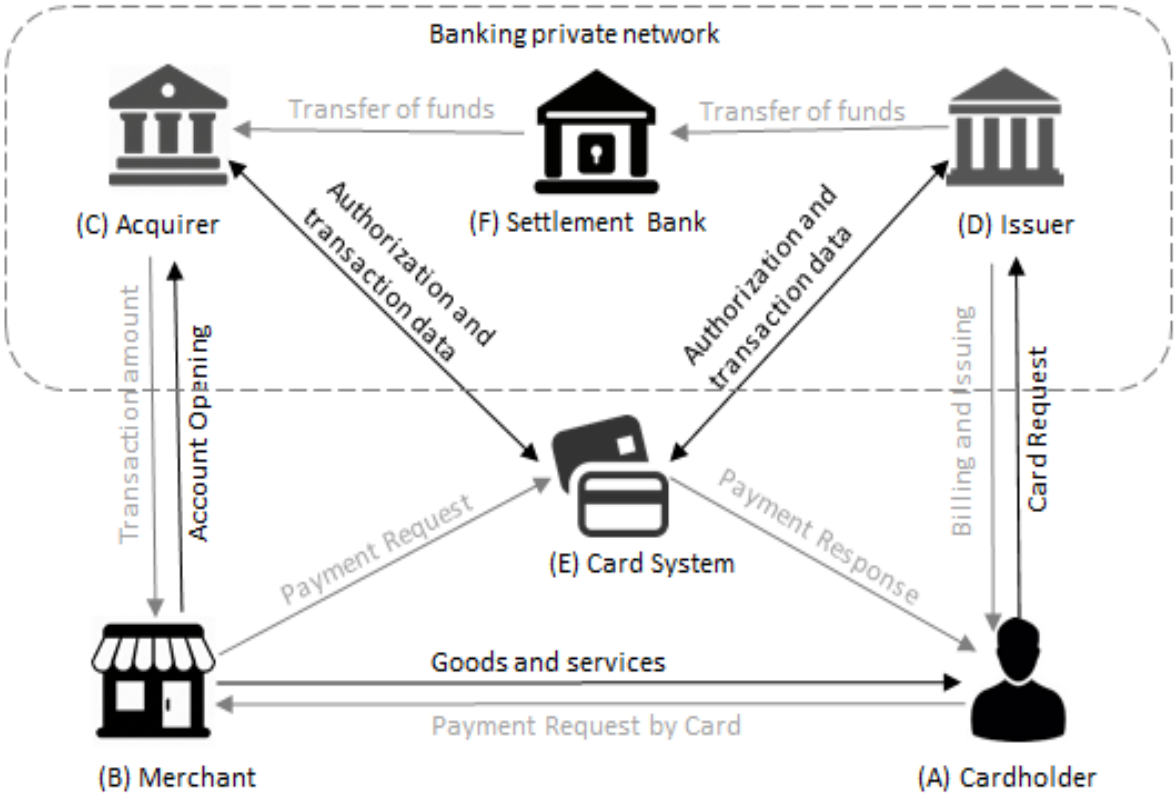

Figure 1 - Éléments et flot d'information du paiement en ligne.

Dans le but de mieux comprendre le processus de paiement par carte de crédit, nous précisons, dans la prochaine section, avec plus de détails, les différentes entités du schéma ainsi que les étapes du processus en les projetant sur un schéma de paiement plus simple.

2.3 Schéma de paiement simplifié

Dans cette section, nous envisageons une architecture de paiement simplifié (Gómez*, et al.*, 2018) telle qu'illustrée dans la Figure 2. Notre but est de décrire, à partir de ce schéma, une représentation du cycle complet des transactions. Ce cycle est généralement caractérisé par les différentes entités et les étapes qui caractérisent le processus de paiement en ligne par carte de crédit.

D'un point de vue général, chaque transaction de carte de crédit est le résultat d'une série d'interactions entre plusieurs participants.

Le premier participant est le client qui souhaite réaliser un achat sur le site Internet d'un fournisseur de service qui est la seconde entité. Une fois décidé, le client déclenche le paiement en utilisant sa carte de crédit. Ce phénomène ajoute deux autres participants essentiels pour intervenir dans le processus du paiement. Ce sont *l'émetteur* et *l'acquéreur*.

En effet, l'émetteur de la carte de crédit émet la carte pour un titulaire afin de lui permettre d'accomplir des achats. En général, l'émetteur peut être la banque ou une institution financière. Il offre des avantages et des services différents à ses clients et propose plusieurs types de cartes de crédit.

Quant à l'acquéreur, il intervient auprès du marchand pour lui offrir différentes méthodes techniques pour pouvoir accepter les transactions par carte de crédit. Grâce aux acquéreurs, le marchand est capable de se connecter avec différents émetteurs de carte et réglementer les commandes. Cela peut être la banque ou l'institut financier qui va procéder aux transactions, recevoir l'argent des émetteurs de cartes et transmettre au compte du marchand. Tout ce que nous venons de décrire se résume dans le Tableau 1.

Un cinquième acteur est souvent impliqué. Il s'agit d'un tiers de confiance qui joue le rôle d'une entité tierce ou d'un intermédiaire entre l'acquéreur et l'émetteur de carte. Son rôle permet d'assurer une plateforme de paiement tiers et de garantir la sécurité des transactions des acheteurs et des vendeurs dans des environnements de commerce électronique (Micu, 2016; Yao*, et al.*, 2018).

Tableau 1 - Descriptif détaillé du processus de paiement en ligne

Étape	Entités	Description
1	Client et Marchand	Le client accomplit la commande et déclenche le paiement en utilisant sa carte de crédit.
2	Marchand et Acquéreur	Le marchand reçoit la demande de paiement et envoie une requête à l'acquéreur pour valider les informations de la transaction provenant de la carte et demande l'autorisation pour le paiement.
3	Acquéreur et Émetteur	L'acquéreur soumet la requête à l'émetteur de la carte pour authentifier le client et autoriser le paiement.
4	Émetteur et Acquéreur	L'émetteur de la carte vérifie les données du client ainsi que son compte et répond à l'acquéreur pour accepter ou refuser.
5	Acquéreur et Marchand	L'acquéreur renvoie au marchand la réponse concernant l'authentification du client et l'autorisation du paiement est soit acceptée ou refusée.
6	Marchand et Client	Le marchand reçoit la réponse de l'autorisation et complète la commande si le paiement est accepté, sinon il la refuse.
7	Émetteur et Client	L'émetteur de la carte envoie le relevé de carte de crédit au client pour régler ses paiements si la transaction est acceptée.

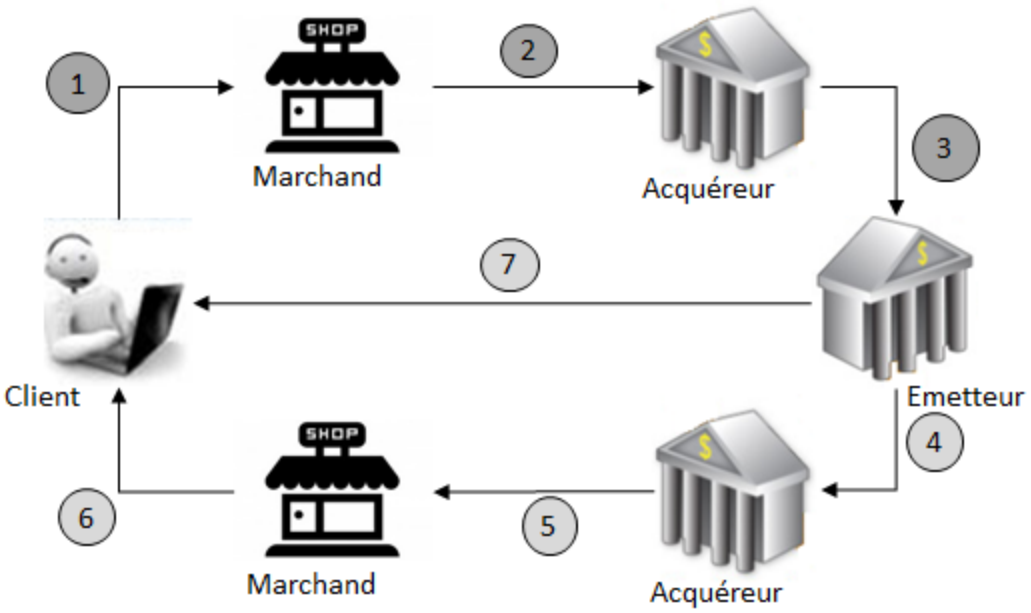

Figure 2 - Architecture simplifiée du paiement en ligne

Tout en considérant le déroulement de la transaction de paiement en ligne et les différentes entités qui y participent, il est important de mentionner que les technologies de paiement et les mécanismes mis en place doivent assurer la sécurité dans les échanges commerciaux afin de minimiser les risques. La sécurité dans les paiements en ligne fera l'objet de notre prochaine section.

2.4 Transaction électronique sécurisée

Les technologies des paiements en ligne permettent de mettre en place une interface qui facilite le transfert d'argent entre les marchands et les consommateurs (See-To & Ngai, 2018). De telles interfaces sont requises pour faciliter les transactions entre les consommateurs *(C2C),* les entreprises et les consommateurs *(B2C)* et les entreprises *(B2B)*, d'où leur nécessité pour notre quotidien d'assumer la sécurité dans de tels échanges commerciaux. Ces échanges sont basés sur des transactions électroniques sécurisées pour assurer à l'utilisateur la protection de ses états financiers d'une part et la protection de sa vie privée d'autre part. En d'autres termes, la transaction doit être sécurisée pour éviter toute perte ou fraude et, en même temps, protéger les données personnelles et financières de toutes attaques ou intrusions malveillantes (Antoniou & Batten, 2011). Des approches

qui combinent ces deux défis pourraient s'avérer intéressantes pour les utilisateurs durant la transaction électronique effectuée.

Dans les prochaines sections, nous abordons la notion de transaction électronique sécurisée tout d'abord par quelques détails sur les exigences de sécurité et de protection de vie privée et ensuite par une description de quelques protocoles spécifiques de signatures, comme la signature aveugle et la signature de groupe. Nous finissons par une vue générale des infrastructures à clé publique et la notion de certificat numérique.

2.4.1 Exigences de sécurité et de protection

Comme nous l'avons décrit, le paiement en ligne est basé sur des transactions électroniques qui échangent des données entre différentes entités. Les protections mises en exergue sont : la protection des données personnelles, souvent confidentielles, ainsi que les données financières. Les marchands ont recours à des solutions techniques impliquant d'utiliser des éléments sécurisés afin de stocker des informations de manière sûre. D'autres technologies avancées, notamment cryptographiques, sont mises en place pour réduire le risque de violation de la confidentialité des données et pour se prémunir contre le phénomène du « hacking ». Plus clairement, le chiffrement a pour fonction première de rendre non intelligibles les données au cours de leur transmission sur Internet. Seul le destinataire du message sera en mesure de les déchiffrer.

Sur Internet, toute information échangée peut être interceptée par des tiers non autorisés. Ces échanges de transactions requièrent aussi des protocoles particuliers basés sur les propriétés usuelles de sécurité : ***authentification, confidentialité, intégrité et non-répudiation.*** Afin d'assurer les principes de protection et la sécurité des données lors de telles transactions, une liste d'exigences a été établie. Ces exigences doivent être prises en compte lors des différentes étapes du processus.

- ***L'authentification des entités*** : il s'agit d'assurer l'identité et la validité des entités qui communiquent telles que le client et le marchand. Ainsi, cette propriété permet de vérifier qu'une entité est bien celle qu'elle prétend être.
- ***La confidentialité des transactions*** : C'est la protection des données contre la divulgation non autorisée. C'est ce qui fait que chaque donnée échangée doit être

chiffrée, et protégée, car une entité extérieure ou étrangère ne doit pas être capable de déchiffrer les informations.

- ***L'intégrité des données*** : C'est une propriété qui traite de la manipulation non autorisée des données par des tiers non autorisés, et ce, dans le but d'assurer l'exactitude des données transmises et leur non-altération lors de leur transmission ou leur stockage.
- ***La non-répudiation*** : C'est une propriété qui empêche une entité de nier ses engagements ou actions antérieures.

2.4.2 Signature aveugle

La signature aveugle est une forme de signature numérique dont le contenu est caché avant d'être signé. C'est un des protocoles spécifiques de signatures ayant été présentés par David Chaum en 1983 dans le cadre des systèmes de paiement (Chaum, 1983).

Ce type de schéma permet de garantir l'anonymat et est utile dans le cas où le signataire et l'auteur du message sont dissociés. En effet, ce procédé permet de signer un document ou un message, préalablement masqué par l'auteur et dont le signataire n'a pas connaissance de son contenu. Cette propriété doit être conservée après la divulgation du message signé, le signataire ne doit pas pouvoir retracer le message après l'avoir signé. Le signataire est souvent une autorité de confiance différente des auteurs du message.

Beaucoup de travaux ont cité des protocoles de paiement basés sur cette théorie permettant d'effectuer un paiement électronique sans dévoiler l'identité, notamment les applications de la monnaie électronique (*E-cash*). Ces schémas sont basés sur le transfert d'argent électronique ou de jetons entre le client et le marchand. Ceci se déroule en présence d'une entité tierce (généralement, une banque) qui garantit l'authenticité du jeton utilisé dans une transaction. La vérification des partenaires est effectuée par leur institution financière respective. Les informations des jetons échangés et les détails de la transaction sont gardés confidentiels (Mazumdar & Giri, 2012).

2.4.3 Déchiffrement aveugle

Un concept similaire à la signature aveugle appelée décodage aveugle a été proposé originalement par (Sakurai & Yamane, 1996) pour la protection de la vie privée des clients

lors de leurs achats en ligne, de telle manière que le propriétaire des documents n'a aucun moyen de savoir quels sont les produits que les clients ont achetés (Y.-C. Chen*, et al.*, 2009).

Dans une étude récente, un schéma de décodage aveugle est proposé avec l'algorithme RSA (Y.-C. Chen*, et al.*, 2014) qui consiste à chiffrer le document en se basant sur des clés dérivées de son résumé.

Le chiffrement RSA est un algorithme de cryptographie conçu en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman. Il est fréquemment utilisé dans le commerce électronique, et plus généralement dans l'échange de données confidentielles. En ce qui concerne son algorithme, il comprend les étapes suivantes (J.-h. Wang*, et al.*, 2009):

1. Alice choisit p et q deux grands nombres premiers et calcule $N = p \times q$.
2. Alice choisit e aléatoirement sans diviseur commun avec $(p - 1)$ ou $(q - 1)$:

$$gcd\,(e, (p - 1)\,(q - 1)) = 1$$

3. Alice publie la paire (N, e) qui constitue la clé publique.
4. La paire (p, q) sert à calculer l'unique d qui constitue la clé privée d'Alice avec :

$$e \times d = 1 \bmod (p - 1)\,(q - 1)$$

5. Bob chiffre son message M et envoie à Alice le message chiffré C :

$$C \equiv M^e \bmod N$$

6. Alice déchiffre le message avec sa clé privée :

$$M \equiv C^d \bmod N.$$

2.4.4 Signature de groupe

Un autre travail est présenté par (Chaum & Van Heyst, 1991) au sujet des signatures. Ces derniers présentent quatre schémas cryptographiques qui varient en fonction du type de signature, du type de groupe (fixe ou non) et du nombre de calculs et/ou bits transmis. Certains se basent sur le problème du *logarithme discret*, d'autres sur *l'algorithme RSA* (Rivest*, et al.*, 1978) décrit dans la section (2.4.3).

Cependant, ces schémas ont une longueur de clé proportionnelle au nombre d'individus dans le groupe. Ainsi, en 1997, Camenisch et Stadler présentent le premier protocole de signature de groupe dont les signatures et la clé publique ne dépendent pas du

nombre de membres du groupe (Camenisch & Stadler, 1997). Ce schéma de cryptographie permet au gestionnaire du groupe d'ajouter de nouveaux membres sans changer la clé publique. La seule personne pouvant ensuite déterminer le signataire est le responsable du groupe.

2.4.5 Infrastructure à clé publique

L'infrastructure complète pour fournir des services de signature numérique et de chiffrement par clé publique est appelée une infrastructure à clé publique (***PKI pour Public Key Infrastructure).*** Le déroulement d'un message chiffré/déchiffré entre deux parties (Bob et Alice) est illustré dans la Figure 3 en utilisant le principe de base de chiffrement à clé publique et privée. Une infrastructure à clé publique (***PKI)*** est composée de trois entités distinctes :

- L'autorité d'enregistrement qui gère les certificats et contrôle l'identité de l'utilisateur final.
- L'autorité de validation qui vérifie les informations des certificats.
- Le répertoire qui stocke les certificats numériques et les listes de révocation.

Le principe de l'autorité de certification a été introduit par (Kohnfelder, 1978). Il est utilisé pour attester la liaison entre la clé publique et un identifiant. Par conséquent, une signature numérique de l'autorité de certification est utilisée pour relier une clé publique au titulaire de cette clé. Ainsi, en prenant la clé publique de l'autorité de certification, tout acteur de la structure de PKI peut vérifier le lien entre une identité et une clé de n'importe quel certificat. Le certificat d'authentification utilise la technique du chiffrement à clé publique (*asymétrique*), soutenu par une infrastructure à clé publique (PKI) pour la gestion des clés et des certificats. Les certificats numériques sont émis par une *Autorité de Certification* (CA). Ils lient l'identité de l'utilisateur à sa clé publique (voir Figure 4).

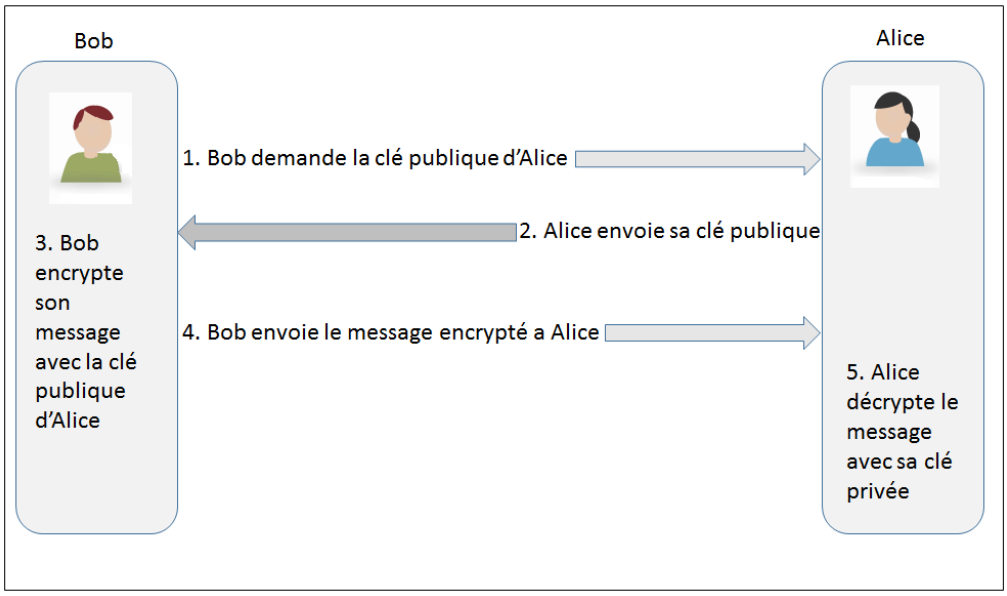

Figure 3 - La paire des clés publique et privée

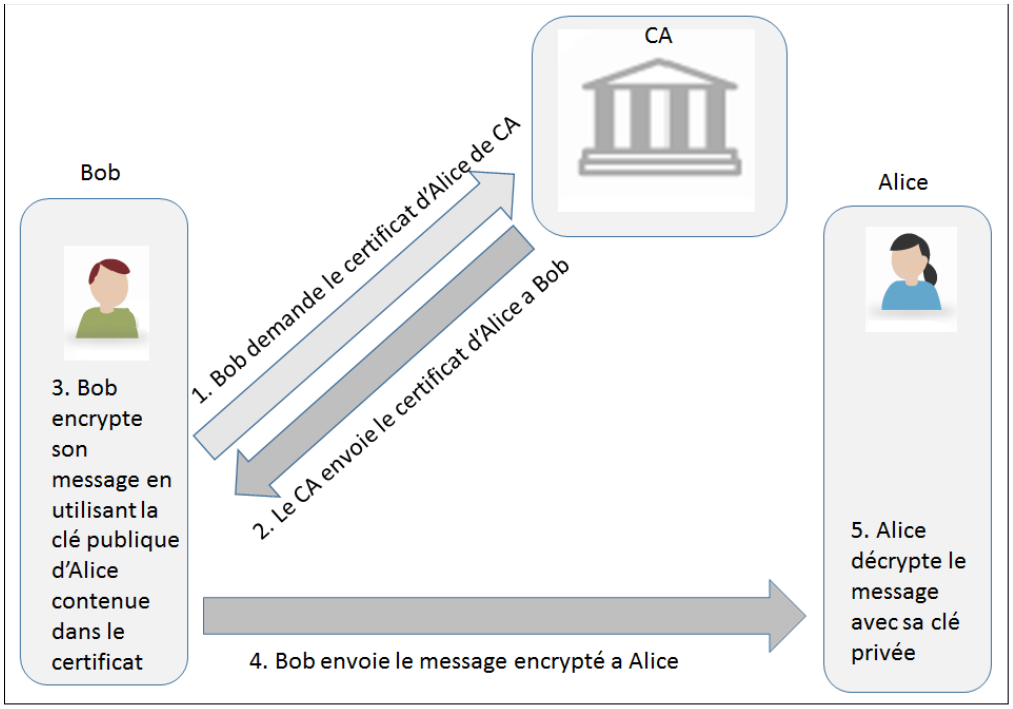

Figure 4 - Schéma d'Infrastructure à clé publique (PKI)

2.4.6 Certificat numérique

Le certificat numérique est un objet numérique permettant d'associer à une entité (client ou serveur) sa clé publique. Il s'agit d'un document électronique signé qui permet de

prouver l'identité de l'entité auprès de l'Autorité de Certification. Pendant son cycle de vie, un certificat est géré par la structure de PKI (2.4.5).

Cette infrastructure se sert de mécanismes de signature afin de certifier des clés publiques qui permettent de chiffrer et de signer des messages ou des flux de données. En matière de normes, les certificats doivent respecter de manière rigoureuse certains standards. La principale norme de définition de ces certificats est la norme X.509.

Des protocoles sont développés par les organismes financiers afin de supporter les paiements en ligne. Dans la section suivante, nous allons introduire quelques protocoles de paiement discutés dans la littérature

2.5 Protocoles de paiement.

Un protocole dans les paiements électroniques se concentre sur l'authentification du client et l'enregistrement du client auprès du marchand. Notons en premier lieu les paiements avec SSL (*Secure Sockets Layer*) et SET (*Secure Electronic Transaction*) et ensuite les protocoles basés sur la monnaie électronique (*E-cash*). Nous terminons par une description du paiement conditionnel, des « *Bitcoin »* et *« block chain »*.

2.5.1 Protocole SSL

Avec SSL, les informations concernant la carte de crédit sont transmises au commerçant pour accomplir le paiement en ligne. Citons le numéro, la date d'expiration et autres informations. SSL a deux caractéristiques principales. La première est l'utilisation d'un mécanisme à base de clé publique et clé privée pour relier les deux côtés d'une connexion réseau. Avec ce mécanisme, ils peuvent échanger entre eux en toute sécurité les messages chiffrés. Le second fait usage de la certification tierce entité pour permettre aux deux côtés de la connexion de confirmer les informations des uns et des autres. La Figure 5 présente les étapes consécutives et interactives du paiement sécurisé par SSL tirées du schéma de base (Khosrow-Pour, 2008).

Notons également que SSL peut assurer la sécurité de la livraison de pair-à-pair, mais ne peut pas confirmer les identités des utilisateurs (Das & Samdaria, 2014; Oppliger*, et al.*, 2008). Pour résoudre ce problème, les entreprises de cartes Visa et MasterCard et autres

compagnies s'adonnent à des efforts pour mettre en place un protocole plus avancé pour le système de paiement électronique qui est le SET (*Secure Electronic Transaction*) (S. Lu & Smolka, 1999) qui sera discuté dans la section suivante.

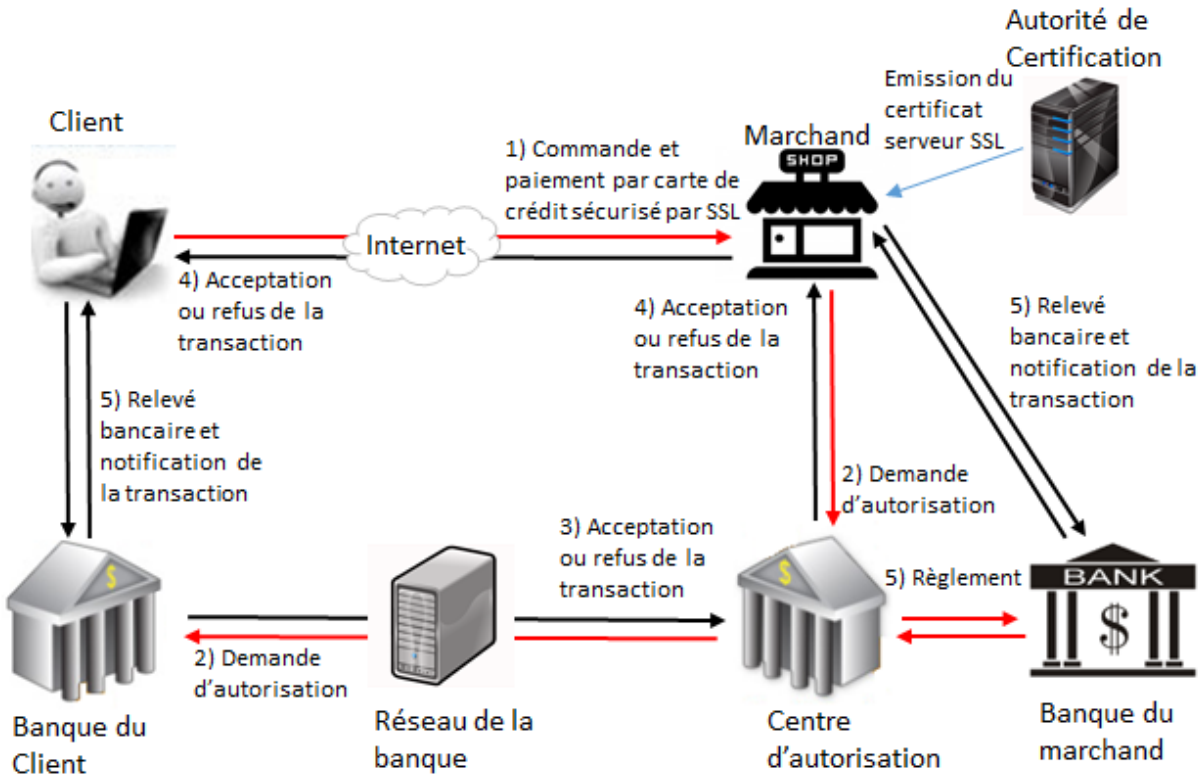

Figure 5 - Le flux d'information avec SSL

2.5.2 Protocole SET

Le protocole SET est développé par les deux plus grandes compagnies de carte de crédit (Visa et MasterCard) dans le but de sécuriser les transactions électroniques de paiement par carte de crédit (LLC, 2002). Celui-ci est partiellement décrit dans la Figure 6 extraite de (Khosrow-Pour, 2008). Dans le cadre de ce protocole, un certificat est installé sur l'ordinateur du client, contrôlé par la banque du marchand et donne une authentification de l'utilisateur. Le protocole peut être décrit comme quatre échanges principaux, tous transmis en SSL.

SET fait intervenir de nouveaux acteurs : *une passerelle de paiement*, jouant le rôle d'intermédiaire entre Internet et *le réseau de cartes de paiement*, ainsi qu'une autorité de

certification maîtresse, qui a pour fonction d'assurer l'authentification de tous les intervenants (Bella, *et al.*, 2001).

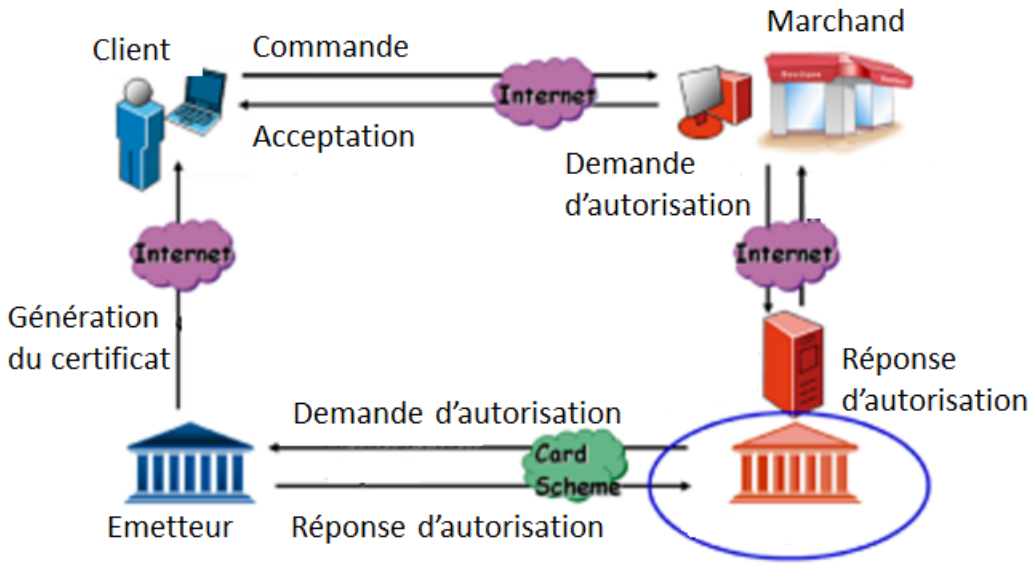

Figure 6 - Le flux d'information dans le protocole SET

Vu la complexité de la gestion de certificat, les organismes financiers ont développé d'autres protocoles tels que le protocole 3D-Secure. Celui-ci a été lancé par Visa en 2001, connu sous le nom de (*Verified by Visa*), mais a également été utilisé par MasterCard. Dans la section suivante, nous prendrons le protocole 3D-Secure pour l'expliquer plus en détail.

2.5.3 Protocole 3D-Secure

Le terme 3D du protocole provient de sa structure qui comprend trois domaines (Carbonell, *et al.*, 2009) tels qu'illustrés dans la Figure 7. Le premier domaine est le Domaine Acquéreur représenté par le marchand et sa banque qui s'occupent du transfert de fonds. Le domaine Émetteur est le client et sa banque, qui ont délivré la carte de paiement. Le troisième domaine est le système de carte bancaire.

Le 3D-Secure effectue les authentifications et réalise les fonctions suivantes :

- Un service d'annuaire, pour déterminer la banque d'un client et son numéro de compte à partir de sa carte.

- Une autorité de certification, qui génère les différents certificats.
- Un historique de toutes les tentatives d'authentifications réalisées au cours de transactions passées.

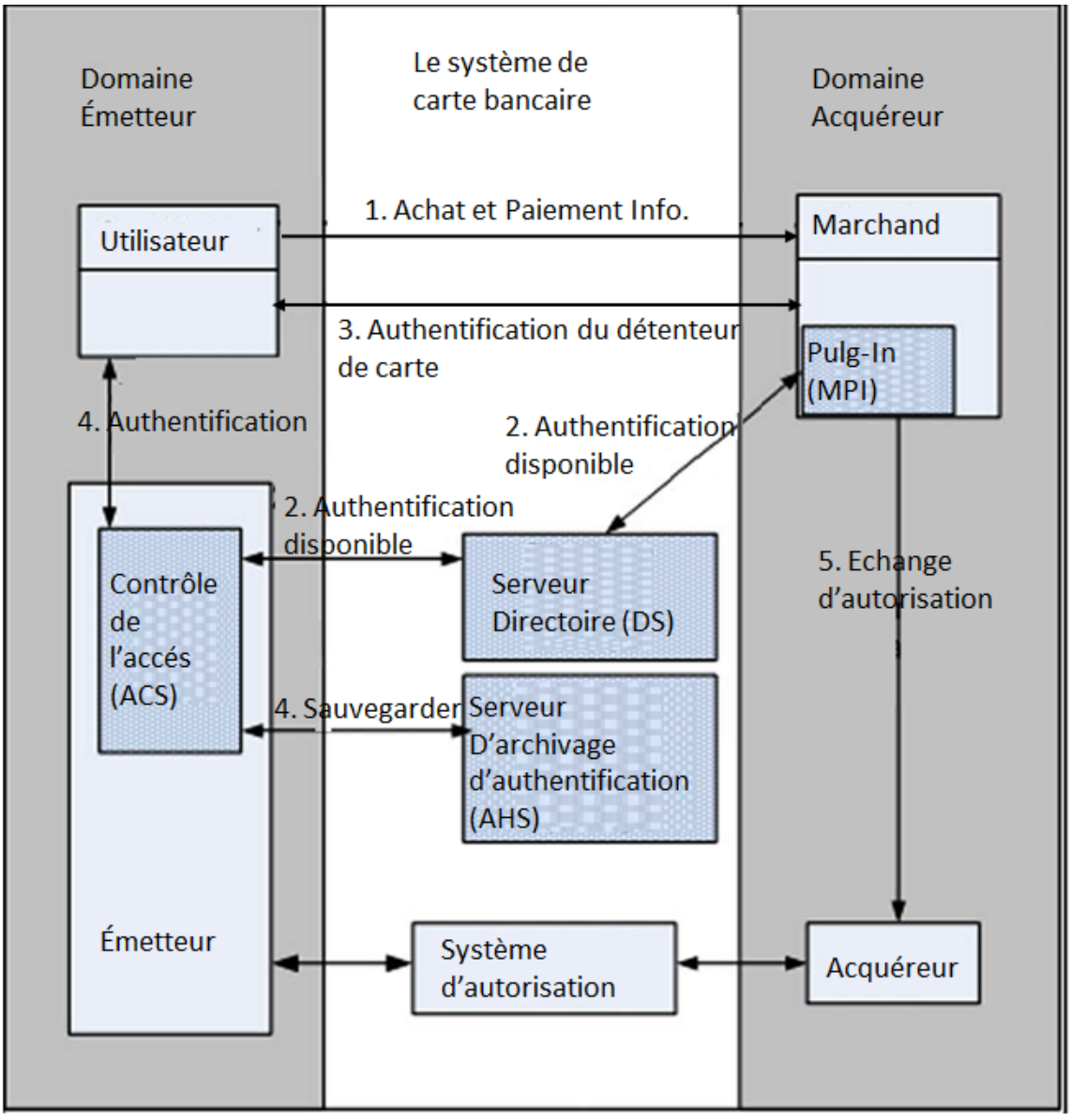

Figure 7 - Schéma de 3D-Secure

Dans 3D-Secure, l'échange est constitué de messages XML acheminés en SSL ainsi que de l'autorisation de paiement qui est effectuée séparément après l'authentification du détenteur de la carte de crédit. En effet, le commerçant déclenche l'authentification du détenteur de la carte, ce qui fait que ce dernier s'authentifie à chaque fois qu'il effectue un

achat. Ceci résulte en une augmentation non seulement du nombre de messages dans le protocole, mais aussi des effets liés aux problèmes de connexion réseau, étant donné que chaque message exige qu'une nouvelle session soit établie.

2.5.4 Paiement conditionnel

Le paiement électronique conditionnel est introduit par Shi et al (L. Shi*, et al.*, 2007). Il permet à l'utilisateur d'encaisser d'une façon anonyme des monnaies électroniques encaissées par la banque à une date ultérieure si et seulement si une certaine condition publique prédéfinie est satisfaite.

Comparée au paiement électronique traditionnel, l'identité des bénéficiaires reste anonyme tout au long du transfert (X. Chen*, et al.*, 2014). Ce type de paiements électroniques est utilisé dans le domaine des applications de prédictions, les systèmes de pari en ligne, ainsi que les applications financières de placements et d'investissements. Chen et al (X. Chen*, et al.*, 2014) ont proposé un nouveau paiement électronique conditionnel assez efficace, qui est basé sur le schéma de signature en aveugle partiellement restrictive décrit par (X. Chen*, et al.*, 2007). Notons que la signature en aveugle consiste à faire signer un document à une autorité, sans que l'usager qui obtient cette signature puisse être tracé. Ils ont ajouté la transférabilité qui permet à la monnaie électronique d'être transférée encore une fois de façon anonyme par une chaîne de bénéficiaires.

2.5.5 Bitcoin

Le Bitcoin a été originalement introduit par (Barber*, et al.*, 2012; Nakamoto, 2008). C'est un type de monnaie électronique qui a émergé rapidement et est devenu système de paiement numérique populaire. Il s'agit d'une devise monétaire ayant une valeur déterminée selon son usage économique et selon le marché des changes (Meiklejohn*, et al.*, 2013). Le système de paiement en Bitcoin circule dans cette devise, et offre un potentiel important aux interactions financières, mais diffère des systèmes bancaires internationaux classiques.

Bien qu'un tel système permette l'anonymat durant la transaction de paiement, il ne s'agit pas d'une infrastructure centralisée. Le Bitcoin a des limites en ce qui concerne la vie privée. La vie privée des utilisateurs est protégée uniquement par l'utilisation de pseudonymes. Toutefois, en dépit de sa dépendance aux pseudonymes, Bitcoin soulève un certain nombre de renseignements personnels à considérer étant donné que toutes les transactions qui ont lieu sont publiquement annoncées dans le système (Androulaki*, et al.*, 2013).

Un protocole Zerocoin est proposé par (Miers*, et al.*, 2013) comme une extension cryptographique de Bitcoin, basée sur le système monétique (*E-cash*) distribué, afin d'augmenter l'anonymat dans les opérations sans la présence des entités de confiance.

De nouvelles technologies sont apparues, dont principalement la technologie des chaînes de blocs (également connue sous le nom *Blockchain*), et ont conduit à une évolution dans la centralisation des protocoles des paiements (Morse, 2018). La notion de Blockchain sera élaborée dans la section suivante avec plus de détails.

2.5.6 Blockchain

Le bitcoin que nous venons de décrire dans le paragraphe précédent se base sur l'application monétaire des Blockchains. Récemment, la technologie des Blockchains a gagné une popularité importante surtout en raison de sa nature distribuée et de l'absence d'une autorité centrale (Y. Zhang*, et al.*, 2018). Cette technologie consiste en un registre décentralisé, infalsifiable grâce au protocole cryptographique, basée sur un algorithme qui établit la confiance entre deux entités inconnues sans la nécessité d'avoir un intermédiaire de confiance. L'indépendance envers la centralisation est le principal avantage des solutions axées sur les Blockchains par rapport aux technologies de paiement traditionnelles. Ceci entraîne des opportunités de pouvoir modifier les pratiques centralisées et intermédiaires utilisées dans le domaine des paiements (Morse, 2018).

Tout en établissant une interface qui facilite le transfert d'argent entre les détaillants et les consommateurs, le processus du paiement en ligne représente aussi une connexion technique qui interagit avec l'usager en ligne, influe de façon assez considérable sur son comportement de consommation (R. R. Burke, 2002; Ho*, et al.*, 2013) et affecte sa prise

de décision (See-To & Ngai, 2018). Dans ce qui suit, nous abordons les influences du processus de paiement en ligne sur le comportement des clients et les diverses conséquences qui en résultent.

2.6 Comportement en ligne

La littérature a élaboré largement le comportement de l'utilisateur en ligne dans les réseaux sociaux, achats en ligne, apprentissage ou toute autre interaction homme-machine. Nous nous intéressons dans cette section au comportement des consommateurs du point de vue des paiements en ligne. Ce processus tient compte non seulement de la sécurité des transactions, mais possède aussi une influence sur les attitudes des consommateurs envers les achats en ligne (Z. Liao & Cheung, 2001).

Des recherches se sont intéressées au sujet du comportement du consommateur en ligne afin de fournir une explication dû à sa résistance à faire des achats en ligne (Mothersbaugh*, et al.*, 2011; Taylor*, et al.*, 2009) et à sa prise de décision. Des études s'efforcent de comprendre comment le contexte du paiement affecte le comportement du consommateur (Gneezy*, et al.*, 2010; Jung*, et al.*, 2014). D'autres études ont mis l'accent sur l'influence des différentes méthodes de paiements sur le comportement du point de vue des dépenses (Chatterjee & Rose, 2012; Runnemark*, et al.*, 2015; M. Thomas*, et al.*, 2011). Le processus de paiement en ligne a également un impact sur la consommation, ce qui a suscité l'intérêt des chercheurs et les ont incités à considérer des réactions affectives dans leurs travaux pour mieux comprendre les attitudes et le comportement dans ce domaine. Dans ce contexte, l'adoption de la technologie est un des facteurs à étudier pour déterminer la facilité d'utilisation et la bienveillance envers une méthode de paiement (See-To & Ngai, 2018).

Toujours dans le cadre du comportement, nous abordons dans ce qui suit :

- Les attitudes en ligne (Nadeem*, et al.*, 2015)
- La confiance en ligne
- La perception du risque
- La perception du concept de vie privée
- Les multi-craintes en ligne
- Les vols d'identités

2.6.1 Attitudes en ligne

Dans un processus d'achat en ligne, l'utilisateur s'adonne à des échanges variés avec le site Web. Il cherche les articles ou services, les évalue, les compare avec d'autres catégories du même site ou de différents sites, les choisit et décide de payer. Ces activités sont liées directement à son expérience en ligne comme étant un état psychologique qui se manifeste comme une réaction subjective au site du marchand (Rose*, et al.*, 2012).

Des études récentes ont souligné les aspects cognitifs et affectifs expérientiels dans le processus d'achat et leurs influences sur la satisfaction des consommateurs (Rose*, et al.*, 2012), sur la confiance et sur l'intention d'acheter à nouveau ou pas (Faqih, 2016; J. Martin*, et al.*, 2015; S. K. Roy*, et al.*, 2017; Stein & Ramaseshan, 2016). Notons que l'approche cognitive correspond aux valeurs liées aux attributs du produit et suppose que les individus se fixent des objectifs, qu'ils cherchent activement de l'information pour procéder à un choix sur la base de leur préférence, tandis que l'approche affective repose sur les sentiments, les émotions et les expériences vécues (Eagly & Chaiken, 1993; Netzer*, et al.*, 2018).

Par rapport à la totalité de l'expérience de l'achat en ligne, le consommateur subit une série d'attitudes variées selon ses besoins et la situation à laquelle il est confronté (C.-W. Liu*, et al.*, 2017; Mohseni*, et al.*, 2018). Une fois qu'il apprend qu'il pourrait subir des conséquences négatives en ligne, il essayera de les éviter et cessera de magasiner sur Internet (Chiu*, et al.*, 2014). Ces conséquences ont attiré l'attention des vendeurs qui essaient de trouver des solutions afin d'atteindre la satisfaction de l'utilisateur. Des efforts sont investis pour mesurer la prédisposition de l'utilisateur à ressentir des émotions négatives, surtout la peur qu'un attaquant malveillant utilise illicitement les informations qui l'identifient (Erkan & Evans, 2018; Hille*, et al.*, 2015; J. Thomas, 2018). D'autres solutions sont introduites pour l'aider à surmonter le plus vite possible toutes les expériences négatives antécédentes puisque la nature et l'ordre de ces expériences peuvent avoir un impact sur l'ensemble de sa satisfaction de leur service (Chase & Dasu, 2001; J. Cho*, et al.*, 2017), d'où l'apparition de solutions interactives qui s'appuient sur les interventions homme-machine en introduisant des agents intelligents qui agissent comme fournisseurs d'information en ligne (Parvinen*, et al.*, 2015; Sivaramakrishnan*, et al.*, 2007).

2.6.2 Confiance en ligne

Dans le contexte d'Internet, la confiance est cruciale. En effet, celle-ci joue un rôle pivot dans l'adoption du commerce électronique. La littérature de plus en plus abondante sur le sujet ne fait que confirmer ce constat. De même, la confiance en ligne constitue un enjeu majeur pour les e-commerçants souhaitant établir des relations à long terme avec les consommateurs (Ruiz-Mafe*, et al.*, 2014). Les recherches sur la confiance électronique ne cessent de proliférer (Casado-Aranda*, et al.*, 2018; J. V. Chen*, et al.*, 2016) et son influence s'avère positive en ce qui concerne les intentions comportementales de l'utilisateur afin d'effectuer la transaction (C. Liao*, et al.*, 2011). D'une part, la confiance du consommateur affecte positivement son attitude envers le site Web, ce qui, finalement, conduit à une visite répétitive de ce même site (Limbu*, et al.*, 2012). D'autre part, la confiance réduit l'incertitude, fournissant ainsi à l'utilisateur des attentes pour une transaction satisfaisante (Limbu*, et al.*, 2012; Williams, 2018).

D'autres études ont discuté des divers facteurs qui favorisent la confiance en ligne. Notons en premier lieu que la qualité de service fournie par le vendeur en ligne est un moyen pour assurer la satisfaction des consommateurs, pour développer leur confiance et enfin pour les mener à un achat répété (J. Martin*, et al.*, 2015; Shin*, et al.*, 2013). Un autre facteur est lié aux messages de confiance propagés par les fournisseurs en ligne dès que le consommateur fournit son numéro de carte de crédit. En effet, les messages de sécurité qui se produisent vers la fin du processus d'achat ont un impact plus important que les messages qui apparaissent au début du processus d'achat. En conséquence, ces messages aident les consommateurs à compléter le processus d'achat, surtout s'ils ont une attitude négative à l'égard de l'utilisation des cartes de crédit (Shu & Cheng, 2012). D'autres facteurs s'occupent des marques de confiance qui figurent parfois clairement sur le site et renforcent la confiance en ligne. En revanche, les consommateurs considèrent en général que les « *trustmarks* » telles que *TRUSTe , VeriSign, et McAfee Secure* (Thompson*, et al.*, 2019) sont juste des symboles/logos et qu'il est important d'ajouter d'autres types de messages aux consommateurs durant les achats en ligne afin d'aboutir à une amélioration dans leurs attitudes (Shu & Cheng, 2012).

Dans le contexte du paiement en ligne, la confiance est largement reconnue comme un facteur clé dans les achats en ligne à la suite de l'intervention des *entités tierces* de

paiement entre le client et le site marchand (K. Kim & Kim, 2011; Ponnapureddy*, et al.*, 2017; Ponte*, et al.*, 2015). Ce genre de compagnie est apparu comme jouant le rôle de tiers pour aider à stimuler la confiance des consommateurs, même si le site Web est inconnu. Dans un environnement en ligne, la présence d'un tiers de confiance externe et certifié est susceptible d'avoir un effet positif sur la perception de la vie privée et la sécurité des consommateurs envers le vendeur en ligne (F. Cui*, et al.*, 2018; Ponte*, et al.*, 2015).

À l'instar de la confiance, le risque constitue également un composant assez important dans le déroulement de la transaction (S. Kim & Park, 2013). La relation confiance-risque vient du fait que les consommateurs évaluent leur confiance à un site Web par rapport au risque perçu. Dans la section suivante, la perception du risque dans le processus de paiement en ligne est abordée.

2.6.3 Perception du risque

La perception du risque est un des sujets assez importants dans le paiement en ligne (J. B. Kim, 2012; Yuan Li, 2014). Les risques proviennent, en premier lieu, du manque de confiance des consommateurs envers les vendeurs en ligne (Nepomuceno*, et al.*, 2014; Ponte*, et al.*, 2015; Vos*, et al.*, 2014). En outre, la perception du risque en ligne est considérablement élevée pour le client, en raison de la distance physique entre lui et le vendeur en ligne, ainsi qu'en raison de la différence temporelle entre le paiement et la livraison du produit (Xiao & Benbasat, 2011; N. Xu*, et al.*, 2017). Cependant, ces perceptions du risque occasionnent une réduction et parfois un abandon des activités en ligne même si elles sont considérées comme sécuritaires (Dunn, 2004).

Pour lutter contre leurs perceptions de risques, les consommateurs sont incités à adopter des techniques dans les achats en ligne afin de réduire au minimum les pertes et les effets négatifs (C.-W. Liu*, et al.*, 2017). De même, dans la présence des normes procédurales liées à la prestation des services, les consommateurs changent leur perception de risque si celui-ci est associé à des valeurs ou informations échangées (Gao*, et al.*, 2015; Morosan, 2014). Cependant, une autre perception entre en vigueur. C'est l'aspect du profit perçu qui pousse en revanche les clients à maximiser leurs aspects positifs (Y. Lu*, et al.*, 2011). En d'autres termes, les consommateurs ont tendance à faire confiance aux certifications offertes par le site, telles que la sécurité et les garanties de protection qui

affectent, en plus de leur perception de risque, quant à la protection de la vie privée que nous précisons dans la section suivante.

2.6.4 Perception du concept de vie privée

Au fil des années, l'expansion du commerce électronique a inspiré des travaux de recherche en vie privée et incité à la protection des données personnelles et confidentielles de l'utilisateur en ligne (Acquisti*, et al.*, 2015, 2018; Acquisti*, et al.*, 2013; Acquisti*, et al.*, 2016; Aïmeur, 2014; Bella*, et al.*, 2011; Yuan Li, 2014). De même, des études dans la littérature ont mis l'accent sur la confidentialité comme étant une préoccupation majeure (Bella*, et al.*, 2011; Morosan & DeFranco, 2015; Sicari*, et al.*, 2015). Les utilisateurs en ligne sont confrontés à un risque de perte de leur confidentialité, étant donné que diverses données personnelles et bancaires sont présentes sur les sites des vendeurs.

En revanche, les internautes sont prêts à céder leurs informations privées en échange de services personnalisés et d'offres adaptées à leurs besoins et selon leurs envies. En d'autres termes, rien n'empêche qu'ils optent pour divulguer des informations personnelles dans un but de personnalisation (Morosan & DeFranco, 2015; T. Wang*, et al.*, 2016). En effet, les recherches sur la vie privée explorent souvent les conditions et situations où les consommateurs sont prêts (avec volonté) à divulguer leurs informations (K. Martin, 2018; K. D. Martin*, et al.*, 2017; K. D. Martin & Murphy, 2017). Ces études ont mis en relief la relation positive entre la perception de la valeur de l'information divulguée et le risque de l'invasion de la vie privée (K. D. Martin & Murphy, 2017). Ce qui signifie qu'une haute anticipation du profit apportée par la personnalisation du service voulu peut aboutir à une haute perception de l'importance de la divulgation de l'information (Kokolakis, 2017; Pappas*, et al.*, 2017; H. Xu*, et al.*, 2011).

Hormis la confiance dans l'application, la valeur totale de l'information divulguée a aussi un impact assez significatif sur la divulgation des informations. Dans ce contexte, des études ont prouvé que les évaluations de la confidentialité ne sont pas normalement ou uniformément distribuées (Acquisti*, et al.*, 2015; Acquisti*, et al.*, 2013; Acquisti*, et al.*, 2016). En effet, ils assignent des valeurs sensiblement différentes à la confidentialité de

leurs données, selon l'ordre dans lequel ils classent les différentes offres pour ces données, ou le montant d'argent qu'ils estiment pour accepter de divulguer les informations privées.

Outre leurs perceptions du risque, les internautes sont exposés à un risque lié directement à Internet : le risque environnemental. Il s'agit d'un risque inhérent à la technologie utilisée et qui échappe au contrôle des deux entités de l'échange. En effet, malgré les efforts de sécurisation, toute information échangée sur Internet ne peut être totalement à l'abri de l'intrusion maligne des « hackers », ce qui amène le sujet des multi-craintes de l'utilisateur en ligne qui sera abordé dans la section suivante.

2.6.5 Multi-craintes en ligne

De nos jours, les attaques malintentionnées en ligne ne forment plus une exception (Arora, *et al.*, 2006). Dans les transactions en ligne, la vulnérabilité renvoie à la possibilité qu'une des entités de l'échange se trouve lésée. Au cours de la dernière décennie, les attaques de sécurité sur les informations sont devenues de plus en plus motivées par des motifs frauduleux et criminels et ont produit une menace pour l'univers d'Internet en le rendant effrayant et encombré de dommages inévitables (Zittrain, 2008).

Étant donné que le nombre de tels incidents augmente de façon exponentielle (McCormac, *et al.*, 2017; Pee, *et al.*, 2008; Weatherbee, 2010), beaucoup d'entreprises subissent de graves menaces (Manworren, *et al.*, 2016) et doivent composer avec des conséquences négatives liées à la confidentialité de leurs clients et leurs profits sur le plan économique (Hiller & Russell, 2013). Nous citons comme exemples le déni des services distribués (*DDoS*), le vol et manipulation des données, l'usurpation d'identité ou même la prise de contrôle sur les systèmes. Ces types d'attaques sur la cybersécurité nuisent aux entreprises comme aux utilisateurs en impliquant généralement des pertes sur le plan financier et de la réputation (Cerdeiro, 2017). Prenons l'exemple du vol des données personnelles de 2,9 millions de membres du Mouvement Desjardins. Des informations sensibles figurent parmi les informations dérobées. Et celles-ci pourraient potentiellement se trouver entre les mains de personnes mal intentionnées[1].

[1] https://ici.radio-canada.ca/nouvelle/1195357/securite-donnees-caisse-desjardins-vol-employe consulté le 25/Oct./2019

Les menaces de cybersécurité ne sont pas sur le point de disparaître (Manworren*, et al.*, 2016). Afin de lutter contre ces violations, de nombreux milieux de travail visent à empêcher les violations potentielles. Pour ce faire, ils utilisent des infrastructures de technologie de l'information qui sont protégées par des contre-mesures techniques (Hadlington, 2017). Ils investissent des efforts considérables afin d'éduquer leurs employés à propos de cybersécurité et les incitent à être plus engagés dans des pratiques de sensibilisation (Hadlington, 2017). Ces craintes auxquelles l'utilisateur est confronté en ligne, surtout en lien avec une expérience qu'il a personnellement vécue, ou dont il a entendu parler.

En dépit de tous les efforts de sécurisation, il n'est guère possible de se prémunir de façon sûre contre toute tentative de fraude. Dans la section suivante, le vol d'identité est abordé.

2.6.6 Vols d'identité

Les vols d'identité constituent une grave menace à la vie privée ainsi qu'à la sécurité financière des utilisateurs en ligne. Ce type de menace implique la crainte de se faire voler intentionnellement des informations personnelles ou financières et la crainte que ces dernières soient stockées pour une utilisation frauduleuse ou malveillante. Devant ce cas, les consommateurs sont envahis par le sentiment de vulnérabilité et altèrent leurs comportements en ligne (Milne*, et al.*, 2009).

Prenons l'exemple de Bob qui reçoit une alerte sur son téléphone. Une transaction de 1300 $ vient d'être effectuée avec son compte PayPal pour un achat fait au magasin IKEA de Montréal. Bob est à Québec, chez son ami. Bob réalise qu'il est victime d'un vol d'identité. Se remettre d'un vol d'identité peut prendre des années. Il faut affronter une panoplie d'embûches, encaisser de durs coups et faire face à de mauvaises surprises. Ce qui fait que Bob va confronter les conséquences : ses informations peuvent être utilisées frauduleusement pour faire des achats en ligne, des demandes de passeport, des retraits bancaires, des demandes de prêt ou toute autre utilisation illégale (Hille*, et al.*, 2015).

Ceci dit, les vols d'identité se situent en tête des craintes en ligne et sont perpétrés grâce aux techniques d'attaques existantes. On cite l'hameçonnage (*phishing*) (Chou*, et al.*, 2004; Gupta*, et al.*, 2017), qui est une forme d'attaque informatique dans laquelle

l'attaquant exploite des techniques d'ingénierie sociale pour effectuer le vol d'identité (Aleroud & Zhou, 2017). Cette technique peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques (Shaji, 2014). Ce genre d'attaque cible des victimes en ligne et consiste à leur faire croire qu'elles s'adressent à des tiers de confiance ou des entités légitimes afin de leur soutirer des renseignements personnels : nom, prénom, mot de passe, numéro de carte de crédit, date de naissance, etc. Ce type de vol de données personnelles et financières peut avoir de graves et de sérieuses conséquences financières à longue durée pour la victime (Eisenstein, 2008; Hille*, et al.*, 2015; Mitchison*, et al.*, 2004) comme encourir une obligation financière ou affecter son dossier de crédit.

2.7. Systèmes de recommandation

À l'ère de l'explosion de l'information, les systèmes de recommandation ont été largement adoptés par de nombreux services en ligne, y compris le commerce électronique, les nouvelles en ligne et les sites de médias sociaux. Les systèmes de recommandation ont pour but de guider les utilisateurs d'une manière personnalisée vers les produits/articles/services intéressants parmi un large intervalle de choix possibles. Ils s'appuient sur différents types d'entrées dépendamment du site : des produits sur *Amazon*, des vidéos sur *YouTube* ou des chansons sur *Spotify*. Les données les plus adéquates sont les commentaires explicites et les notes des usagers.

En s'appuyant sur les systèmes de recommandation, les vendeurs en ligne scrutent l'historique des recherches et des achats de l'utilisateur pour identifier les produits qui pourraient l'intéresser (Hannak*, et al.*, 2014). Deux défis se présentent. Le premier est de réussir à fournir aux utilisateurs des informations assez efficaces et fiables pour les aider à choisir. Le deuxième défi a trait à leur confiance envers les vendeurs. En effet, les systèmes de recommandation peuvent briser la confiance que le vendeur en ligne mérite, et ce, quand des utilisateurs malveillants fournissent des notations qui ne représentent pas leurs véritables opinions (Ricci*, et al.*, 2015; Schafer*, et al.*, 2007).

Dans les systèmes de recommandation, l'information sémantique d'un article comprend ses attributs, les relations entre les articles eux-mêmes et la relation entre les méta-informations et les articles. Au cours des dix dernières années, des ontologies ont été

adoptées avec succès dans les systèmes de recommandation pour combler les lacunes de ces systèmes (López-Nores*, et al.*, 2010; Martín-Vicente*, et al.*, 2014).

Au regard des travaux menés sur les systèmes de recommandation, des solutions se présentent notamment pour améliorer la qualité ou la fiabilité des évaluations (G. Guo*, et al.*, 2014; X. Zhang*, et al.*, 2017) ainsi que pour fournir un moteur de recommandation personnalisé (Pereira*, et al.*, 2018). Les algorithmes de recommandations sont apparus aussi pour aborder des problèmes tels que le **démarrage à froid** (G. Guo*, et al.*, 2014; Scholz*, et al.*, 2017). Ceci se traduit par des situations dans lesquelles le système de recommandation est incapable d'accomplir des recommandations utiles en raison d'un manque initial de notations, collectées de façon explicite ou implicite (Elahi*, et al.*, 2016) ou dans le cas où un nouvel article n'a pas été encore évalué. Dans ce contexte, des travaux ont été proposés en se basant sur des méthodes telles que la théorie des valeurs d'attributs multiples *(MAVT)* traitant dans le même contexte ce problème dont l'idée principale est de prédire des décisions en se basant sur des valeurs de fonctions spécifiques au consommateur et des attributs de poids d'importance estimés au moment de l'achat. Le **changement de préférences** (Lops*, et al.*, 2011) est une autre complication dans les systèmes de recommandation qui réduit ainsi la précision des recommandations fournies aux consommateurs (Scholz*, et al.*, 2017). En outre, **le manque d'informations** suffisantes liées aux profils des utilisateurs conduit à des problèmes dans le système de recommandation (Núñez-Valdez*, et al.*, 2018) tel que **le problème de diversification** qui se manifeste quand il est difficile d'identifier les utilisateurs similaires en raison du manque d'informations (Papagelis*, et al.*, 2005). Habituellement, ce type de problème apparait lorsque le nombre d'évaluations nécessaires pour la prédiction d'un article est supérieur au nombre de notations obtenues par les utilisateurs envers ce même article (Moreno & Redondo, 2016).

Les systèmes de recommandation sont basés sur les systèmes de filtrage d'information et sur les décisions d'achat précédentes dans le but de prédire les décisions futures (Scholz*, et al.*, 2017). Actuellement, les deux approches de filtrage les plus communes dans les implémentations des systèmes de recommandation (Jafarkarimi*, et al.*, 2012; Y. Shi*, et al.*, 2014) sont : celle basée sur le *contenu* (Lops*, et al.*, 2011; Pazzani & Billsus, 2007) et celle *collaborative* (Huang*, et al.*, 2007; Martínez*, et al.*, 2017; Schafer*,*

et al., 2007). Une troisième approche est apparue (Adomavicius & Tuzhilin, 2005) : celle-ci combine les deux approches pour obtenir des systèmes de recommandation hybrides (R. Burke, 2002; Hagemann*, et al.*, 2018; Katarya & Verma, 2017; D. Kim*, et al.*, 2017). Le filtrage basé sur le contenu compare les objets/articles par rapport au profil de l'utilisateur, et recommande ceux qui sont les plus proches (D. Wang*, et al.*, 2018). Le filtrage collaboratif compare les utilisateurs entre eux sur la base de leurs notations et jugements antécédents, et chaque utilisateur reçoit les objets/articles jugés pertinents par ceux qui lui sont similaires (Ricci*, et al.*, 2015). Le filtrage hybride combine le filtrage basé sur le contenu et le filtrage collaboratif pour exploiter au mieux les avantages de chacun et surmonter leurs limitations (Katarya & Verma, 2017). Dans la suite de cette section, nous présentons plus en détail ces approches de filtrage.

2.7.1 Filtrage collaboratif

Le filtrage collaboratif (*Collaborative Filtering ou (CF)*) est la technologie de recommandation la plus largement appliquée dans les systèmes réels en ligne (Ładyżyński & Grzegorzewski, 2015; F. Zhang*, et al.*, 2017). C'est une des méthodes de filtrage, qui a pour principe d'exploiter les évaluations que les utilisateurs ont faites en ligne à l'égard de certains articles/services, afin de les recommander à d'autres utilisateurs ayant des profils ou des goûts similaires, et sans qu'il soit nécessaire d'analyser leurs contenus (Katarya & Verma, 2017). Afin d'établir des recommandations, ces systèmes font le lien entre deux entités différentes : les articles et les utilisateurs (Koren & Bell, 2015), et tiennent compte de la similarité de comportement (achats, clics, notes, visites) entre les utilisateurs (voir Figure 8).

La propriété de personnalisation dans ce type de système de recommandation est dans la modélisation des préférences des utilisateurs envers des articles en se basant sur leurs interactions antécédentes (par exemple, les cotations et les clics) (X. He*, et al.*, 2017). À ce sujet, la notion de communauté dans les méthodes de filtrage collaboratif s'impose comme étant un groupe d'utilisateurs qui partagent les mêmes intérêts ou tendances (R. He & McAuley, 2016). En conséquence, un des objectifs cruciaux des systèmes de filtrage collaboratif est d'exploiter de façon intelligente les communautés afin de produire de meilleures recommandations. Pour ce faire, la gestion des communautés joue un rôle très

important puisque, selon le principe de base du filtrage collaboratif, la qualité des recommandations envoyées aux utilisateurs dépend fondamentalement de la qualité des communautés formées par le système.

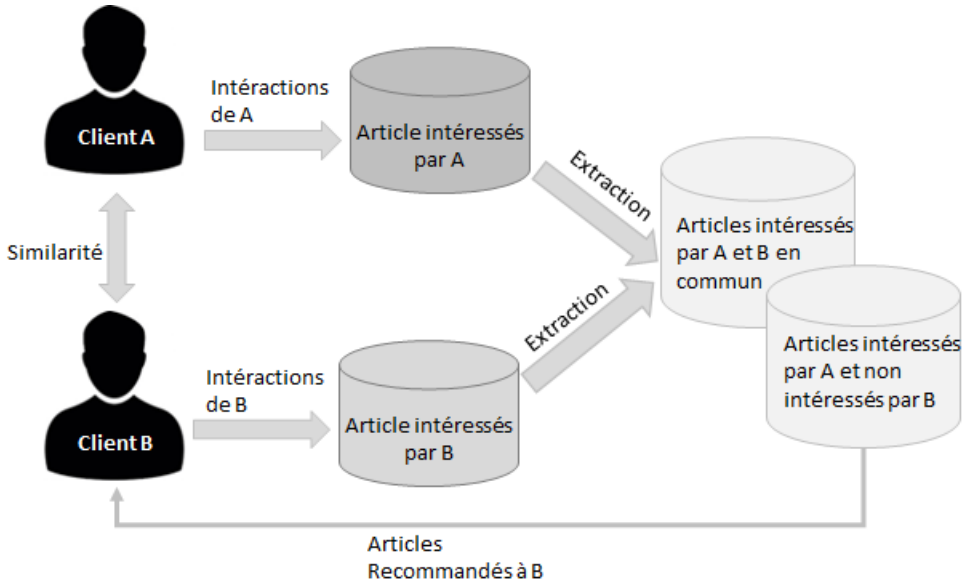

Figure 8 - Filtrage collaboratif

Parmi les différentes techniques de filtrage collaboratif, la factorisation matricielle *(MF)* est la technique la plus populaire (X. He*, et al.*, 2016; Koren, 2008). Elle consiste à projeter les utilisateurs et les articles dans un espace partagé latent, en utilisant un vecteur de caractéristiques latentes pour représenter un utilisateur ou un article. Des études plus récentes ont développé des techniques basées sur les réseaux neurones telles que le NCF *(Neural network based Collaborative Filtering*) (X. He & Chua, 2017; X. He*, et al.*, 2017).

2.7.2 Filtrage basé sur le contenu

Les techniques de filtrage basées sur le contenu (*Content-Based Filtering (CBF)*) recommandent des produits similaires ou à contenu similaire à ceux qu'un consommateur a positivement notés dans le passé (D. Wang*, et al.*, 2018), ce qui associe la similarité du profil de l'utilisateur avec le profil des articles. En d'autres termes, ces articles ont été cotés précédemment par un utilisateur et le système effectue une recherche de « Mots-clés » pour savoir si un élément est similaire à l'autre (Núñez-Valdez*, et al.*, 2018). Tel que montré dans la Figure 9, le profil des articles se constitue par l'intermédiaire des attributs ou descripteurs qui identifient l'article, tandis que le profil des usagers se forme de deux

façons : implicite selon les interactions avec les articles, ou explicites à partir des questions directes.

Les travaux sur les systèmes de recommandation ne cessent de proliférer. Certains travaux ont proposé un système de recommandation basé sur le contenu des produits en ligne à l'aide de la notation des livres d'Amazon pour prendre en charge les services de *B2C* dans le commerce électronique (Lee, *et al.*, 2012) d'autres ont analysé Twitter pour recommander des nouvelles dans le média (Phelan, *et al.*, 2009).

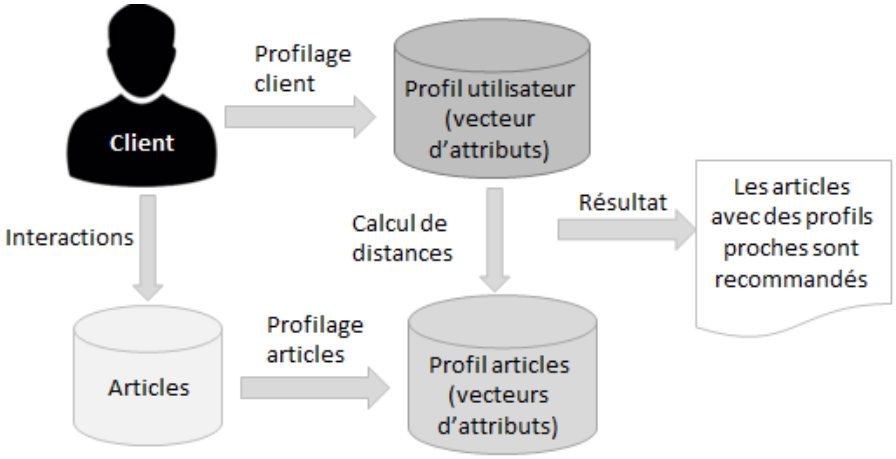

Figure 9 - Filtrage basé sur le contenu

Cependant, les systèmes de recommandation à base de contenu doivent composer avec quelques problèmes. Ces systèmes ont tendance à échouer (Ahn, 2008; Scholz, *et al.*, 2017), s'ils ne disposent pas de suffisamment de données, et si les algorithmes de filtrage à base de contenus ne peuvent fournir de bonnes recommandations. De même que dans le cas de démarrage à froid, le système ne possède pas de suffisamment de données pour formuler une recommandation crédible (H. M. Kim, *et al.*, 2017).

2.7.3 Filtrage hybride

Les techniques de recommandations hybrides (Z. Liu, *et al.*, 2010; Lucas, *et al.*, 2013) sont basées sur une combinaison des filtrages collaboratifs et des approches axées sur le contenu pour aborder le problème de démarrage à froid et améliorer la performance du système de recommandation (Bagherifard, *et al.*, 2017). Tout en exploitant les caractéristiques de ces

deux techniques, les systèmes hybrides cherchent à surmonter les limites des deux systèmes pour obtenir de meilleures recommandations.

Prenons l'exemple des systèmes de recommandation hybrides de *Netflix* et *Cinematch*. Ceux-ci analysent les scores cumulés de films et les utilisent pour faire des prédictions personnalisées aux abonnés, de façon hebdomadaire, chacune basée sur leurs goûts particuliers. Le système de recommandation *Cinematch* analyse automatiquement les scores cumulés de films avec tous les autres films afin de déterminer une liste de films «semblables» qui sont susceptibles de plaire. Puis, comme l'utilisateur fournit des scores, le système détermine une prédiction unique et personnalisée pour chaque film recommandable fondée sur ces scores.

Nous abordons la prise de décision dans la section suivante puisque celle-ci constitue un élément de base dans tout environnement du commerce électronique.

2.7.4 Prise de décision

Le processus décisionnel constitue un intérêt majeur dans le cadre du commerce électronique. Des modèles de développement sont accomplis sur le plan commercial (Vincent*, et al.*, 2017; Wu*, et al.*, 2018), comme sur le plan sociocommercial (Aladwani, 2018; A. Chen*, et al.*, 2017; Hajli, 2015). Dans le contexte de prise de décision, nous nous intéressons à l'environnement commercial.

À ce sujet, les modèles décisionnels ont favorisé le succès du domaine dans les ventes aux enchères en ligne (Adomavicius & Gupta, 2005) pour assurer les stratégies de négociations en ligne. Par ailleurs, ils étaient aussi le principal mécanisme d'échanges dans les interfaces homme-machine (Bichler*, et al.*, 2010) et l'introduction des agents intelligents qui répondent aux consommateurs d'une façon autonome (Liang*, et al.*, 2012). Le domaine commercial repose sur deux principes. Le premier est fondé sur la confiance entre l'utilisateur et le fournisseur pour obtenir des bénéfices. Le second correspond à la satisfaction de l'utilisateur. Du point de vue du client, le processus d'achat passe par différentes phases afin d'adopter ou non le service/produit. Cependant, l'introduction des transactions en ligne dans les activités commerciales a compliqué le processus et a rendu les clients souvent incapables d'évaluer profondément toutes les options disponibles avant

de prendre leur décision (Beach, 1993; H. Li*, et al.*, 2014), ce qui fait que les transactions en ligne renferment de l'incertitude dans leur déroulement en comparaison avec une transaction qui se fait dans le magasin en raison du manque d'interaction entre le consommateur et le vendeur.

Pendant le processus décisionnel de leur achat, les consommateurs recueillent de l'information concernant les attributs du produit ou services voulus (Bai*, et al.*, 2015) et les recommandations sollicitées par d'autres sources d'information (K. Z. Zhang*, et al.*, 2014). Parfois, ils décident en se basant sur des expériences et des conséquences antérieures (Filieri*, et al.*, 2015). En outre, ils s'appuient sur quelques informations collectées à partir des facteurs sociaux comme les commentaires et les interprétations des clients précédents (Seckler*, et al.*, 2015), ou bien les interprétations du e-marchand lui-même (Alese & Ayeni, 2013). Dans d'autres situations, un niveau de connaissance relativement assez élevé des garanties de confiance pourrait inciter les consommateurs à savoir de quelle information ils ont besoin pour les étapes de leur prise de décision. En conséquence, ils ont recours à des garanties de confiance sur le site (H. Li*, et al.*, 2014), ce qui a des impacts positifs sur la confiance en ligne du point de vue du processus décisionnel.

Des facteurs humains comme les intentions, les attitudes, la confiance et la perception de risque ont été impliquées d'une façon critique et ont influencé la prise de décision du consommateur en ligne (Shen & Chiou, 2010; Yang*, et al.*, 2015). D'autres facteurs explicatifs ont pu être identifiés comme ayant aussi un impact plus substantiel sur la prise de décision. Nous pouvons citer les facteurs liés au marchand tels que : la conception des pages Web, réputation, qualité de service, et autres en relation avec le produit/service tels que la spécification, la qualité ou le contenu (Rouibah*, et al.*, 2016; See-To & Ho, 2016).

Chapitre 3 : Problématique de recherche

La technologie de paiement est l'une des interfaces en ligne qui facilite le transfert d'argent entre les détaillants et les consommateurs. Les progrès dans ce domaine s'avèrent d'une importance stratégique pour les fournisseurs de services de paiement ainsi que pour les commerçants, afin d'introduire des solutions adéquates et sécuritaires. D'une part, les vendeurs investissent des efforts dans le but d'offrir des systèmes de paiement bien conçus (Ho & See-To, 2018; Othman*, et al.*, 2017) et de faciliter l'expérience des consommateurs en ligne. D'autre part, il existe un intérêt pour les consommateurs qui essaient constamment d'éviter la perte du contrôle de leurs dépenses (Haws*, et al.*, 2012), et ceci, en naviguant à travers les pages du site Web pour choisir la méthode la plus adéquate pour conclure leurs transactions.

Malgré tous ces efforts, des recherches ont montré que les mécanismes de paiement affectent de manière significative la décision des consommateurs ainsi que leurs habitudes de consommation (See-To & Ho, 2016; See-To & Ngai, 2018). Cela influence considérablement leurs comportements (Ho*, et al.*, 2013) et leurs perceptions du risque (Beltramo*, et al.*, 2015). En dépit de l'importance de cette problématique pour les professionnels en commerce ainsi que pour les académiciens, peu de recherches ont examiné l'effet de tels mécanismes sur les consommateurs et leurs processus de prise de décision. Parmi les conséquences, *l'abandon de la page de paiement* est l'une des décisions que le consommateur peut envisager durant le processus de la transaction. La Figure 10 révèle les différentes raisons de quitter la page et s'abstenir de payer suite à une statistique faite aux États-Unis en 2019 engageant 4263 réponses[2].

Par ailleurs, d'autres problèmes surviennent dans le processus du paiement en ligne. Dans un premier temps, nous commençons par positionner la problématique par rapport à la protection de vie privée et toutes les conséquences négatives qui en découlent. Dans le même contexte, nous traitons le sujet de la cybersécurité et toutes les problématiques qui en résultent.

[2] https://baymard.com/lists/cart-abandonment-rate consultée le 16/Sep/2019

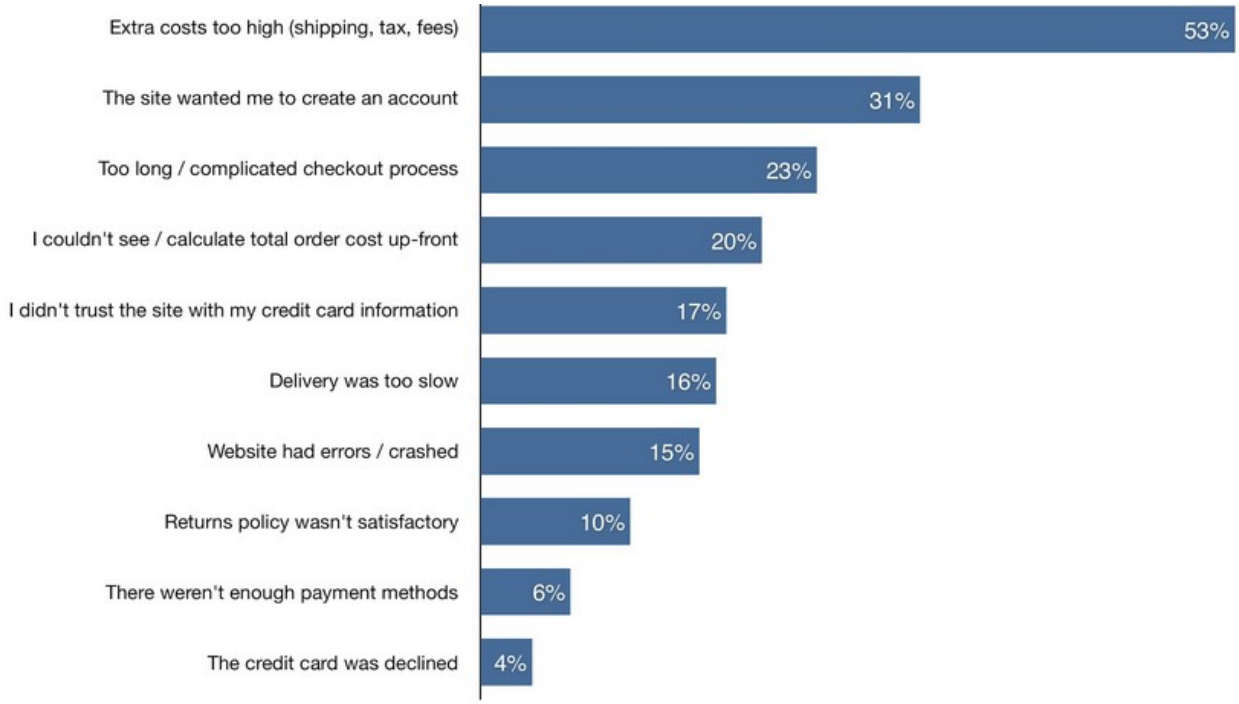

Figure 10 - Raisons pour abandonner la page du paiement en ligne

Par la suite, nous abordons l'étude des facteurs qui influencent l'adoption de la technologie de paiement en ligne (M. Cui & Pan, 2015; See-To & Ho, 2016). Enfin, nous visons plus particulièrement le domaine des systèmes de recommandation afin de remédier au problème de la protection de la vie privée et la variation des préférences des usagers.

3.1 L'adoption de la technologie de paiement en ligne

La procédure de transaction dans les paiements électroniques est différente de celle adoptée dans les paiements traditionnels, ce qui peut engendrer une série de nouveaux problèmes de sécurité, y compris les préoccupations sur le statut d'utilisation mal intentionné ou illégal, les transactions non autorisées (Hwang*, et al.*, 2007; Lim, 2008; N. Xu*, et al.*, 2017) ou fraudes d'identité. Comme les consommateurs utilisent ces solutions de plus en plus par l'intermédiaire de téléphones portables, d'assistants numériques personnels, d'ordinateurs et de décodeurs de télévision pour acheter des biens et des services partout dans le monde, il y a une croissante préoccupation associée aux questions de sécurité et de confidentialité des transactions en ligne. Contrairement à la façon traditionnelle de vendre des biens et des

services, le commerçant en ligne doit traiter les transactions par l'intermédiaire d'une **carte** de débit/crédit**,** ce qui en fait une cible très vulnérable pour les fraudeurs.

Par ailleurs, des recherches envisagées dans les paiements en ligne ne visent pas seulement la perspective de la sécurité de la transaction, mais aussi l'étude psychologique du comportement et des attitudes en ligne. Par exemple, Plouffe *et al.* (Plouffe*, et al.*, 2001) ont essayé de comprendre l'adoption des paiements par cartes intelligentes par les marchands à la lumière de la perspective psychologique du consommateur. Plus récemment, des études (See-To & Ho, 2016) ont abordé la façon dont le consommateur perçoit les différents attributs discernés dans la solution de paiement électronique. Les travaux réalisés nous ont beaucoup appris sur les fonctionnalités de la technologie, mais aucune étude ne s'est encore intéressée aux questions suivantes : **comment les consommateurs perçoivent-ils la crainte de perte financière et affrontent les problèmes de protection de vie privée ? Quelles sont leurs préoccupations au sujet de la cybersécurité en termes de sensibilisation et confiance en ligne ? Quelles sont les caractéristiques du site qui influencent le processus de prise de décision** ?

Afin de remédier à ces problématiques, nous réalisons une nouvelle approche en deux phases. La première consiste à présenter une étude sur les multi-craintes de l'usager en ligne. À cette fin, nous menons une enquête sur **l'adoption du paiement en ligne**. À partir des résultats, nous analysons dans le chapitre 4 les facteurs influençant le processus de prise de décision. La seconde étape consiste à lancer en ligne une expérience d'achats virtuels dans le contexte de la cybersécurité. Durant l'expérience, nous ciblons le sujet du comportement de l'usager et ses perceptions de préservation de vie privée.

3.2 Manque de contrôle dans les paiements en ligne

Avec le développement du commerce électronique et des capacités d'interactivité avec le consommateur, beaucoup de chercheurs intensifient leurs efforts pour mettre en place de nouvelles solutions techniques. Leur but est de rendre les transactions en ligne plus simples et rapides, sans toutefois sacrifier la sécurité des informations. D'un point de vue technique, le paiement en ligne est au centre de trois entités : (i) **la passerelle d'information** qui s'occupe de la sécurité et protection des données (ii) **le site Web** par lequel les échanges

d'informations circulent (iii) **les échanges avec le marchand** ou fournisseur de services qui conservent les transactions générées. La convergence de ces trois entités, aux fonctions distinctes, implique de complexes conciliations lors des transactions. Par ailleurs, dans un environnement financier où la sécurité occupe une place extrêmement importante, les transactions doivent satisfaire les propriétés suivantes (C. Kim*, et al.*, 2010) :

La **confidentialité** : assure que les données et les transactions ne peuvent être interceptées par une entité non autorisée.

L'a**uthentification** : assure que la transaction est bien issue du partenaire de la transaction.

L'**intégrité** : assure que les informations restent intactes tout au long de la transaction et ne peuvent être altérées.

L'**autorisation** : assure que les entités engagées sont capables de vérifier si toute personne impliquée dans la transaction est autorisée à effectuer une transaction.

La **non-répudiation** : assure que personne ne peut réclamer qu'une transaction soit effectuée par quelqu'un d'autre.

Comme toute interface technique, des régulations s'imposent dans les solutions de paiement pour sécuriser les transactions liées à la méthode de paiement, ainsi que pour contrôler les échanges monétaires. Toutefois, les clients n'ont aucun contrôle sur le flux d'information, et ils ne possèdent pas le pouvoir de gérer leurs informations sensibles. Puisque les marchands peuvent être localisés n'importe où dans le monde, le fait de fournir des informations sensibles pose de grandes menaces à la vie privée (Antoniou & Batten, 2011; Sahnoune*, et al.*, 2015). Ces dernières rendent les clients de plus en plus concernés en matière de vie privée et estiment qu'ils pourraient être victimes de vols d'identités ou de fraudes (Hille*, et al.*, 2015). Effectivement, **juste 2% des internautes aux États-Unis** estiment que leurs données personnelles en ligne ne sont pas exposées de façon vulnérable[3] (voir Figure 11).

[3] https://www.statista.com/statistics/972911/adults-feel-data-personal-information-vulnerable-hackers-usa/ consulté le 29/sep/2019

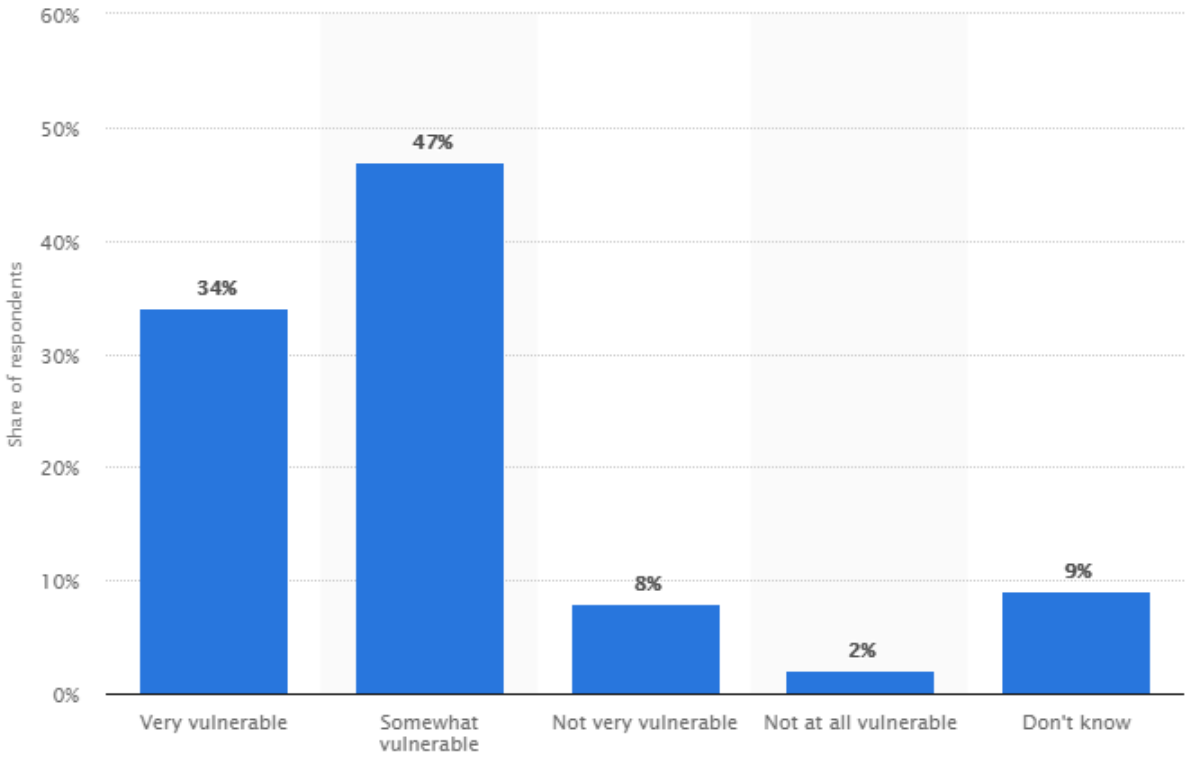

Figure 11 - Pourcentage des internautes aux États-Unis qui pensent que leurs données personnelles sont vulnérables

Dans notre recherche, nous proposons *un nouveau système de paiement électronique conditionnel, personnalisé et basé sur les systèmes de paiement par carte***,** avec l'agrégation des cartes de crédit virtuelles et qui procurent le contrôle et la supervision totale du détenteur de carte sur ses paiements en ligne.

3.3 Menaces en ligne

Afin d'assurer une communication en ligne, les ingénieurs en informatique détectent des innovations dans les protocoles de paiement pour assurer des transactions sécurisées en ligne, empêchant les intercepteurs de capturer les détails des comptes des clients. Le commerçant devra traiter les transactions dans un environnement virtuel, tandis que le client devra généralement fournir plus d'informations sensibles que lorsqu'il conduit l'opération dans un environnement physique pour des raisons de vérification telles que *son adresse, son numéro de carte de crédit, son numéro de vérification* **(***CVV***)**. En conséquence, les commerçants tentent de conserver ces informations aussi longtemps qu'ils le souhaitent.

Ils peuvent être parfois malhonnêtes ou incompétents. Les fichiers contenant les données des clients personnelles, sensibles et chiffrées peuvent être dévoilés et par la suite volés ou vendus. Notons qu'en Juin 2019, les membres du Mouvement Desjardins ont fait face à un enjeu dans lequel les renseignements personnels de 2,9 millions de personnes ont été volés et communiqués à des entités à l'extérieur de l'organisation[4].

Dans l'ensemble, l'expérience due aux incidents de *vols d'identité* est majoritairement importante et devrait être prise en compte lors de l'évaluation des coûts de fraudes potentiels et des habitudes de paiement (Kahn & Liñares-Zegarra, 2016). Sur Internet, les effets inhérents au contexte (notamment le risque perçu) exposent l'internaute à plus de fraudes et posent, en corollaire, la question de la confiance avec plus d'acuité.

Par ailleurs, les consommateurs essaient différentes méthodes pour prévenir et combattre les fraudes d'identités comme le montre une enquête faite en 2019 par **CompareCards**, portant sur 750 consommateurs qui ont au moins une carte de débit ou crédit[5]. La Figure 12 révèle les résultats d'une façon comparative pour les années 2018 et 2019. Malgré ces préventions, les clients peuvent être exposés involontairement et sans qu'ils le sachent à une menace sérieuse pour la vie privée (C. Kim*, et al.*, 2010) lors de la divulgation de leurs détails de paiement et autres renseignements sensibles en effectuant une transaction en ligne.

[4] https://www.tvanouvelles.ca/2019/06/20/les-renseignements-personnels-de-29-millions-de-membres-desjardins-divulgues consultée le 14/Déc./2019

[5] https://www.cnbc.com/2019/09/06/two-years-after-equifax-breach-consumers-still-vulnerable-to-id-theft.html consultée le 16/Sept./2019

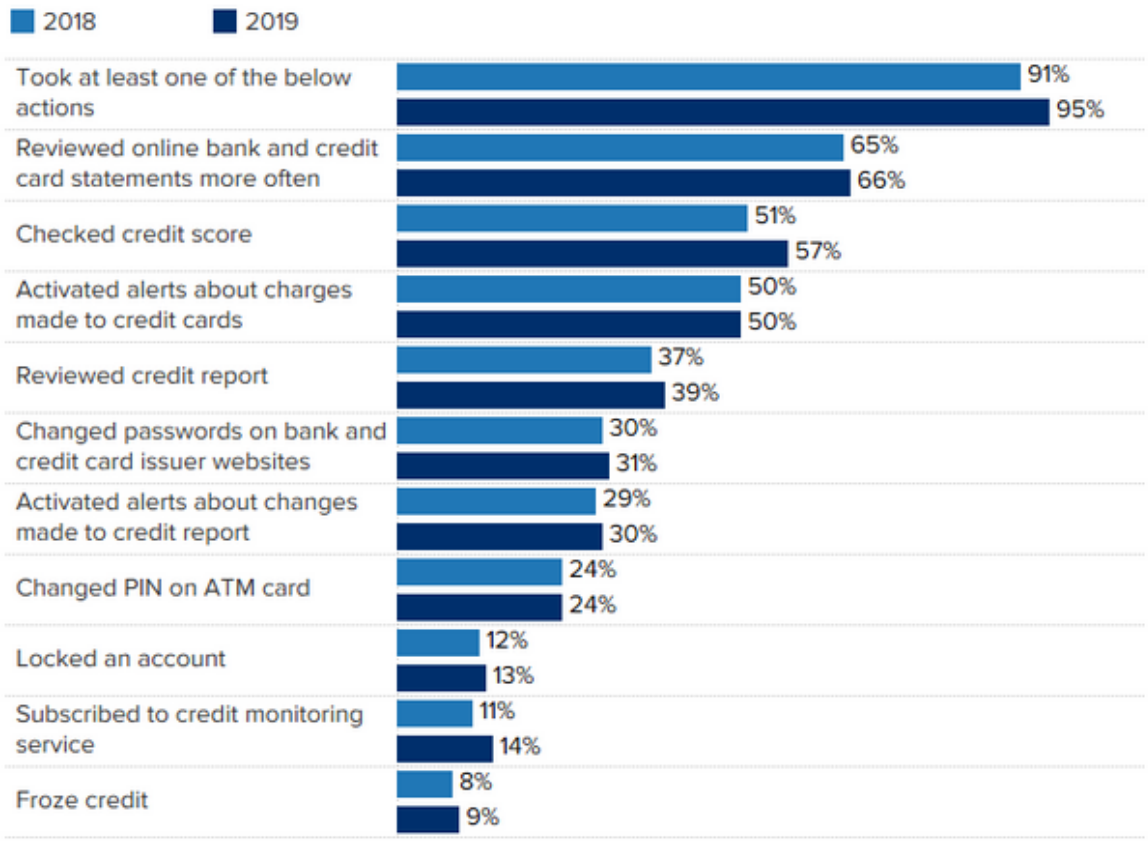

Figure 12 - Actions envisagées pour prévenir et combattre les vols d'identités

En conséquence, le consommateur est plus que jamais vulnérable en ligne. Pour répondre à cette problématique, nous proposons dans le chapitre 5 un **nouveau protocole de paiement en ligne** dans le cadre de notre plateforme de paiement innovatrice qui *minimise les risques de vols d'identités et assure la protection de la vie privée*. Effectivement, le client ne dévoilera pas son identité ni ses informations personnelles dans notre protocole. De même, il pourra configurer des préférences de nature publiques ou privées, réalisant ainsi un environnement d'échanges qui respecte les exigences de vie privée et garantit en même temps l'authenticité.

3.4 Cybersécurité en ligne

Bien que la plupart des individus semblent considérer l'Internet comme un environnement sûr et sont prêts à l'utiliser continuellement et sans cesse, des cyberattaques surviennent sur une base quotidienne (de Bruijn & Janssen, 2017). Ces dernières ne visent pas seulement les nations et les entreprises, elles affectent aussi les individus (Hiller & Russell,

2013). Prenons la menace en Juin 2019 contre les membres du Mouvement Desjardins suite à la divulgation de leurs renseignements personnels (voir section 3.3). Leurs conséquences peuvent varier en fonction de l'ampleur et de la gravité de l'incident, allant de l'impact nul ou limité, au déni de services distribués (*DDoS*), aux vols de données, à la manipulation de données, aux vols d'identités jusqu'à la prise du contrôle du système d'information.

Ceci dit, garantir la sécurité en ligne s'avère difficile. Avec l'intrusion des logiciels malveillants, les sites Web ont une sécurité limitée (J. J. Zhao & Zhao, 2010) et peuvent être facilement piratés. De tels incidents engendrent une grave menace sur la sécurité des internautes (Bauer & Van Eeten, 2009) et causent des dommages inévitables sur leurs données (Ten*, et al.*, 2008) (Leuprecht*, et al.*, 2016).

Par ailleurs, la préoccupation dans les domaines de cybersécurité se concentre sur les impacts et la façon de traiter les incidents *après qu'ils surviennent*. Dans la plupart des cas, l'internaute ne prend conscience du problème qu'après avoir été victime d'une fraude ou d'un vol d'identité et, donc, après avoir subi une perte financière ou une catastrophe personnelle. Prenons l'exemple des utilisateurs des systèmes au sein des entreprises. Le renforcement de la sécurité passe par l'instauration de barrières qui servent de lumières rouges telles que limiter l'accès des documents à certaines personnes, obliger la double authentification, bloquer l'accès à certains sites ou définir des mots de passe sécurisés. Toutes ces mesures permettent à l'employé d'éviter certains comportements qui pourraient mettre à risque la sécurité des systèmes informatiques. En outre, des études antérieures ont signalé l'importance de la théorie de protection par motivation (Tsai*, et al.*, 2016) (*Protection Motivation Theory* or *PMT*). Cette dernière suggère que lorsque les individus perçoivent qu'ils sont plus sensibles aux menaces de sécurité et lorsque les menaces sont plus sévères, ils sont plus susceptibles d'adopter la solution recommandée pour combattre cette menace (McBride*, et al.*, 2012). Prenons l'exemple de la recherche de logiciels résistants contre les programmes malveillants et la sauvegarde des données. Dans la plupart des cas et même si l'usager ne possède pas un niveau de compétence suffisamment technique, il ira jusqu'à compléter des activités telles qu'installer des logiciels de sécurité, utiliser des mots de passe complexes et s'abstenir d'ouvrir des courriels risqués (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010).

Compte tenu de la gravité de la situation, les questions suivantes se posent **:** pourquoi existe-t-il si peu de sensibilisation ? Et pourquoi ne prenons-nous pas de mesures draconiennes de prévention ? Afin de répondre à ces problématiques, nous présentons dans le chapitre 6 une expérience de magasinage en ligne. La démarche de l'expérience propose une liste de scénarios inspirée du *questionnaire sur les aspects humains de la sécurité de l'information* (*The Human Aspects of Information Security Questionnaire* ou *HAIS-Q***)**. Comme indiqué dans la Figure 13, le *HAIS-Q* comprend sept domaines d'intérêt basés chacun sur les connaissances, l'attitude et le comportement (*Knowledge, Attitude and Behavior* ou *KAB*) (McCormac*, et al.*, 2017). À savoir : utilisation d'Internet, utilisation des courriels, utilisation des médias sociaux, gestion des mots de passe, signalement des incidents, la manipulation de l'information, l'infographie mobile. Dans ce travail, nous cherchons à examiner la relation entre la connaissance en cybersécurité, le comportement en ligne et la sensibilisation à la sécurité de l'information (*Information Security Awareness* or *ISA*) chez les internautes.

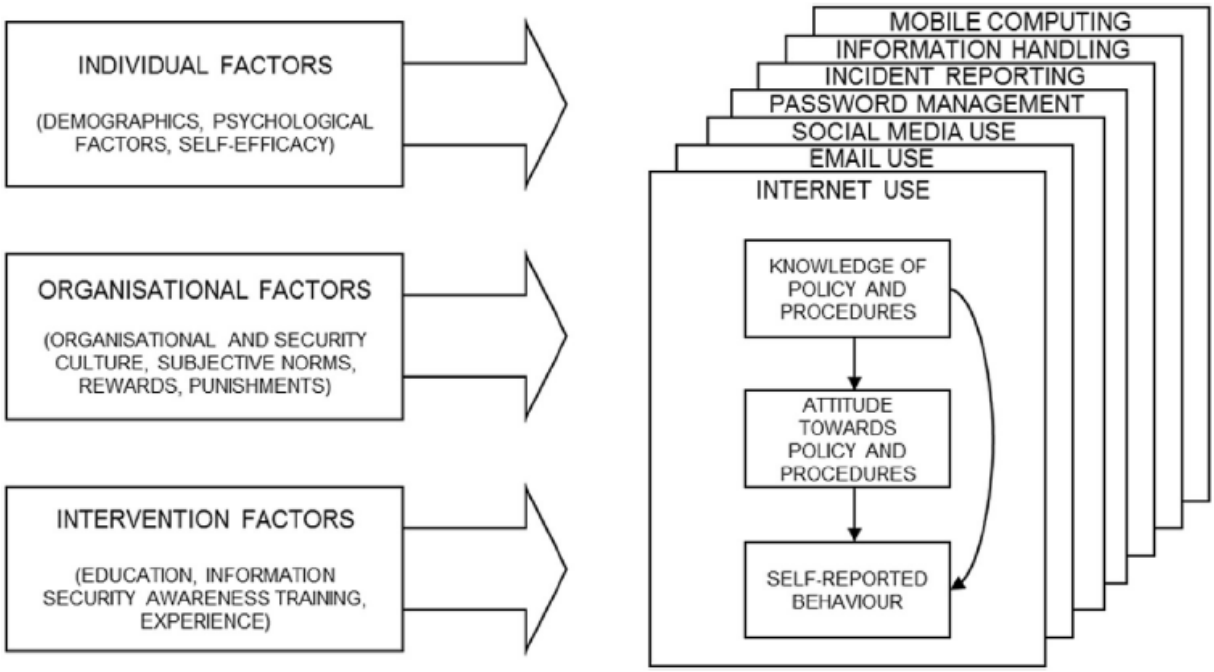

Figure 13 - Le modèle des aspects humains de la sécurité de l'information inspiré de (Parsons*, et al.*, 2014).

3.5 Systèmes de recommandation

Les systèmes de recommandation posent une problématique en matière de vie privée puisque cette technologie s'appuie sur les profils des usagers. Dans ce contexte, le système recommande des items qui sont similaires à ceux que l'utilisateur a aimés dans le passé (Pazzani & Billsus, 2007). Par exemple, si l'utilisateur a apprécié positivement un film qui est de genre romantique, alors le système peut fournir des recommandations sur d'autres films de même genre. Par conséquent, le maximum d'informations échangées à propos de l'utilisateur peut assurer une prédiction selon son profil. Les méthodes qui explorent implicitement l'historique des pages Web visitées pour construire les profils posent un problème de confidentialité tel que le « *Profinder* » (Isinkaye*, et al.*, 2015).

Cependant, une extrême protection de la vie privée peut rendre les recommandations inutiles. Les questions suivantes se posent : **comment assurer un équilibre entre la divulgation des données et leur utilité pour le filtrage collaboratif** tout en gardant une meilleure source de recommandations ? **Comment gérer la publication des données tout en respectant la vie privée** et surtout si ces données sont exigées par les systèmes de recommandation collaboratifs ? Afin de répondre à ces problématiques, nous proposons dans le chapitre 7 un nouveau modèle d'équilibre entre la protection de vie privée et l'utilité. Afin d'assurer un équilibre adéquat entre les deux caractéristiques, notre modèle est basé sur le « ***k*-coRating** » qui est un modèle de protection de la vie privée. Non seulement il masque les évaluations originales de telle sorte qu'une confidentialité de k données anonymes est préservée, mais il améliore également l'utilité des données.

Outre la problématique de préservation de vie privée, les systèmes de recommandation s'appuient sur les appréciations données par un ensemble d'utilisateurs sur un ensemble d'articles (Harper & Konstan, 2016) (cas de filtrage collaboratif). Ces appréciations révèlent leurs préférences et aident à retrouver les groupes ou communautés ayant des goûts en commun. Cependant, ce type de filtrage ne tient pas compte de la probabilité de changer d'avis dans le futur. La prédiction en fonction des articles les plus proches de ceux qu'ils ont déjà notés n'aboutit pas nécessairement à un résultat positif et satisfaisant. Il existe une probabilité non négligeable de changer de préférence dans la fois suivante. Afin de remédier à cette problématique, nous analysons dans le chapitre 8

l’instabilité des usagers dans leurs préférences qui peut engendrer une déception en ligne et un abandon des articles recommandés.

Chapitre 4 : Les multi-craintes des usagers en ligne

Dans les paiements en ligne, les clients doivent transmettre leurs informations personnelles et financières par l'intermédiaire d'un site Web pour conclure leurs achats et payer les services ou articles sélectionnés. Ils ont trois principaux intervenants qu'ils doivent considérer afin de prendre une décision de payer en ligne: *le vendeur, la page du paiement, et leurs propres perceptions.* Cependant, peu d'études ont exploré ces trois facteurs dans un environnement d'achat en ligne. Dans le présent chapitre, nous nous concentrons sur les préoccupations des clients en matière de confiance et de perception à savoir la perception du risque, la perception de la sécurité des paiements et la perception envers la crainte de perte financière.

4.1 Confiance et perception du risque en ligne

De nos jours, la croissance du commerce électronique ainsi que le développement rapide de la technologie impliquent plusieurs innovations dans les services offerts sur le Web tels que les systèmes de recommandation, les outils de négociation en ligne, les moteurs de recherche, la sécurité des voies de communication, les méthodes de recherche de produits, l'historique des factures ainsi que le suivi des commandes.

Le concept de **confiance** en ligne est à la croisée de plusieurs champs disciplinaires. Dans le commerce électronique, la confiance en ligne constitue un enjeu majeur pour les marchants souhaitant établir des relations à long terme avec les consommateurs (Ruiz-Mafe*, et al.*, 2014).

En règle générale, l'utilisateur est confortable à l'idée de fournir des informations vagues et générales, telles que ses préférences, mais ne se sent pas tellement à l'aise de fournir son compte bancaire ou les numéros de ses cartes de crédit qui sont considérés comme des informations sensibles (Mahadevan & Kaleta, 2017). En plus de la confiance, d'autres facteurs peuvent influencer le comportement de l'utilisateur au niveau de la **perception du risque** (Dahlberg*, et al.*, 2015; Slade*, et al.*, 2015).

Des études antérieures ont montré que la perception du risque peut influencer l'adoption et l'acceptation du service de paiement électronique (See-To & Ho, 2016). Dans

un scénario commercial caractérisé par un risque d'une menace sur la vie privée, les clients peuvent changer l'évaluation de leurs pertes et profits liés au processus de divulgation (Acquisti & Grossklags, 2004; Barth & de Jong, 2017). Par exemple, lors des transactions en ligne, les utilisateurs divulguent des informations privées telles que leur numéro de téléphone afin d'obtenir des notifications sans frais à propos des horaires de vols, surtout s'ils voyagent à une fréquence élevée et ceci même si leurs préoccupations en matière de confidentialité s'opposent en général avec ce comportement.

Bien qu'il existe un important flot de littérature sur la confiance et la perception de risque dans le commerce électronique, des études scientifiques ont largement abordé théoriquement d'autres facteurs comme le comportement, les intentions, les croyances qui peuvent influencer la décision du client et améliorer son expérience en ligne (Choi*, et al.*, 2016; Shen & Chiou, 2010). Cette dernière peut être intensifiée en ajoutant des messages de promotion de la confiance sur la page du check-out ce qui implique une **attitude positive** dans le contexte des transactions en ligne (Shu & Cheng, 2012). En revanche, **l'attitude négative** est causée par une expérience négative due à une vulnérabilité qui peut être liée soit à une violation de vie privée ou fraude (Meuter*, et al.*, 2000), soit à un échec de la technologie ou un manque d'interaction humaine (Meuter*, et al.*, 2000; Shankar*, et al.*, 2003). Cet état indésirable peut augmenter la perception du risque de la part de l'utilisateur au cours de l'expérience en ligne.

Néanmoins, peu de recherches ont étudié l'influence des composants du site Web du vendeur (tels que *la facilité d'utilisation, la qualité des informations et les signes de sécurité*) sur la **perception de la sécurité des paiements** telle qu'une connexion en ligne sur un réseau non sécurisé ainsi que leur impact sur la **perception envers la crainte de perte financière** telle qu'une déclaration de confidentialité ambiguë et compliquée. Ces perceptions, que nous allons envisager dans ce chapitre, nous amènent au sujet de la prise de décision en présence des craintes en ligne.

4.2 Craintes et paiements en ligne

Dans un effort continu, les vendeurs en ligne tentent de minimiser les risques liés aux transactions de paiement électronique, de gagner la confiance des clients et d'entretenir des

relations à long terme avec eux (N. Xu*, et al.*, 2017). Ceci se déroule en maintenant l'équilibre entre l'adoption de la technologie appropriée et la prévention des menaces contre la sécurité en ligne. De même, la satisfaction du client est un objectif essentiel pour les vendeurs en ligne afin d'augmenter les intentions d'acheter de nouveau (T.-H. Liao, 2017).

Cependant, les vendeurs en ligne ne peuvent garantir la satisfaction du client après chaque achat. Ce qui explique la croissance des valeurs des retours des marchandises annuelles de *75.2%* de plus par rapport aux quatre dernières années. Selon *Statista*, la valeur des retours est estimée aux États-Unis à *550 milliards en 2020*[6]. À signaler aussi que *93%* des clients vérifient la politique des retours avant de faire un achat en ligne[7].

Par ailleurs, les fournisseurs cherchent à implémenter des environnements sécurisés afin d'exploiter leurs services de paiement. Toutefois, ceci ne garantit pas la protection de la vie privée et ne minimise pas les fraudes. Selon le rapport de « *Federal Trade Commission* », **trois millions** de plaintes concernant les fraudes et les vols d'identités ont été reçues durant l'année 2018 (Commission, 2018). En parallèle, les vendeurs exploitent des efforts pour une collecte de données plus obscure au lieu de privilégier la vie privée des utilisateurs. En conséquence, les vendeurs peuvent utiliser les données des consommateurs sans leur consentement et même sans notification pour des buts commerciaux. Prenons l'exemple d'un des plus grands piratages de l'histoire, celui d'*eBay* où un pirate a réussi à se procurer des codes d'accès et à voler des données personnelles de *145 millions* de victimes potentielles[8].

Dans ce contexte, les craintes du client en ligne *(représenté en anglais par **Online Customer Fears (OCF))*** constituent notre principale préoccupation.

Pour ce faire, nous étudions principalement les relations spécifiques à la décision du client de payer en ligne avec l'intégration de trois déterminants : la protection de vie privée, la sécurité et la crainte d'une perte financière ou d'une fraude et la confiance. Dans ce

[6] https://www.shopify.com/enterprise/ecommerce-returns consulté le 25/Sep/2019
[7] https://dotcomdist.com/2019-dotcom-distribution-ecommerce-study/ consulté le 25/Sep/2019
[8] https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html consulté le 25/Sep/2019

contexte, notre objectif principal consiste à fournir une meilleure compréhension des *OCF* et à obtenir un aperçu de leurs influences potentielles sur les usagers dans un environnement en ligne (El Haddad, Aïmeur*, et al.*, 2018).

4.2.1 Objectifs de recherche

Après avoir lancé une enquête en ligne, nous avons recueilli des données à partir des réponses de 392 participants. Les questions portaient sur le magasinage en ligne et la prise de décision de payer en ligne. Suite à ça, nous avons défini les facteurs essentiels qui affectent les craintes en ligne. Comme point de départ, nous avons extrait les influences de la conception des sites d'achats sur la prise de décision de paiement en ligne incitée par trois facteurs : *la facilité d'utilisation, les signes de sécurité et la qualité de l'information.* Par la suite, nous avons défini un modèle de recherche qui examine les effets et l'influence de ces composants mentionnés sur les quatre déterminants : *la confiance, la perception de la sécurité du paiement, la préservation de vie privée contre la violation et la perception de crainte de perte financière***.** La présente étude a visé principalement à répondre aux questions de recherche suivantes : (1) quels sont les facteurs qui influencent la décision du client pour payer en ligne ? (2) est-ce que la confiance du client surmonte ses craintes en ligne ? (3) est-ce que la perception de crainte de perte financière a un impact sur la protection de sa vie privée ?

Pour atteindre nos objectifs, nous fournissons dans la section suivante notre modèle de recherche empirique et citons les hypothèses développées pour élaborer les questions précitées.

4.2.2 Hypothèses et modèle de recherche

Nous avons intégré dans notre recherche les préoccupations du client en matière de confidentialité et défini la relation avec la décision de payer en ligne. Nous avons obtenu un modèle de recherche conceptuel (illustré à la Figure 14) indiquant les hypothèses à développer et à valider. La méthode des équations structurelles a été retenue pour tester notre modèle conceptuel. Vu que la méthode des équations structurelles est une approche méthodologique et empirique, elle a également été considérée comme une extension de la

régression, car elle offre la possibilité de traitement des relations linéaires simultanées entre les variables explicatives et les variables à expliquer d'un modèle prédéfini (Byrne, 2013).

En nous basant sur le modèle conçu, nous avons extrait **onze hypothèses** définies comme suit :

H1. *L'apparence des signes de sécurité sur le site a un effet positif sur la perception de la sécurité des paiements du client.*

H2. *La facilité d'utilisation du site a un effet positif sur la perception de la sécurité des paiements du client.*

H3. *La qualité de l'information du site a un effet positif sur la perception de la sécurité des paiements du client.*

H4. *L'apparence des signes de sécurité sur le site a un effet positif sur la confiance du client.*

H5. *La facilité d'utilisation du site a un effet positif sur la confiance envers un vendeur en ligne.*

H6. *La qualité de l'information du site a un effet positif sur la confiance du client.*

H7. *La perception de la sécurité des paiements a un effet positif sur la perception de la crainte de perte financière.*

H8. *La confiance du client a un effet positif sur la perception de la crainte de perte financière.*

H9. *La perception de la crainte de perte financière a un effet positif sur les préoccupations relatives à la vie privée.*

H10. *La perception de la crainte de perte financière a un effet positif sur la décision de paiement en ligne.*

H11. *Les préoccupations relatives à la protection de la vie privée ont un effet positif sur la décision de paiement en ligne.*

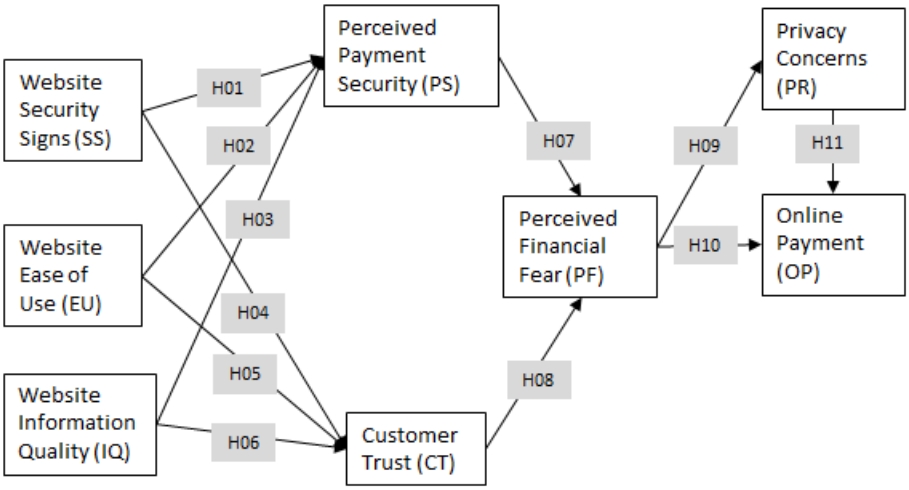

Figure 14 - Modèle de recherche en commerce électronique

La vérification du modèle conceptuel présenté précédemment suppose le choix d'une méthodologie de recherche convenable à la problématique. Pour atteindre les objectifs de l'étude, nous décrivons dans la prochaine section plus en détail la méthodologie appliquée et discutons les limitations de notre recherche.

4.3 Méthodologie

4.3.1 Données collectées

Au début de septembre 2017, nous avons mené une enquête empirique sur la prise de décision de paiement en ligne, en prenant en considération la conception du site et la perception des utilisateurs envers les technologies de paiements. Pour collecter des données, nous avons lancé le questionnaire en ligne par l'intermédiaire de la plateforme **Amazon Mechanical Turk (*MTurk*)**[9]. Le sondage contenait un total de 57 questions, y compris cinq questions démographiques. Le temps moyen de réponse au sondage était de 12 minutes, ce qui rendait la rémunération conforme aux normes de paiement de la collectivité de *Mturk*. Tous les éléments du questionnaire utilisent l'échelle des Likert en 5 points, variant de fortement en désaccord (1) à fortement en accord (5), avec (3) comme pas de décision (voir un exemple d'une question dans la Figure 15). Les participants ont

[9] https://www.mturk.com/ consulté le 26/Oct./2019

choisi leur degré de désaccord ou d'accord selon une affirmation. Cette méthode de collecte de données permet le traitement statistique par des méthodes quantitatives. L'analyse de ces données suppose la construction des variables latentes, non observables directement, mais estimées à travers plusieurs variables manifestées.

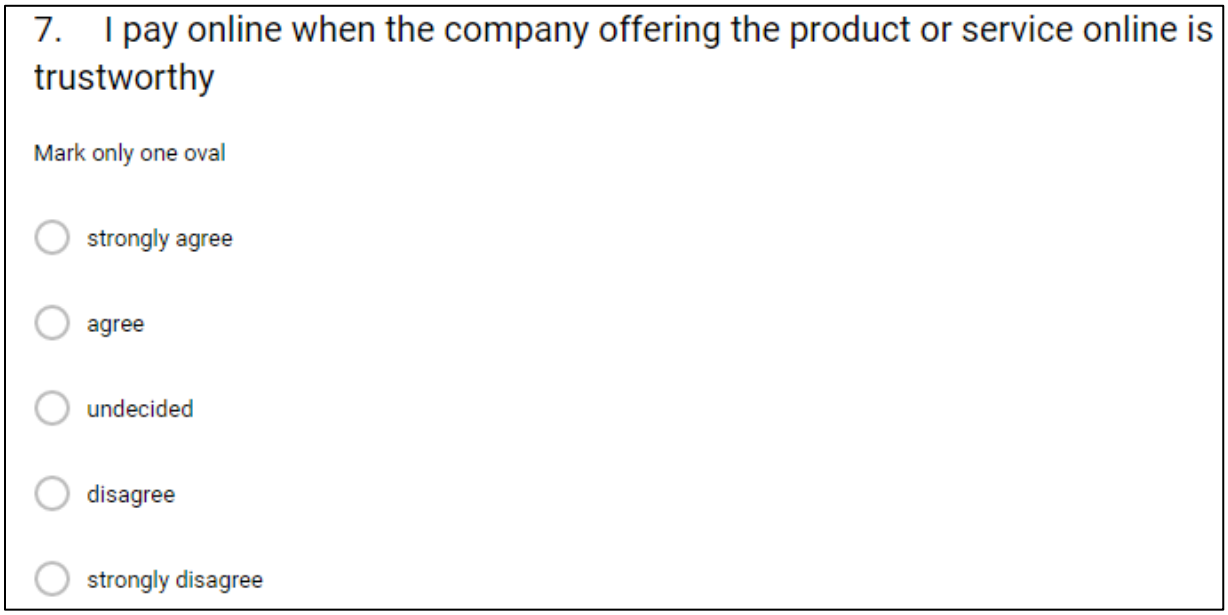

Figure 15 - Exemple de question

Nous avons établi les contraintes suivantes : localisation aux États-Unis ou au Canada, nombre de tâches où « Human Intelligence Task » (HITs) approuvés ou réalisés dans l'historique doit être supérieur à 100, taux d'approbation des HITs doit dépasser 95%. Par exemple, si un participant a complété 5000 HITs et son travail a été rejeté 250 fois, le taux d'approbation est de 95%[10]. Ces critères restreignent le nombre de participants admissibles à l'enquête et fournissent une sélection fondée sur les statistiques et l'historique des comptes de chaque répondant (Hara*, et al.*, 2017).

Les répondants ont fourni des renseignements démographiques, tels que le genre, l'âge, le niveau d'éducation, le revenu annuel et la profession, en plus d'autres renseignements comme le montant des dépenses mensuelles en ligne, le mode de paiement en ligne, la fréquence des achats en ligne, le prix des articles achetés en ligne (voir Tableau 2).

[10] https://blog.mturk.com/tutorial-understanding-requirements-and-qualifications-99a26069fba2 consulté le 26/Oct./2019

Tableau 2 - Données descriptives

Demographic Information	**Category**	**Total**	**%**
Gender	Male	179	45.7%
	Female	213	54.3%
Age	18-25	59	15.1%
	26-30	85	21.7%
	31-35	66	16.8%
	36-40	51	13.0%
	41-45	26	6.6%
	45-50	33	8.4%
	Above 50	71	18.1%
	I prefer not to answer	1	0.3%
Education	High School/college	0	0%
	Technical/trade school	112	28.6%
	Bachelor's degree	66	16.8%
	Master's degree	152	38.8%
	Doctoral degree	42	10.7%
	I prefer not to answer	10	2.6%
	Associate's Degree	2	0.5%
	Professional degree	5	1.3%
	Certificate and 3 years of college	1	0.3%
	Other	2	0.4%
Annual income (in cad $)	Less than 39,999	149	38.0%
	Between 40,000 and 64,999	90	23.0%
	Between 65,000 and 99,999	89	22.7%
	Between 100,000 and 119,999	23	5.9%
	Above 120,000	25	6.4%
	I prefer not to answer	16	4.0%
Occupation	Student	21	5.4%
	Employee	162	41.3%
	Professional	64	16.3%
	Business owner/Self-employed	50	12.8%
	Manager/official	23	5.9%
	Researcher	2	0.5%
	Homemaker	18	4.6%

	Retired	15	3.8%
	Unemployed	27	6.9%
	I prefer not to answer	7	1.8%
	Warehouse tech	1	0.3%
	Disabled	2	0.4%
Online monthly spending	Average less than 499 by month	322	82.1%
	Average between 500-1499 by month	59	15.1%
	Average between 1500-3499 by month	8	2.0%
	Other	3	0.8%
Online payment methods	Paypal	130	33.2%
	Cheque	1	0.2%
	Debit	109	27.8%
	Credit Card	148	37.8%
	Other	4	1.0%
Online shopping frequency	Once a month	91	23.2%
	More than once a month	301	76.8%
Online Item Price	Any amount	196	50.0%
	If amounts less than 250.0	153	39.0%
	If amounts less than 750.0	26	6.6%
	If amounts less than 1500.0	13	3.3%
	less than 20	1	0.3%
	less than 50	2	0.5%
	It depends on the specific item	1	0.3%
Personality Perception	I'm a pessimist. I always expect the worst	17	4.3%
	I'm anxious. No matter what you say, I'll worry	75	19.1%
	I'm cautious but open to new ideas. Convince me	116	29.6%
	I'm objective. Show me the pros and cons, and I can make a decision and live with it.	130	33.2%
	I'm optimistic. Things always work out in the end	54	13.8%
Risk Perception	Loss	102	26.0%
	Uncertainty	254	64.8%
	Thrill	4	1.0%
	Opportunity	32	8.2%

Deux questions ont été ajoutées pour expliquer selon leur point de vue la signification du mot « risque » et celle du concept de « personnalité ».

Au total, 399 participants ont répondu au questionnaire. Puisque notre intérêt est centré sur les participants qui magasinent en ligne, le sondage a commencé par la question suivante : « À quelle fréquence magasinez-vous en ligne ? » un participant a été retiré parce qu'il/elle n'a jamais fait d'achats en ligne, et six autres ont été retirés parce qu'ils avaient des réponses uniformes à un grand nombre de questions d'affilée, ce qui indique leur manque de sérieux. Par conséquent, seules les réponses des 392 autres participants (54,3 % de femmes, 45,7 % d'hommes) ont été prises en compte, ces derniers magasinent en ligne au moins une fois par mois (où 76,8 % ont déclaré faire des achats en ligne plus d'une fois par mois, voir le Tableau 2.)

4.3.2 Limitations de la recherche

La plateforme *Mturk* présente des limites qui ne peuvent être ignorées : Parmi ces limites, il existe celles qui sont communes à l'expérimentation en ligne : par exemple, la viabilité du lieu d'expérience ne peut pas être garantie, car il n'y a pas un moyen facile pour les expérimentateurs de contrôler exactement le cadre expérimental. Par exemple, il se peut que le participant réponde au questionnaire dans un milieu public (restaurant, café ou autre) ce qui aboutit à des distractions non négligeables dues à l'environnement physique. D'autres problèmes potentiels peuvent parvenir durant la participation et sont reliés à l'utilisation de différents types de navigateurs *(Internet Explorer, Mozilla Firefox ou Google Chrome)* tels que le temps de réponse, la facilité d'utilisation. De plus, l'absence de soutien physique aux participants durant l'activité est comptée parmi les limites à considérer lorsque le participant a besoin de clarifier une certaine question. Néanmoins, la plateforme peut fournir des résultats aussi pertinents que ceux des méthodes d'enquête traditionnelles (Kittur*, et al.*, 2008).

Après avoir examiné la méthodologie de notre enquête, la section suivante explique en détail l'analyse des données recueillies et met en évidence les résultats et la validation des hypothèses.

4.4 Résultats et validation

Cette section met en lumière les résultats et les constatations de notre recherche. Premièrement, la validité des données recueillies est évaluée, puis les hypothèses soulevées sont testées et validées.

4.4.1 Validité des construits et fiabilité

Pour analyser nos résultats, nous adoptons un logiciel de modélisation d'équations structurelles conçu par IBM qui est AMOS 25.0.0. Les modèles d'équations structurelles (*MES*) ont pour but de traiter statistiquement des relations de causalités hypothétiques multiples et permettent de prendre en compte des corrélations à tous les niveaux. Ils permettent également d'analyser simultanément les effets linéaires qui sont censés relier plusieurs variables latentes indépendantes et dépendantes (Kline, 2015; J. Wang & Wang, 2019). Selon (Hoyle, 1995), la modélisation par les équations structurelles représente «une approche statistique globale permettant de tester des hypothèses traitant des relations entre les variables observées et les variables latentes».

Pour ce faire, notre modèle englobe un ensemble de variables latentes (ou non observables) représentées dans le Tableau 3 par les construits : PS, SS, IQ, CT, PF, EU, PR et OP et des relations de causalité sous-jacentes qu'on appelle aussi relations cause-effet. Prenons l'exemple de la relation causale entre les deux construits « IQ » et « CT » qui s'exprime comme suit : l'amélioration de la Qualité des informations sur la page web (la cause) aura un impact sur la « confiance des clients » (l'effet). Pour tester les relations structurelles, nous estimons les voies de causalité hypothétiques et définissons l'hypothèse proposée pour évaluer si elle est appuyée ou non. Pour évaluer les résultats extraits des réponses des participants, nous examinons d'abord *la fiabilité, la moyenne, l'écart-type et l'interdépendance de chaque construit*. Les résultats, y compris la moyenne et l'écart-type (SD), sont présentés dans le Tableau 3. Le tableau comprend également les « factor loading », c'est-à-dire les coefficients de corrélation entre les différentes variables et construits qui nous permettent d'évaluer la validité du modèle de mesure en vérifiant que chacun des construits est bien rattaché au groupe de variables latentes.

Tableau 3 - Opérationnalisation des construits et des caractéristiques de mesure

Constructs	**Items**	**Loading**	**Mean**	**SD**
Website Information Quality (IQ)	IQ1. The website should provide accurate information about the product that I want to purchase (Kuan*, et al.*, 2008; Ponte*, et al.*, 2015).	0.819	4.66	0.631
	IQ2. The website should provide up-to-date information about the product that I want to purchase (Ponte*, et al.*, 2015).	0.771	4.64	0.594
	IQ3. The company offering the product in this e-commerce website should keep its promises and commitments	0.752	4.69	0.581
Website Security Signs (SS)	SS1. I feel secure when the online payment page shows me clear security signs	0.763	4.12	0.809
	SS2. I feel secure when the online payment page shows me clear privacy and/or security statement	0.866	3.98	0.873
	SS3. I feel secure when the online payment page shows me clear privacy and/or security policy	0.853	4.08	0.849
	SS4. I feel secure when the online payment page uses a secure connection	0.726	4.42	0.704
Website Ease of Use (EU)	EU1. When I purchase, the website should be easy to use/navigate	0.738	4.61	0.584
	EU2. The website should allow me to find what I wanted easily. The search is quick and simple.	0.792	4.52	0.602
	EU3. The website should be well designed	0.658	4.52	0.585
Customer Trust (CT)	CT1. I pay online when I know and trust the e-commerce website	0.808	4.62	0.565
	CT2. I pay online when the company offering the product or service online is trustworthy	0.792	4.61	0.561
	CT3. I pay online if the company behind the e-commerce website is well known	0.775	4.48	0.659
	CT4. I pay online if the company behind the e-commerce website has a good reputation	0.796	4.57	0.595
Perceived Payment Security (PS)	PS1. I feel secure when the online payment page asks me to register my login information using my fingerprint	0.514	3.37	1.144

	PS2. I feel secure when the online payment page requires from me to enter my credentials before final checkout	0.908	3.85	0.924
Perceived Financial Fear (PF)	PF1. I believe the misuse of my financial information affects my personal life	0.817	4.24	0.891
	PF2. I believe the misuse of my financial information affects my professional life	0.760	3.78	1.083
	PF3. I believe the misuse of my financial information leads me to have significant legal and financial problems	0.797	3.99	0.996
Privacy Concerns (PR)	PR1. I feel concerned about my privacy when paying online	0.909	3.62	1.063
	PR2. I feel concerned about my financial loss when paying online	0.774	3.32	1.147
	PR3. I believe that my personal and financial information I provide when I pay is sensitive.	0.398	4.35	0.763
Online Payment (OP)	OP1. My friends and family did not report an unpleasant experience with the website, so I began to trust the site with my personal information.	0.657	3.69	0.944
	OP2. I pay online if I do not have any unpleasant experience reported by my friends and/or family	0.780	3.91	0.829
Website Visual Appearance (VA)	VA1. The website displays should provide a high level of artistic sophistication/creativity	N/A	N/A	N/A
	VA2. If the website looks “cheap,” it makes me feel not safe shopping there, and I ignore it	N/A	N/A	N/A
	VA3. The visual appearance and design of the website should be professional (not amateur-looking)	N/A	N/A	N/A

La première étape consiste en une analyse factorielle confirmatoire (*Confirmatory Factor Analysis ou CFA*) qui permet de tester les hypothèses émises dans la partie théorique. Les CFA permettent de tester formellement des hypothèses de liens et dépendances multiples entre variables, sans recourir nécessairement à des relations de type causal écrites sous forme de régression. Ils permettent également de valider la structure du modèle en définissant de façon formelle les variables latentes PS, SS, IQ, CT, PF, EU, PR, et OP. Dans le Tableau 4, nous présentons les indicateurs d’ajustement du modèle et les

résultats du test d'aptitude du modèle structurel. La vérification de l'ajustement du modèle de structure vient après l'acceptation du modèle de mesures et suit la même logique que la sienne. Sept mesures communes d'ajustement du modèle sont utilisées pour estimer le modèle de mesure adaptée : (1) chi-carré/degré de liberté (chi2/df) (2) indice de qualité de l'ajustement (GFI) (3) indice de qualité de l'ajustement (AGFI) (4) indice d'ajustement comparatif (CFI) (5) indice d'ajustement normé (NFI) (6) racine moyenne résiduelle carrée (RMR) et (7) erreur carrée moyenne racine d'approximation (RMSEA). Certaines de ces valeurs étaient légèrement différentes des valeurs recommandées. Ces valeurs indiquent une aptitude acceptable du modèle par rapport aux valeurs recommandées selon (Hair*, et al.*, 1998). Par conséquent, nous pouvons conclure que le modèle de mesure est bien adapté aux données recueillies.

Tableau 4 - Valeurs des indices d'ajustement du modèle de structure

	chi²/df	**GFI**	**AGFI**	**CFI**	**NFI**	**RMR**	**RMSEA**
CFA	3.066	0.858	0.822	0.881	0.834	0.069	0.073
SM	2.256	0.904	0.871	0.933	0.887	0.039	0.057

L'approche de Fornell et Larcker (Fornell & Larcker, 1981) a été adoptée pour l'évaluation de la validité convergente et discriminante du modèle de mesure. Selon leur méthode, la validité convergente indique la variance commune entre les indicateurs et leurs structures. Elle signifie que les items doivent partager plus de variables latentes avec leur construit qu'avec leurs erreurs de mesure. En effet, ils proposent trois indices à calculer pour l'analyse de la validité convergente des échelles de mesure soit : les contributions factorielles (CF), le coefficient de fiabilité composite (CR) et la moyenne de la variance extraite (AVE) associée à chaque variable latente et le maximum de variance partagée (MSV) qui sert à évaluer le résultat de (AVE). En suivant cette méthode, les résultats indiquent une corrélation significative entre tous les construits tels que présentés dans le Tableau 5. Ils sont également valides puisque la statistique (AVE) dépasse largement le seuil de 0,50 pour l'ensemble des construits du modèle. De plus, toutes les variables du modèle de mesure ont enregistré des valeurs d'AVE considérablement supérieures à la (MSV). Le coefficient Alpha de Cronbach, présenté dans le Tableau 5, permet de vérifier la cohérence interne d'un construit, avec les corrélations entre les huit construits (PS, SS,

IQ, CT, PF, EU, PR, et OP). Ce dernier montre également que les réponses obtenues sont cohérentes avec l'ensemble des énoncés mesurant le même concept (Chauvet, 2003). Selon Nunally (1978), le coefficient Alpha de Cronbach est considéré comme acceptable dépassant le 0.60 pour tous les construits. Ce qui est valide dans notre cas.

Tableau 5 - Validité convergente du modèle de mesure

Construct	CR	AVE	MSV	Cronbach's Alpha	PS	SS	IQ	CT	PF	EU	PR	OP
PS	0.689	0.544	0.296	0.626	**0.738**							
SS	0.879	0.647	0.296	0.877	0.544	**0.804**						
IQ	0.824	0.610	0.464	0.823	0.174	0.343	**0.781**					
CT	0.871	0.629	0.315	0.869	0.289	0.422	0.546	**0.793**				
PF	0.834	0.627	0.118	0.829	0.275	0.218	0.293	0.320	**0.792**			
EU	0.774	0.535	0.464	0.774	0.279	0.310	0.681	0.561	0.278	**0.731**		
PR	0.754	0.528	0.118	0.721	0.014	-0.038	0.038	0.113	0.344	0.161	**0.727**	
OP	0.683	0.520	0.118	0.674	0.336	0.269	0.258	0.340	0.235	0.343	-0.070	**0.721**

En plus de l'extraction des valeurs du modèle structurel, une validation des hypothèses est nécessaire pour vérifier l'impact de chaque facteur sur la décision de paiement en ligne. Par conséquent, la prochaine section présente la vérification des hypothèses.

4.4.2 Test des hypothèses

Pour tester nos hypothèses, nous utilisons les « modèles d'équations structurelles » (*Structural Equation Modelling ou SEM*) qui étudient les relations complexes entre les variables. Comme décrit dans notre méthodologie, notre modèle englobe un ensemble de variables latentes (ou non observables) PS, SS, IQ, CT, PF, EU, PR et OP et des relations de causalité sous-jacentes qu'on appelle aussi relations cause-effet. Les modèles d'équations structurelles nous permettent de quantifier les relations causales décrites dans le modèle théorique représenté dans la Figure 14 et d'analyser la validité de nos variables latentes. La signification des liens de causalité permet la validation des hypothèses de recherche que nous avons définies. Prenons l'exemple de la relation causale entre les deux construits « SS » et « PS » qui s'exprime comme suit : l'amélioration des signes de sécurité

sur la page web (la cause) aura un impact sur la «perception de la sécurité des paiements» (l'effet). Le modèle causal permet de tester la significativité et l'intensité des liens de causalité entre les variables latentes. Les hypothèses de recherche sont vérifiées grâce à l'examen du Critical Ratio (C.R.), ainsi qu'à la vérification des niveaux de probabilité pour chacun des liens de causalité. Pour ce faire, nous déterminons pour chaque hypothèse le Critical Ratio (C.R.) et le niveau de probabilité (P) qui nous permet de nous prononcer sur sa validation. Les résultats figurent sur le modèle structurel tel que montré dans la Figure 16 et appuient les facteurs influents sur la prise de décision dans les paiements en ligne.

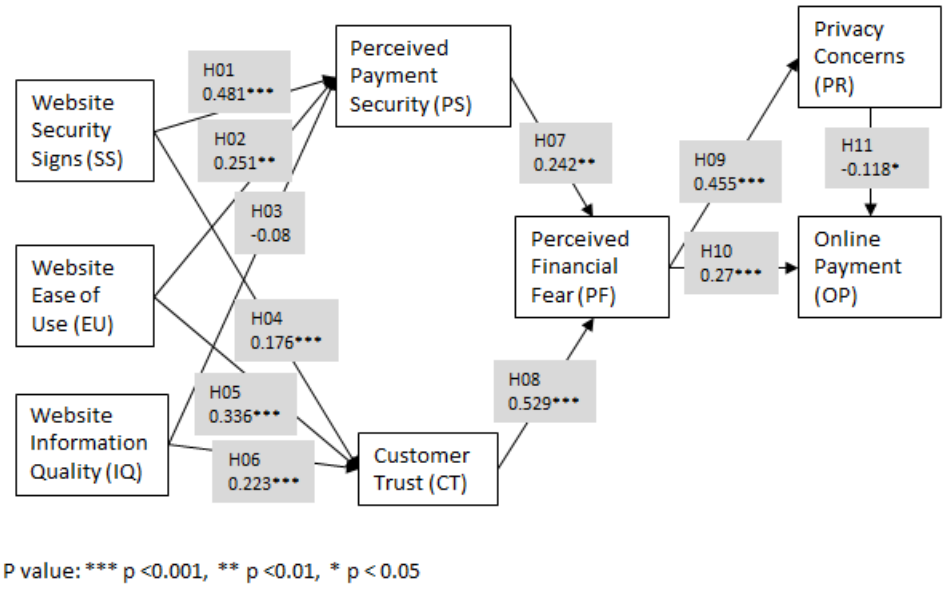

Figure 16 - Le résultat du modèle structurel

Par ailleurs, ces résultats figurent dans le Tableau 6 avec les estimations des paramètres (Estimate), les erreurs-types (S.E). Tous ces résultats permettent de vérifier la significativité et l'importance des liens de causalité entre les qualités du site Web, à savoir la *facilité d'utilisation*, *les signes de sécurité* et *la qualité de l'information*, *la prise de décision de payer en ligne et la perception de la protection de vie privée* dans le but de valider les hypothèses de recherche.

Comme déjà mentionné, notre modèle propose onze hypothèses. L'analyse du modèle en fonction des hypothèses élaborées et la discussion des résultats sont présentées dans la section suivante.

Tableau 6 - Résultats des liens de causalité et validation des hypothèses de recherche

Hypothesis	**Path**	**Estimate**	**S.E.**	**C.R.**	**P**	**Supported?**
H01	Website Security Signs → Perceived Payment Security	0.481	0.091	5.31	***	Yes
H02	Website Ease of Use → Perceived Payment Security	0.251	0.084	2.981	0.003	Yes
H03	**Website Information Quality → Perceived Payment Security**	**-0.08**	**0.058**	**-1.376**	**0.169**	**No**
H04	Website Security Signs → Customer Trust	0.176	0.035	5.105	***	Yes
H05	Website Ease of Use → Customer Trust	0.336	0.057	5.949	***	Yes
H06	Website Information Quality → Customer Trust	0.223	0.041	5.392	***	Yes
H07	Perceived Payment Security → Perceived Financial Fear	0.242	0.076	3.194	0.001	Yes
H08	Customer Trust → Perceived Financial Fear	0.529	0.116	4.572	***	Yes
H09	Perceived Financial Fear → Privacy Concerns	0.455	0.08	5.69	***	Yes
H10	Perceived Financial Fear → Online Payment	0.270	0.069	3.911	***	Yes
H11	Privacy Concerns → Online Payment	-0.118	0.046	-2.549	0.011	Yes

4.5 Discussion

Dans cette recherche, notre objectif est de concevoir un modèle de recherche qui explique les facteurs qui contribuent à une décision de paiement en ligne. D'après les résultats

illustrés dans le Tableau 6, la seule hypothèse non étayée est **H03** (p=0.169). En fait, la *qualité de l'information* du site Web n'a aucune incidence sur la *perception de la sécurité* des paiements, par contre elle favorise la *confiance* des clients **(H06)**. De plus, il est important de noter l'effet de la *confiance* des clients sur la *perception de la crainte de perte financière* **(H08)**, qui est en fait l'objet principal et la contribution de notre travail.

Conformément aux recherches antérieures qui étudient l'effet des signes de sécurité du site Web, les éléments probants de cette recherche appuient empiriquement le modèle proposé. En effet, notre recherche souligne le fait que la clarté des signes de sécurité, des politiques de sécurité et des déclarations de confidentialité dans une page de paiement a un impact positif sur la *perception de la sécurité des paiements*. Par conséquent, l'hypothèse **H01** est validée. Ceci dit, les clients ont besoin de se trouver en sécurité lorsqu'ils effectuent des transactions financières. Par exemple, une navigation par l'intermédiaire d'une connexion non sécurisée, indiquant HTTP au lieu de HTTPS influe négativement sur la sécurité de la transaction. Lors du paiement en ligne, il faut donc vérifier que l'URL dans la barre d'adresse soit la suivante : https://... Le "s" ajouté au HTTP habituel signifie "sécurité", de plus le symbole d'un cadenas fermé doit aussi apparaitre dans la barre d'adresse du site Web. Si c'est le cas, les données personnelles sont transmises en toute sécurité.

Ces mêmes facteurs favorisent la *confiance* du client comme indiqué dans l'hypothèse **H04.** Des études antécédentes ont conclu que les déclarations de confidentialité et les signes de sécurité (comme les symboles de cadenas) ont des effets à la fois sur la confiance et la méfiance (Seckler*, et al.*, 2015).

De plus, les résultats aident à interpréter l'effet de la *qualité de l'information*, y compris les renseignements exacts et mis à jour, sur la *confiance* envers le site. Cette caractéristique du site renforce la *confiance* du client et implique une relation significative. Il en ressort que l'hypothèse **H06** est validée. D'ailleurs, si Bob visite un site Web et qu'il détecte que la dernière mise à jour date depuis 2013. Il est évident qu'il va se demander : est-ce que le site n'a pas été mis à jour depuis plus de six ans? Est-ce qu'il peut faire confiance à ce qu'il lit sur la page ? En d'autres termes, pour accroître la confiance de Bob, le site doit mettre à jour continuellement ses informations afin de fournir un contenu fiable

et adéquat. Il doit montrer aussi des dates de mise à jour récentes même si l'information présentée porte sur un évènement déjà passé. Ceci fait référence au client qui procède à l'évaluation de l'excellence de fournisseur, du service en confrontant ses attentes en matière de services, et à la performance effective de ces services (Parasuraman*, et al.*, 1988). Ces résultats sont conformes aux résultats des recherches antérieures qui ont montré que la *qualité du service* est le principal facteur influençant la *confiance* des clients et favorisant leur fidélité envers les détaillants (Andrade*, et al.*, 2012; Chang & Fang, 2013; Nadeem*, et al.*, 2015). Ce qui parait intéressant est que le niveau d'effet de la *qualité de l'information* du site Web sur *la perception de la sécurité* des paiements n'est pas assez important. Par conséquent, sur la base des résultats, l'hypothèse **H03** n'est pas supportée (p=0.169). Par exemple, dans l'éventualité de faire un paiement en ligne, Bob se préoccupe plus des signes de sécurité que des informations affichées sur la page de paiement.

En outre, les résultats prouvent que la *facilité d'utilisation* du site révèle un facteur critique influant la *perception de la sécurité* des paiements. Une fois que le client ressent une *facilité d'utilisation* importante durant la navigation sur la page Web, ceci aura un impact positif sur sa *perception de la sécurité*, tel que montré dans l'hypothèse **H02**. Par exemple, face à un site où la navigation est difficile ou compliquée, Bob va trouver que l'application Web est mal construite, incompréhensible, voire carrément inutile, puisqu'elle contient de nombreuses failles de fonctionnement. Par conséquent, Bob va se questionner sur la sécurité du site. La difficulté de navigation se manifeste dans le site Web par la barre de menu mal organisée, l'absence d'une barre de recherche, les liens éparpillés partout dans les pages (la plupart devraient se trouver en bas de page), et les coordonnées du vendeur difficiles à trouver. En effet, cette dernière est la probabilité avec laquelle un consommateur croit que ses informations privées ne vont pas être vues, emmagasinées ou manipulées durant le transfert et le stockage des données, par des parties inappropriées (Pavlou, 2001).

L'effet de la *facilité d'utilisation* sur la *confiance* du client est expliqué par l'hypothèse **H05.** Ce résultat confirme des observations mentionnées précédemment concernant la facilité de navigation sur le site à savoir qu'elle n'affecte que la confiance, mais pas la méfiance (Seckler*, et al.*, 2015). En d'autres termes, l'amélioration du site au

niveau de la facilité d'utilisation favorise la confiance du client. Par contre, si Bob n'a pas une confiance envers le site, la facilité d'utilisation ne va pas le rendre confiant. Cette caractéristique du site Web se manifeste quand Bob se connecte à la page pour conclure son paiement. Il doit comprendre clairement ce qu'il peut faire comme prochaines étapes ou bien il doit savoir quelles sont les actions à prendre pour atteindre son but. Donc, la navigation doit être claire et non compliquée afin de ne pas rendre l'utilisateur plus confus.

En ce qui concerne la *perception de la crainte d'une perte financière*, nous extrayons un résultat significatif sur les préoccupations relatives à la vie privée à l'appui de l'hypothèse **H09** en révélant une relation hypothétique importante. Compte tenu de l'importance de la *perception de la crainte d'une perte financière*, on peut conclure qu'une telle perception accrue se traduit par une meilleure perception des préoccupations en matière de protection de la vie privée. La crainte d'une atteinte à la vie privée implique une surveillance de près des comptes susceptibles d'être touchés, surtout si l'atteinte concerne des renseignements de nature sensible comme des renseignements financiers. Dans ce cas, Bob va chercher à protéger ses comptes auprès de l'institution financière s'il croit que ses comptes ont pu être compromis.

De plus, nos constatations soulignent l'importance de la *confiance* du client envers la *perception de la crainte d'une perte financière*, comme l'indique l'hypothèse **H08**. Ces résultats sont conformes aux résultats de (K. Martin, 2018; Mou*, et al.*, 2017).

L'hypothèse **H07** stipule que la *perception de la sécurité des paiements* influence de manière positive la *perception de la crainte de perte financière*. Les résultats montrent un effet significatif. Un environnement en ligne sécurisé réduit la vulnérabilité, protège les données pendant la transmission sur le réseau externe et évite que les cybercriminels soient à l'affut des faiblesses dans le site. Par conséquent, Bob ne cherchera pas à appliquer des mesures pour atténuer les risques associés aux fraudes. Par contre, il tentera de continuer le paiement sans prendre des préventions contre les menaces en ligne.

Dans le même contexte, il existe une corrélation modérée entre la *perception de la crainte de perte financière* et la *prise de décision* de paiement en ligne, qui apparait dans le lien structurel validé de **H10**. Les résultats du lien entre ces variables sont significatifs.

Ceci s'explique par le fait que si Bob est dans la quiétude de continuer la transaction, il va décider de payer.

Pour l'hypothèse **H09,** nous avons prédit que la *perception de la crainte de perte financière* a un effet positif sur les *préoccupations relatives à la vie privée*. Les résultats du lien entre ces variables sont significatifs. En effet, si Bob est conscient des risques en cas de fraudes, il commencera à s'intéresser également à la préservation de sa vie privée afin de minimiser les risques de perte ou de vol de ses informations.

Nous avons émis dans l'hypothèse **H11** que les *préoccupations relatives à la protection de la vie privée* ont un effet positif sur la *décision de paiement en ligne.* En effet*,* la relation causale, telle que validée par la valeur du lien structurel**,** montre que les *préoccupations relatives à la protection de la vie privée* ont un effet négatif sur la *décision de paiement en ligne*. Cette relation indique que si Bob se préoccupe plus de la préservation de sa vie privée en ligne, il va éviter les paiements en ligne et choisir éventuellement une autre méthode de paiement.

En fonction des résultats, notre modèle renforce la présence continue de *la perception de la crainte de perte financière* dans le commerce électronique. Il souligne aussi clairement le rôle de la relation de *confiance* avec le vendeur en ligne. Dans l'ensemble, les résultats montrent que notre modèle de recherche démontre de solides valeurs prédictives et explique la prise de décision de paiement en ligne.

4.6 Conclusion

Malgré la prolifération des sites de magasinage en ligne et les améliorations technologiques, les paiements en ligne font toujours face à une préoccupation considérable concernant la *confiance et le risque perçu* et leurs relations avec les *craintes* des utilisateurs en ligne. Ce travail permet de mettre en relief un modèle de recherche qui définit divers facteurs qui influencent la prise de décision du client en matière de paiement en ligne. En outre, nous avons développé et validé onze hypothèses qui explorent la relation de confiance des clients avec les caractéristiques du site Web, ce qui implique que la f*acilité d'utilisation, la qualité de l'information et les signes de sécurité* affectent la **confiance** en ligne et la **perception de la sécurité des paiements**. Enfin, une autre contribution dans

cette recherche réside dans la distinction établie entre deux types de perception : **la perception de la sécurité des paiements** et la **perception de la crainte d'une perte financière** (El Haddad, Aïmeur*, et al.*, 2018).

Dans le cadre des travaux futurs, nous nous efforcerons d'examiner plus en détail comment d'autres attributs du site Web, comme l'absence d'erreurs et l'apparence visuelle, influent sur les craintes des clients à effectuer des paiements en ligne. La présence d'erreurs comprend l'affichage des liens introuvables ou inactifs, les messages d'erreurs inattendus lors de navigation, et la lenteur de chargement de la page. En ce qui concerne l'apparence visuelle, nous pourrions considérer l'attraction esthétique du site Web, l'affichage des blocs de texte et les éléments visuels tels que les images et les couleurs.

Chapitre 5 : Une nouvelle plateforme de paiement en ligne

Au cours des deux dernières décennies, le développement de solutions de paiement en ligne a considérablement permis la simplification des tâches des vendeurs, l'amélioration des expériences des clients, et la fluidification des échanges. Dans cette optique, le monde numérique a élargi la portée de nombreuses technologies de paiement offertes sur le marché. Malgré la multitude de solutions de paiement, les systèmes de cartes bancaires demeurent les plus répandus. Bien qu'ils soient sécurisés, les systèmes fondés sur les cartes n'assurent pas la protection de la vie privée, et ne donnent pas à l'utilisateur ni le contrôle ni la supervision de ses paiements par carte. D'ailleurs, une estimation provenant du rapport de Nilson[11] prédit que le total des fraudes par cartes va dépasser 35 milliards de dollars en 2020.

Par ailleurs, les ventes en ligne continuent à croître d'une façon exponentielle. À ce sujet, il y a eu une augmentation considérable des ventes en ligne de **1,34 billion en 2014** à **1,86 billion en 2018**, et estimé d'atteindre **4,87 billions en 2021**, d'après **emarketer**[12]. Cette croissance dans l'ère du commerce électronique attire l'attention des chercheurs et pousse à réaliser des travaux académiques dans le domaine des paiements en ligne. Ceci dit, nous proposons dans la présente étude **une nouvelle plateforme de paiement électronique** fondée sur les systèmes de paiement par carte, qui considère l'agrégation des cartes de crédit virtuelles et la notion de paiement électronique conditionnel personnalisé défini par le détenteur de la carte lui-même.

Dans notre solution proposée, la confidentialité du titulaire de carte est assurée par l'utilisation de cartes de crédit virtuelles. De plus, avec le service du plan de paiement électronique (***E-Payment Plan Service Manager ou E-PPSM***), notre système présenté apporte des améliorations considérables à la pratique d'achat. En effet, par l'intermédiaire de ce système, les titulaires de cartes peuvent contrôler et superviser efficacement leurs

[11] https://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.Vch_sPlViko consulté le 24/sep/2019

[12] https://www.emarketer.com/content/amazon-only-shoppers-on-the-rise?ecid=NL1014 consulté le 24/sep/2019

achats en ligne. De plus, le système proposé est applicable dans les scénarios d'achats multiples et assure trois contributions: **personnalisation, contrôle et supervision**. Celles-ci constituent, en plus de la protection de la vie privée, nos principales contributions.

Dans les sections suivantes, nous donnons un aperçu des systèmes de paiement ainsi que de leurs différents défis. Ensuite, nous proposons une nouvelle plateforme de paiement électronique en décrivant les composants. Enfin, nous expliquons nos principales contributions tout en fournissant une analyse des propriétés de la plateforme.

5.1 Processus du Paiement en ligne

Nous présentons, dans cette section, un aperçu des systèmes de paiement ainsi que de leurs défis.

5.1.1 Systèmes de paiement

Depuis quelques décennies, le marché de paiement a noté une croissance rapide en raison de l'augmentation des systèmes de paiement électronique. Plusieurs solutions de paiement ont été déployées : *le virement bancaire, les cartes de crédit bancaires, les téléphones mobiles, les porte-monnaie électroniques, les cartes prépayées*. Les systèmes de porte-monnaie électroniques ont élevé le degré de protection des renseignements personnels si bien que même la police est parfois incapable d'associer le paiement avec le payant, tout comme pour les paiements en espèces dans le monde physique (Cellary & Rykowski, 2015).

Dans le contexte des cartes de crédit, des innovations considérables sont apparues dans le commerce électronique afin d'intégrer cette méthode dans l'implémentation des systèmes de paiement. Par conséquent, les grandes entreprises, comme WeChat, PayPal et Google Wallet, investissent des efforts remarquables pour créer et offrir des solutions de paiement en ligne. Les environnements mobiles ont également subi des améliorations dans les domaines des solutions de paiement avec Apple Pay (Gray, 2015). Dans les intégrations avec les cartes, les entreprises agissent comme intermédiaires. D'un point de vue conceptuel, la participation des intermédiaires a un impact sur la protection de la vie privée des clients, car ils sont en mesure d'accéder aux informations sensibles de paiement qui

peuvent être utilisées pour construire un profil détaillé du client (Preibusch*, et al.*, 2015). Ainsi, une telle exposition de données personnelles et financières sur Internet donne lieu à un certain nombre de défis de protection des renseignements personnels pertinents (Carminati*, et al.*, 2016; Pascual-Miguel*, et al.*, 2015), en plus du manque de personnalisation et de flexibilité dans les systèmes de paiement par carte qui doivent être également abordés.

Par ailleurs, il existe des tentatives pour fournir des systèmes de paiement anonymes tout en intégrant la carte de crédit virtuelle dans les mécanismes de paiement (Luo*, et al.*, 2016), et ce, dans le but d'atténuer les fraudes en raison de vols de cartes. Une autre approche, concernant la protection des renseignements personnels, consiste à mettre en place un modèle de paiement qui garantit l'authenticité tout en gardant les informations sensibles du client à l'abri des différentes entités qui sont impliquées dans la transaction en ligne (Ashrafi & Ng, 2009).

À cet égard, nous visons à fournir une nouvelle plateforme de paiement, configurable et contrôlable qui protège également la vie privée des clients.

5.1.2 Systèmes de paiement à base de cartes

Ces dernières années, le commerce électronique est devenu un domaine d'activité important pour la négociation, la distribution et la vente de produits entre les entreprises *(B2B)*, les entreprises et les consommateurs *(B2C)* et entre les consommateurs eux-mêmes *(C2C)*. Les systèmes à base de cartes constituent notre objectif. Ils sont fondés sur les modèles d'affaires traditionnels à deux entités : un client (titulaire) et un marchand (fournisseur de produit/service) (Ashrafi & Ng, 2009). Les méthodes de paiement dans ces systèmes représentent une forme particulière du commerce électronique, généralement appelée transactions avec **Cartes Non Présentes** *(CNP)*. Cela signifie que les transactions sont initiées par les clients à partir du site Web du marchand, par conséquent les informations de la carte sont fournies sur la page de paiement sans la machine de paiement et sans que la carte soit présentée physiquement au marchand. En effet, malgré leur sécurité, les systèmes basés sur les cartes sont encore loin de pouvoir protéger la vie privée, du contrôle et de supervision. En fait, ces systèmes ne fournissent pas un environnement

de paiement qui empêche le vendeur ou un utilisateur malveillant d'abuser des informations envers le détenteur de la carte (Dixon & Pinckney, 2013). Le marchand peut toujours contrôler les champs de données qui sont utilisés pour autoriser le paiement, même s'il ne peut pas vérifier physiquement que le client a utilisé une carte de débit ou de crédit. En conséquence, les transactions échangées avec le marchand généralement incluent des informations sensibles (**financières et non financières**) des clients. Les informations financières se réfèrent à des détails de paiement. Les informations non financières comprennent *les produits achetés, leur modèle, leur prix*.

Généralement, les clients doivent fournir les informations de la carte après chaque achat : *le numéro et le type de carte de crédit, la date d'expiration et le numéro de vérification*. Ces informations sont alors transmises aux diverses entités qui procèdent à la demande du paiement pour autoriser ou rejeter la transaction. Toutefois, le processus de paiement à base de cartes ne tient pas compte des propriétés suivantes : personnalisation, contrôle de paiements tout en respectant la gestion d'achats multiples.

Pour mieux mettre en évidence ces attributs, nous considérons le scénario suivant : dans une entreprise de vente en détail, Bob, responsable des achats, veut fournir des cartes de crédit à ses employés pour effectuer des achats en ligne pour leur département. Il doit décider de la limite de crédit de chaque carte et doit donner des instructions concernant les conditions d'achat en ligne, telles que la liste des marchands, le type d'achats, les dépenses, la marge de prix, etc. De façon périodique, Bob reçoit des relevés de compte. Pour accomplir cette tâche, il doit vérifier chaque paiement, le classifier avec les autres achats de même type et s'assurer que c'est conforme aux instructions avant de comptabiliser les factures. Ceci dit, il ne peut pas spécifier les marchands qu'il veut autoriser, ni définir les limites de chaque dépense, ni même spécifier les caractéristiques des produits à acheter en ligne. En effet, Bob ne peut pas restreindre la liste des marchands : Best Buy, Staples, Amazon. Il ne peut pas spécifier 500$ pour Best Buy, 750$ pour Staples et 1300$ pour Amazon. De même, il ne peut pas préciser quels types d'imprimantes choisir Lazer, Inkjet ou 3D ni quelle marge de prix (entre 100$ et 300$). Par conséquent, les systèmes actuels de paiement par carte reculent en termes de protection de vie privée, de contrôle et de supervision dans un scénario d'achats multiples. À noter que ce scénario peut être

facilement étendu à d'autres cas, y compris les parents qui fournissent des cartes de crédit à leurs enfants.

Dans ce travail, nous proposons un nouveau système de paiement en ligne basé sur le travail de **Martínez Ruiz *et al.*** (Ruiz-Martínez*, et al.*, 2012). Ce dernier a fourni une approche générale, fondée sur un ensemble de composants génériques qui aident à la mise en application des systèmes de paiement dans un but de négociation et de sélection du protocole de paiement. En résumé, nous présentons une amélioration du système tout en ajoutant de nouvelles partitions afin d'assurer d'une part la protection de la vie privée et d'autre part la personnalisation de service pour l'utilisateur, la protection des données, la supervision et le contrôle sur les paiements. Cette amélioration contribue à l'amélioration du déroulement de la transaction en ligne. De plus, notre système supporte des scénarios d'achats multiples ainsi que le paiement conditionnel.

5.2 E-PPSM système conditionnel avec achats multiples

Dans cette section, nous effectuons une description détaillée de notre nouvelle plateforme de paiement **(E-payment Plan Service Manager ou *E-PPSM***). Comme illustré dans la Figure 17, notre plateforme est détaillée en deux partitions, soit l'espace du titulaire de carte (***Cardholder Space***) et l'espace du service du plan du paiement électronique (***E-PPSM***). Chaque partition contient des sous-partitions et des composants listés dans le Tableau 7.

À noter que les mécanismes de transport/sécurité représentent la communication qui permet d'échanger des renseignements sensibles. Dans cette partie, il est primordial de choisir un protocole garantissant un échange sécurisé d'informations, comme le protocole Transport Layer Security (*TLS*) (Turner, 2014).

Tableau 7 - Partitions de la plateforme (E-PPSM)

Partition	Sous-partition	Composant
Espace du titulaire de carte (*Cardholder Space)*		Carte de Crédit (Credit Card)
		Système de paiement par carte de crédit (CC Payment System ou CCPS)
	Génération de carte de crédit virtuelle (VCC Generation)	Carte de Crédit virtuelle (Virtual Credit Card ou VCC)
		Personnalisation (*Personalization*)
		Conditions privées et publiques (*Private/Public Conditions*)
Espace du service du plan de paiement électronique (E-Payment Plan Service Manager ou E-PPSM)	Espace usager (User Space)	Système de Paiement par Carte de Crédit Virtuelle (VCC Payment System)
		Carte de crédit virtuelle (*Virtual Credit Card* ou *VCC*)
		Personnalisation (*Personalization*)
		Conditions privées et publiques (*Private/Public Conditions*)
	Moteur de paiement conditionnel (Payment Conditional Engine ou PC Engine)	Conditions Publiques (Public Conditions)
		Évaluation et vérification (Evaluation and Verification)
		Système de paiement automatisé (Automated Teller Payment)
	Espace Commerçant (Merchant Space)	Applications Web (Web Application)
		API Web paiement (Payment Web API)
		Méthodes de paiement (Payment Instruments)
		Mécanismes de négociation (Negotiation Mechanisms)

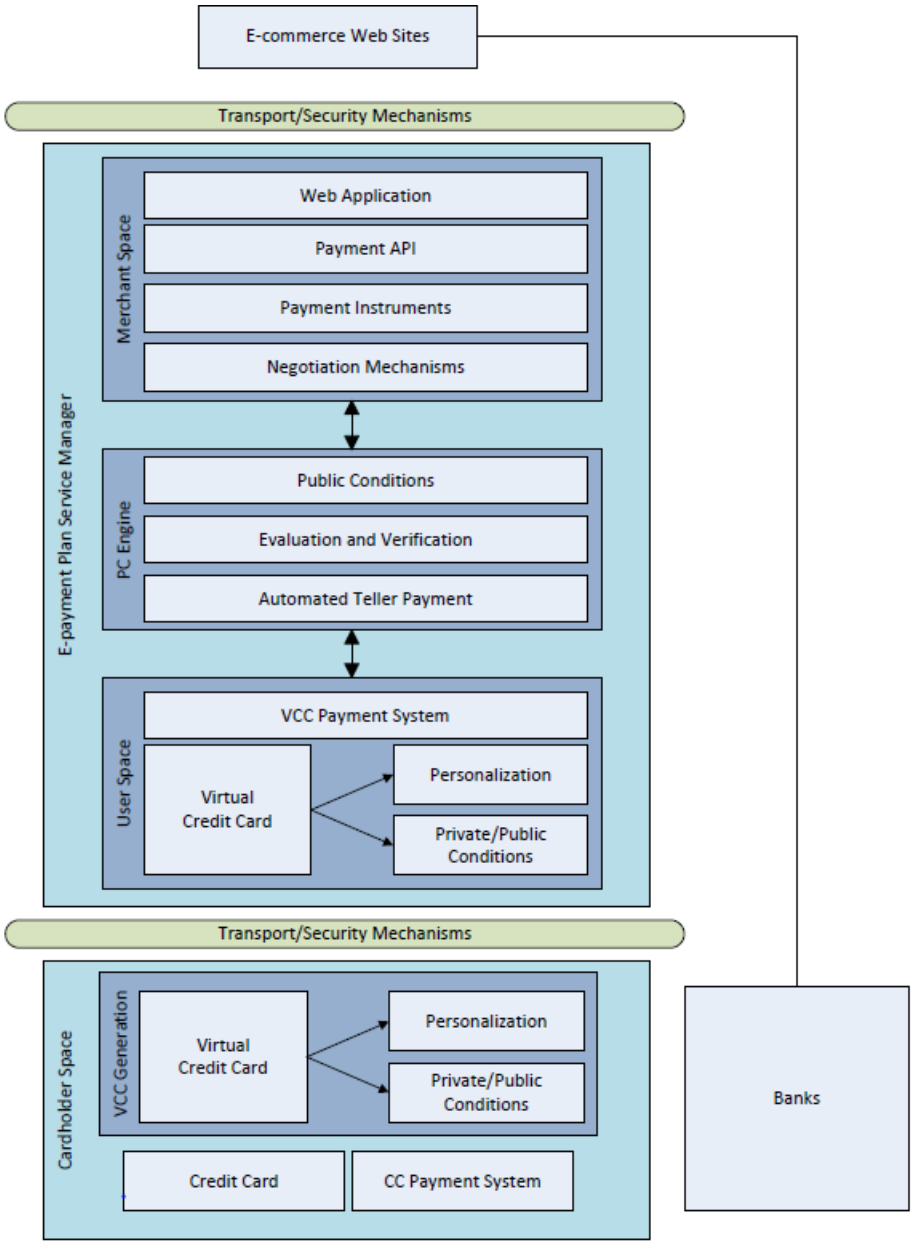

Figure 17 - Nouvelle plateforme de paiement (*E-PPSM*)

5.3 Espace du titulaire de carte (*Cardholder Space*)

L'espace du titulaire de carte reflète deux composants fondamentaux qui appuient le système proposé en tant que système de paiement : la **Carte de Crédit** (*Credit Card*) et le **Système de paiement par carte de crédit** (*Credit Card Payment System ou CCPS*). La **Génération de cartes de crédit virtuelles (***VCC Generation*) est une sous-partition qui, à la fois, fournit un système de paiement électronique de protection de vie privée et garantit

l'authenticité tout en préservant les informations financières et non financières du détenteur de la carte. Elle contient la carte de crédit virtuelle y compris la personnalisation et les conditions privées/publiques que nous expliquerons en détail plus tard.

5.3.1 Carte de crédit

La **Carte de crédit** contient les renseignements du détenteur de la carte de crédit et de la banque émettrice. Contrairement au système de paiement par carte traditionnel, dans notre plateforme de paiement, les renseignements financiers et non financiers du détenteur de carte ne sont pas divulgués au commerçant, ce qui empêche un commerçant de les utiliser à mauvais escient ou d'effectuer des transactions frauduleuses

5.3.2 Système de paiement avec carte de crédit

En général, ce système s'occupe du transfert de fonds entre le payeur et le bénéficiaire. Le montant du paiement est débité de la banque émettrice du titulaire de la carte et déposé dans le compte du marchand à la banque acquéreuse. Dans notre plateforme de paiement, le règlement du processus de paiement n'exige pas la divulgation de renseignements financiers et non financiers du détenteur de la carte. Une fonctionnalité pour le processus de paiement multiple est nécessaire pour soutenir les achats multiples.

5.3.3 Génération de cartes de crédit virtuelle

La **génération de carte de crédit virtuelle** (***VCC Generation***) représente une sous-partition principale de notre plateforme. Celle-ci génère les détails nécessaires pour l'inscription, l'identification et l'authentification des utilisateurs qui effectuent les transactions en ligne en plus de leurs plans de paiement. Dans cette sous-partition, les titulaires de cartes peuvent 1) générer une carte liée à leur carte de crédit physique, 2) désigner différents utilisateurs et 3) leur attribuer un nouveau *VCC* plan. Par exemple, Bob possède une carte de crédit avec le numéro suivant : 5646780479A34814. Bob, étant le responsable des achats, s'enregistre dans notre plateforme, désigne les employés Alice, Jeff et Fred comme utilisateurs, et génère pour chacun une carte virtuelle avec les numéros D543765H7F, J633843J7T, H377821T7U respectivement. De plus, Bob est en mesure de définir un plan de paiement électronique pour Alice, Jeff et Fred grâce à ces deux

composants, soit la **personnalisation** (*Personalization*) et les **conditions privées et publiques** (*Private/Public Conditions)*. Par conséquent, Alice, Jeff et Fred, étant les utilisateurs désignés dans le *VCC,* peuvent obtenir les justificatifs nécessaires pour effectuer des transactions.

5.3.3.1 Personnalisation

La **Personnalisation** (*Personalization*) constitue un composant principal de *(VCC Generation)*. L'objectif ici est d'utiliser efficacement divers renseignements contextuels pour personnaliser la liste des commerçants désirés (exemple Sears, La Baie, Mobilia) et pour restreindre la liste des produits choisis (exemple des caméras de surveillance, appareils électroniques ou des équipements bureautiques). En d'autres termes, il est décrit comme toute instance ou action qui limite les achats en ligne lorsqu'ils sont effectués par les usagers de *VCC* en dépendant des préférences du titulaire de la carte. En conséquence, son rôle est de mener une assistance guidée et intuitive à l'utilisateur. Ceci dit, le système assure la compatibilité des transactions avec les préférences/exigences du titulaire de la carte tel que limiter les achats en ligne selon la liste des marchands désignée. Pour maintenir ses tâches, la Personnalisation comprend **la gestion du contexte** (*Context Management*) et **la gestion des rétroactions/commentaires** (*Feedback/Reviews*).

- **Gestion du contexte :**

Pour fournir au titulaire de la carte un contenu personnalisé, la gestion du contexte (*Context Management*) s'appuie sur: préférences (*preferences)*, caractéristiques du commerçant et du produit (*merchant/product characteristics*) et environnement (*environment*).

- **Préférences** : Elles peuvent être dynamiques et peuvent changer en fonction des produits/services visés ou de l'identité de l'utilisateur de la carte. En général, les mécanismes de recherche récupèrent le contenu Web qui répond aux objectifs des utilisateurs, mais pas à leurs préférences. Les titulaires de carte peuvent générer des préférences, y compris des paramètres comme *le mode de paiement, les sites Web de magasinage, les limites de coût, le type de marchandises, les marques, les conditions d'achat et de livraison, la zone d'intérêt, etc.* Ces préférences sont indiquées comme requises ou privilégiées. Dans certains cas, le détenteur de la

carte peut être strict au sujet de certaines préférences, tout en étant flexible avec d'autres. Par exemple, le détenteur de la carte peut préciser : « Je veux seulement acheter des livres, et je préfère qu'ils soient expédiés gratuitement avec une possibilité de remboursement dans un délai d'un mois ».

- **Caractéristiques du commerçant et du produit** : Incorporer des informations à propos du commerçant et du produit afin d'assurer la compatibilité entre les caractéristiques et les contraintes du magasinage en ligne. Toute préférence établie par le détenteur de la carte peut être évaluée en fonction du contexte des caractéristiques du commerçant/du produit. Par exemple, le paiement serait rejeté si un commerçant exigeait des paiements dans une devise autre que celle demandée par le titulaire de la carte.
- **Environnement** : Cette partie fournit aux titulaires de cartes des services qui correspondent à leur contexte actuel, *comme l'emplacement, l'heure, le type d'entreprise et les responsabilités* qui leur sont assignés. L'objectif de l'intégration du contexte de l'environnement au *VCC* est double : sélectionner des produits qui correspondent à un certain contexte et s'assurer que les paiements par carte sont bien effectués en fonction de conditions environnementales particulières. Par exemple, limiter les achats aux sites canadiens uniquement (Costco, Walmart), utiliser la carte de crédit durant une période déterminée (de mars à octobre) et générer un courriel de notification après chaque commande.

- **Gestion des rétroactions/commentaires :**

Les titulaires de cartes peuvent fournir des commentaires après avoir fait leur achat pour indiquer leur niveau de satisfaction à l'égard du service ou du produit choisi. Le contenu de ces informations peut être rempli pour être affiché pour les utilisateurs *VCC* afin d'améliorer leur expérience d'achat. Par exemple, une fois la commande accomplie, une notification est envoyée au titulaire de la carte. Ce dernier a l'occasion d'ajouter des informations supplémentaires pour partager des détails à propos du produit tel que : lieu de livraison dans les dépôts de la région ouest, et une note allant de 1 à 5 étoiles pour marquer son appréciation. Ces informations aident au classement des commandes dans l'historique des achats et les rendent plus visibles et facilement trouvables.

5.3.3.2 Conditions privées et publiques

Les **Conditions Privées/Publiques** sont un élément additionnel de la carte de crédit virtuelle (***VCC***) et sont incluses dans le processus de la génération de carte virtuelle (***VCC Generation***). Les *Conditions privées* sont reliées à tout renseignement privé au détenteur de la carte, comme des renseignements personnels (nom, prénom, âge, sexe, adresse et courriel) ou des renseignements sur le paiement (numéro de compte, date d'expiration de la carte, renseignements sur la facturation, limite). Ces informations ne sont pas révélées au commerçant ni même à l'utilisateur de *VCC*. Notre plateforme conserve la propriété de l'anonymat du titulaire de la carte pendant la transaction d'achat. Les *Conditions publiques* sont reliées à toute information considérée comme publique et peuvent être révélées à d'autres entités. Soit P une condition publique, elle peut être représentée comme suit : (P_n, T_n, V_n) où P_n est le numéro de la condition, T_n est le contenu, et V_n est le type de condition. Dans le cas du $V_n = 0$, le P_n est considéré comme une condition publique, sinon P_n est réservé comme condition privée. Par exemple, une condition peut être comme suit : (« C1 », « achat des imprimantes laser de Mars à Octobre 2019», « 0 ») donc la condition C1 est publique (« C2 », « date d'expiration est 02/2020», « 1 ») donc la condition C2 est privée.

5.4 Service du plan e-paiement (*E-PPSM*)

Dans notre plateforme, le service du plan e-paiement *(*E-*PPSM*) se compose de trois sous-partitions : l'espace du commerçant (*Merchant Space*), le moteur de paiement conditionnel (*PC Engine*) et l'espace usager (*User Space*).

5.4.1 Espace commerçant (*Merchant Space*)

Il existe quatre composants dans l'espace commerçant : Les applications Web (*Web Application*), l'API Web paiement (*Payment Web API*), les méthodes de paiement (*Payment Instruments*), et les mécanismes de négociation (*Negotiation Mechanisms*).

Les applications Web (***Web Application***) représentent la page Web où les renseignements sur le paiement sont affichés. Deux aspects fondamentaux devraient être présents : l'identification/authentification et la confiance. Plusieurs mécanismes sont

disponibles pour l'identification et l'authentification, incluant : *X.509 certificats, Mozilla Persona* (Baden*, et al.*, 2009), *WebID* (Faísca & Rogado, 2016). En ce qui concerne la confiance, plusieurs efforts ont été faits pour déterminer à quel point un site Web est digne de confiance. Par exemple, *TRUSTe* (Shneiderman & Zhao, 2016) utilise des répertoires de certification d'identité, Google a toujours préféré les sites ayant un certificat SSL (HTTPS), GoDaddy.com le vendeur de noms de domaines le plus connu fournit un nom de domaine à la fois intéressant et professionnel.

L'API Web paiement (***Payment Web API***) est chargée de définir une interface de programmation d'applications (API) qui permet le développement de divers processus. Ces processus sont liés à l'utilisation de différents instruments de paiement qui aident le client à gérer ses paiements de façon uniforme sur le site Web du commerçant. Ils comprennent la négociation d'une méthode de paiement, le paiement et l'obtention d'un reçu.

Les méthodes de paiement (***Payment Instruments***) sont définies pour soutenir divers outils de paiement. En général, le système de paiement offre une solution pour réduire le risque de fraudes et améliorer la sécurité et l'anonymat des utilisateurs. Dans ce travail, le système de paiement considère le *VCC* comme une solution de paiement. Cependant, d'autres modèles existent pour les solutions de paiement sur Internet (les cartes de crédit, les paiements par jetons, Bitcoin, WeChat, PayPal, EMV, Google Wallet, etc.) pourraient également être inclus.

Les mécanismes de négociation (***Negotiation Mechanisms***) sont responsables de l'entente entre le client en tant que payeur et le commerçant en tant que bénéficiaire. Ils supportent différentes questions liées à la transaction telles que la méthode de paiement et, éventuellement, le prix ou toute autre condition de paiement. Pour faciliter la procédure d'achat, l'objectif principal est d'effectuer des échanges de négociation basés sur les préférences des consommateurs afin de leur permettre de sélectionner le système qui leur convient le mieux (Mu*, et al.*, 2014). D'une façon explicite, les modèles de négociations sont conçus pour mettre en place des stratégies en ligne pour faciliter les échanges entre les vendeurs et les acheteurs. De telles stratégies sont reliées aux offres des prix, aux caractéristiques de produits, aux garanties ou aux contrats de services en vue de collaborer

et ceci avant de conclure les transactions, comme lors de l'achat d'un billet d'avion, le vendeur propose un prix avec la réservation de deux nuits d'hôtel.

5.4.2 Moteur de paiement conditionnel (*Payment Conditional Engine*)

Dans le système *E-PPSM*, le moteur de paiement Conditionnel (*Payment Conditional Engine ou PC engine*) comprend les principales tâches de base pour préserver la vie privée des utilisateurs et les achats conditionnels multimarchands. Le moteur comprend trois composants: les conditions publiques (*Public Conditions*), l'évaluation et la vérification (*Evaluation and Verification*) et le système de paiement automatisé (*Automated Teller Payment*).

- Conditions Publiques (***Public Conditions***) sont basées sur l'extension des différents critères utilisés pour accéder aux produits offerts par les commerçants. Pour définir ces conditions, un ensemble d'expressions logiques peut être configuré avec différents paramètres. Par exemple, supposons qu'une base de données D contienne des enregistrements de données transmises par un ensemble de *N* commerçants au sujet de M éléments. Chaque article pourrait représenter en réalité un service ou un produit inclus dans la transaction d'achat. Chaque enregistrement dans l'ensemble de données D est un enregistrement (*rID; mID; pID; attrP*), où *rID* est le numéro de l'enregistrement, *mID* correspond au commerçant qui a contribué à cet enregistrement, *pID* est l'élément dont il s'agit, et *attrP* détient les conditions publiques définies par le commerçant. En réalité, divers renseignements peuvent être personnalisés dans un ensemble d'attributs liés aux caractéristiques des articles (prix, type ou qualité) ou aux qualifications des commerçants (classification, notation ou crédibilité). Prenons l'exemple de l'enregistrement (Id2343, BestBuy, imprimante laser, livraison en 3 jours).
- Évaluation et vérification (***Evaluation and Verification***) est l'un des composants importants. Il effectue la comparaison et la vérification entre les conditions publiques de l'utilisateur de *VCC* et celles du commerçant afin de prendre la décision d'accepter ou rejeter le paiement. Les conditions des deux paires doivent correspondre afin d'accepter la transaction. Dans le cas inverse, la transaction sera

rejetée. Prenons l'exemple de l'enregistrement défini par Bob : (CondA1, livraison gratuite dans 3 jours, 0). CondA1 est une condition publique. Au niveau du commerçant, les produits dont la livraison dure plus que 3 jours sont rejetés.

- Système de paiement automatisé (***Automated Teller Payment***) prend en charge la fonction de traiter des marchands multiples. Il fournit à l'utilisateur l'option d'effectuer différentes opérations d'achat, dont chaque transaction peut appartenir à un commerçant distinct. Grâce à cette fonctionnalité, le consommateur effectue le paiement en utilisant le *VCC* pour multiples achats et multiples commerçants. En tant que récepteur, son rôle est d'interpréter le message provenant de l'**Évaluation et Vérification** quand cette dernière autorise le paiement. Par conséquent, il peut obtenir les informations du paiement et peut entamer la procédure pour le consommateur enregistré. Il agit en tant qu'entité impliquée dans les services de non-répudiation, en tant qu'initiateur envoyant des messages à de multiples destinataires et en tant que récepteurs de messages. Supposons que Fred est un utilisateur de VCC. Il soumet trois requêtes pour trois marchands : BestBuy, Sears et Amazon. Dans le moteur de paiement conditionnel, les enregistrements sont comme suit : (Id2343, BestBuy, imprimante laser, livraison en 3 jours), (Id7847, Sears, cafetière, prix moins que 50.0$), (Id194A, Amazon, livre, livraison gratuite). Une fois soumis, les enregistrements seront validés par l'évaluation et la vérification. Fred reçoit le résultat. Si les requêtes sont acceptées, le système de paiement automatisé les reçoit, les traite et envoie les paiements aux marchands désignés.

5.4.3 Espace usager (User Space)

Il existe quatre composants dans l'espace usager : le Système de Paiement par Carte de Crédit Virtuelle (*VCC Payment System*), la carte de crédit virtuelle configurée par le détenteur de carte (*Virtual Credit Card or VCC*), la Personnalisation (*Personalization*), et les Conditions privées et publiques (*Private/Public Conditions*).

Le Système de Paiement par Carte de Crédit Virtuelle (***VCC Payment System***) est la pierre angulaire du soutien du message généré par le système de paiement automatisé

(***Automated Teller Payment***). Dans ce message, les renseignements sur le paiement peuvent être inclus et utilisés pour lancer la transaction. Les messages concernant le paiement doivent être échangés au moyen d'un protocole de paiement. En outre, il est important de garantir l'identité d'un utilisateur dans une transaction. Une demande est envoyée pour authentifier l'émetteur du message en fonction des informations de la carte utilisée.

La carte de crédit virtuelle **(*VCC*)** est responsable de l'information de la carte de crédit virtuelle; celle-ci est chargée de dissimuler l'identité du titulaire de la carte et de protéger ses renseignements. L'utilisateur est authentifié dans cette partie au moyen d'une authentification à haute sécurité (p. ex., un schéma d'authentification à trois facteurs qui combine la biométrie, un mot de passe et un élément sécurisé comme la carte à puce) (Cellary & Rykowski, 2015).

À l'instar de la Génération de la carte virtuelle (***VCC Generation***) dans l'espace du titulaire de carte (voir le paragraphe 5.3.3), le *VCC* inclut: la **personnalisation** et les **conditions privées/publiques**.

- Personnalisation (***Personalization***) aide les utilisateurs de *VCC* à modéliser leur plan de paiement électronique en fonction de leurs intentions et de leur situation actuelle. L'automatisation de ces tâches dépend fortement du contexte personnel de l'utilisateur. De plus, il garantit que le contexte est conforme à la personnalisation et aux préférences du détenteur de la carte, spécifiées lors de la génération de la carte. Le plan de paiement électronique peut comprendre un ensemble de sites Web privilégiés en fonction de la nature des objectifs personnels de l'utilisateur tels que Amazon.ca, Sears.com, Costco.ca, un ensemble de mots clés qui décrivent l'intérêt de l'utilisateur et les produits souhaités que l'utilisateur s'attende à récupérer tel que caméras de surveillance, accessoires bureautiques, imprimantes, etc. En outre, il détient tout l'historique des plans de paiement électronique modifiés par l'utilisateur et apporte un avantage considérable à notre plateforme.
- Conditions Privées/Publiques (***Private/Public Conditions***) représente un élément supplémentaire dans *VCC*. Il améliore l'expérience de l'utilisateur par l'automatisation des tâches répétitives et ordinaires pour atteindre les buts et

l'information contextuelle. Supposons que (P_n, T_n, V_n) est la condition où P_n est le numéro de la condition, T_n est le contenu, et V_n est le type de condition. Dans le cas où $V_n = 0$, la condition P_n est considérée comme une condition publique donc peut être publiée, sinon la condition P_n est réservée comme condition privée. Prenons l'exemple des conditions (C1, achat des imprimantes laser avec livraison gratuite, 0) et (C2, limite du crédit est 5000$, 1). Comme décrit, la condition C1 est publique, par contre la condition C2 est privée.

La prochaine section décrira plus en détail notre système de paiement électronique, expliquera les procédures et fournira le flux d'information avec un scénario d'application.

5.5 Scénario d'exécution

Prenons l'exemple d'un détenteur de carte qui a déjà acquis une carte de crédit. La banque émettrice lui fournit une solution pour obtenir des cartes virtuelles. On peut aussi supposer que le détenteur de carte a une liste d'utilisateurs à qui il veut fournir des cartes virtuelles. Supposons que Bob, responsable des achats, est le titulaire de la carte de crédit. Afin de gérer les achats dans son département, Bob s'enregistre dans notre plateforme et sélectionne cinq usagers afin de leur donner des cartes de crédit virtuelles.

Pour ce faire, Bob suit le processus dans notre plateforme selon deux flux.

Le premier flux, illustré à la Figure 18, commence à partir de la validation de la carte de crédit jusqu'à ce que le *VCC* et le plan de paiement électronique soient prêts pour une utilisation future. Par souci de simplicité, seules les opérations effectuées du point de vue de l'utilisateur sont incluses, alors que les différentes opérations que l'émetteur de carte effectue pour générer une carte de crédit et *VCC* sont omises. Donc dans ce processus Bob ouvre une session, s'enregistre, présente sa carte de crédit et soumet une demande de création de cartes virtuelles pour cinq usagers. Bob définit également son plan de paiement avec les conditions suivantes:

- (C1, date d'expiration 05/2020, 1) comme une condition privée
- (C2, limite de la carte virtuelle 600$, 1) comme une condition privée

- (C3, achat des imprimantes laser de mars à octobre 2019, 0) comme une condition publique
- (C4, sélection des vendeurs Bestbuy ou Costco, 0) comme une condition publique.

Le *E-PPSM* valide les informations, accepte ou rejette la demande. Une fois accepté, le service du plan de paiement configure les données et assigne à chaque usager un plan tel que défini par Bob au niveau de la carte *VCC*. À la fin de son travail, Bob ferme sa session.

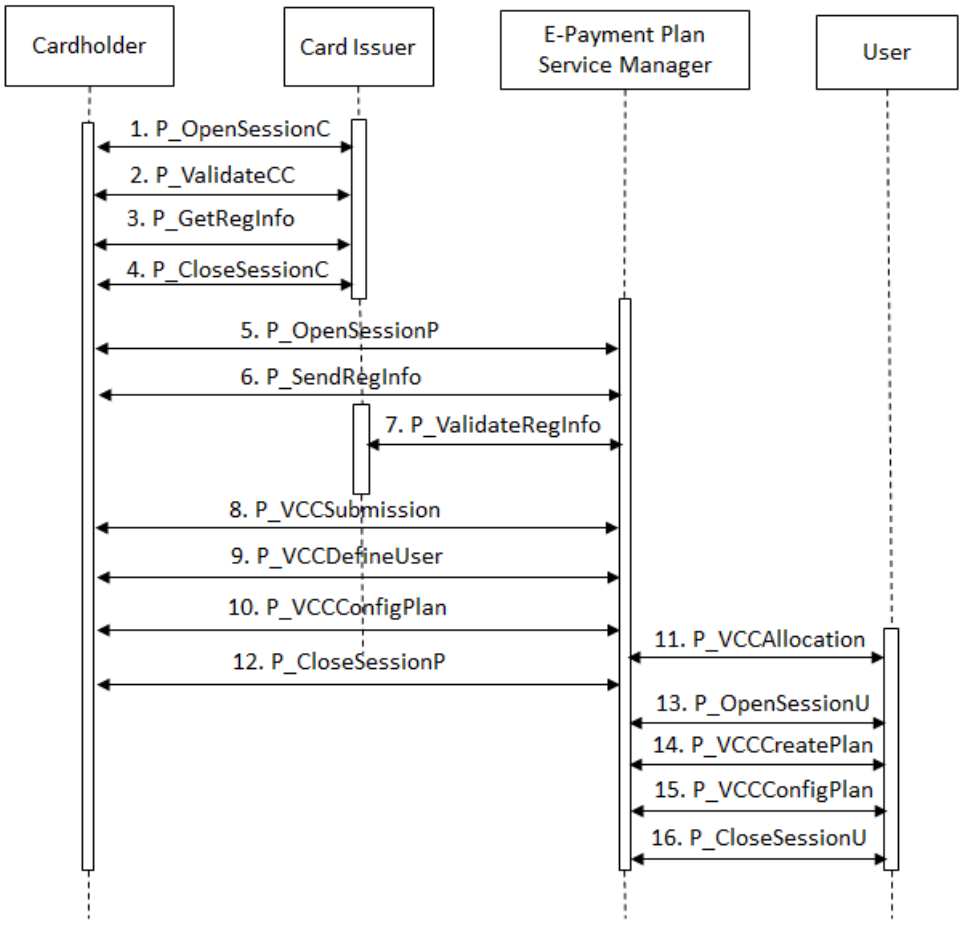

Figure 18 - Configuration du VCC et plan de paiement en ligne

Le deuxième flux, illustré à la Figure 19, comprend une transaction d'achat en ligne avec plusieurs commerçants. Il comprend différentes fonctions liées au moteur du paiement conditionnel (PC Engine), au commerçant et au déroulement de la transaction. Supposons

qu'Alice est l'un des usagers que Bob a sélectionnés pour lui assigner une carte virtuelle. Dans le deuxième flux, Alice est capable de se loguer dans notre plateforme, s'identifier et procéder aux achats sélectionnés. Par l'intermédiaire du *E-PPSM*, Alice peut communiquer avec les marchands et choisir les produits. Comme défini dans notre plateforme, le *E-PPSM* s'occupe de la validation des achats avec les conditions publiques prédéterminées. Seuls BestBuy et Costco sont acceptés comme marchands, les imprimantes laser sont permises et tout ceci devra se dérouler de Mars 2019 à Décembre 2019. En dehors de ces conditions, la transaction sera rejetée.

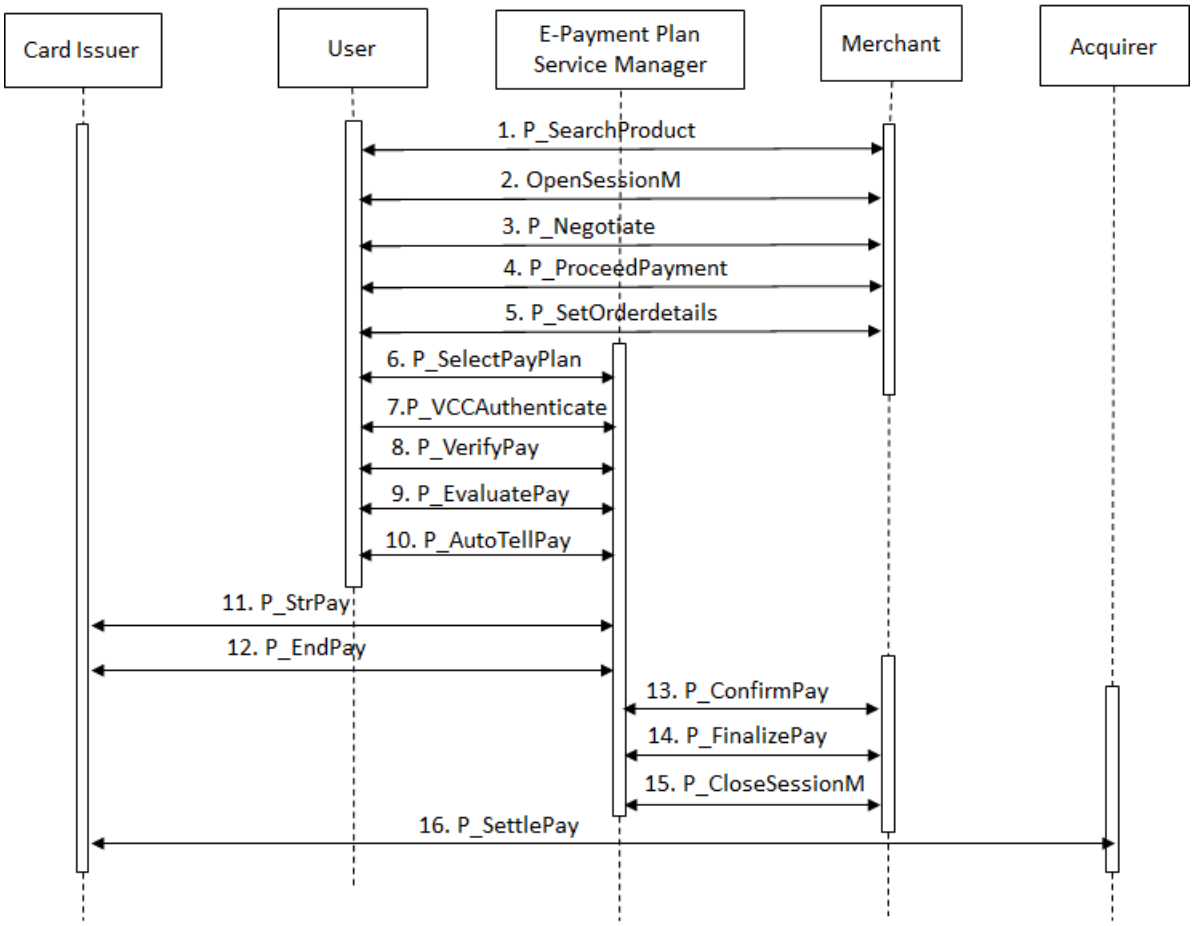

Figure 19 - Procédures pour un scénario d'un achat multiple

5.5.1 Configuration du VCC et plan de E-paiement

Dans le premier flux, le processus serait le suivant, tel qu'illustré à la Figure 18 :

1- Bob effectue l'ouverture d'une session avec la banque émettrice en utilisant ses identifiants (étape 1).
2- La banque émettrice valide sa carte de crédit (étape 2).
3- Après validation, Bob envoie une demande d'inscription à un nouveau plan de paiement (**E-Payment Plan**) (étape 3).
4- Une fois Bob authentifié, la banque émettrice lui retourne les informations d'enregistrement ***VCC*** nécessaires pour être déployées dans le E-PPSM. Après avoir finalisé la validation et l'inscription, Bob ferme la séance (étape 4).
5- Par la suite, Bob amorce une session sécurisée avec le *E-PPSM* (étape 5).
6- Lorsque la fonction correspondante est invoquée, Bob peut s'inscrire (étape 6) en utilisant les informations d'enregistrement précédemment acquises auprès de la banque émettrice. Pour la première fois, le *E-PPSM* fournit à l'utilisateur un nouveau plan de E-Payment Plan. Dans notre exemple, si Alice est pour la première fois un utilisateur de la carte virtuelle définie par Bob, le *E-PPSM* lui assigne un nouveau plan, sinon le plan déjà existant sera modifié.
7- L'émetteur et le *E-PPSM* échangent les informations d'identification (étape 7). La banque émettrice ajoute un ensemble d'entités au profil d'utilisateur : (E_IdInf, E_PayPlan, TimeStamp, StatEvent) où E_IdInf est l'information d'identification fournie par la banque émettrice, E_PayPlan est le E-Payment Plan complété par le E-PPSM, TimeStamp est la date/heure de l'événement, et StatEvent représente l'état de l'événement. Au départ, l'état est « en attente ». Lorsque le détenteur de la carte valide le E-Payment Plan, l'état est remplacé par « validé », sinon il ne peut être déployé.
8- Après la génération de la carte virtuelle, les cartes sont soumises au *E-PPSM* (étape 8).
9- Bob définit une liste d'utilisateurs (étape 9)
10- Bob configure le *E-Payment Plan* avec un ensemble de conditions privées/publiques (étape 10), ce qui signifie la liste des commerçants désignés, les prix limités, les marques, le type d'achats, et la plage de temps. En conséquence, les fonctions retournent un message indiquant si le *VCC* est configuré avec succès ou pas. Une fois configuré correctement, le *VCC* est créé avec un statut « non

attribué » pour indiquer que le *VCC* peut maintenant être attribué à un utilisateur enregistré. En fait, un utilisateur *VCC* doit être enregistré pour accéder aux services offerts par le *E-PPSM*.

11- Le processus d'attribution commence (étape 11), et l'état du *VCC* est mis à jour pour « attribué », ce qui signifie qu'il ne peut pas être attribué à un autre utilisateur, et le gestionnaire de service renvoie un message de confirmation au détenteur de la carte.

12- Enfin, Bob peut mettre fin à sa session (étape 12).

13- Par la suite, Alice démarre le processus de configuration *VCC* et ouvre une session sécurisée (étape 13).

14- Une fois authentifié par le service, le *E-PPSM* génère un plan pour Alice (étape 14).

15- Alice configure le plan avec un ensemble de conditions privées/publiques (étape 15). En plus de ces étapes, le *E-PPSM* valide toutes les entrées et considère le *E-Payment Plan* d'Alice comme un sous-plan dans le plan du détenteur de carte, en gardant potentiellement la possibilité de le personnaliser à sa discrétion. Dépendamment des résultats de la validation, le *E-PPSM* accepte ou refuse le plan modifié.

16- Une fois terminée, Alice peut mettre fin à la session (étape 16).

5.5.2 Procédures de scénario d'achats multiples

Dans le second flux, le processus serait le suivant, tel qu'illustré à la Figure 19 :

1- Avant le paiement, le *E-PPSM* peut invoquer différentes fonctions pour gérer le processus ou pour demander des renseignements concernant les achats, par exemple la recherche du produit, le lancement d'une séance avec le commerçant, la négociation des prix et des offres, la conclusion du paiement et la préparation des détails de la commande (étapes 1, 2, 3, 4 et 5). Ces fonctions peuvent être invoquées à tout moment, répétées pour le prochain achat et avant l'exécution du plan de paiement.

2- Lorsqu'Alice effectue tous les achats et passe à la caisse, cette page comprend habituellement le nom du commerçant, les détails de la commande et le montant

final à payer. Par conséquent, tous les achats seront regroupés dans une page où Alice peut passer par une série d'étapes, par exemple vérifier les détails de la commande et décider de retirer, d'ajouter ou de garder des articles. Enfin, Alice peut décider de procéder au paiement final, de sorte qu'elle vérifie la prochaine étape pour invoquer la sélection plan de paiements (étape 6 de).

3- Selon le rôle du plan, trois actions se produisent : authentifier l'utilisateur, identifier la carte virtuelle attribuée et valider les détails du paiement (étapes 7, 8 et 9).
4- L'étape suivante (étape 10) traite le message reçu qui contient les détails de la caisse.
5- Le message doit être sans erreur pour l'ouverture du paiement (étape 11), sinon l'opération est rejetée. À cette étape, E-PPSM et la banque émettrice de la carte de crédit envoient/reçoivent les informations nécessaires pour l'autorisation et la validité.
6- L'émetteur de carte renvoie un message d'approbation ou de refus au système *E-PPSM*. À la fin, la séance est terminée (étape 12).
7- Par la suite, le système *E-PPSM* envoie le statut au commerçant (étape 13), qui peut mettre à jour l'état de commande dans son propre serveur et le renvoyer pour confirmer le résultat (étape 14).
8- Enfin, le processus se termine par la fermeture de la session (étape 15).

Après avoir examiné l'ensemble du processus, la section suivante présente une analyse détaillée des principales propriétés de notre plateforme.

5.6 Analyse et utilisation

Notre nouvelle plateforme de paiement électronique comprend des renforcements au niveau de la protection de la vie privée, du paiement électronique conditionnel, du contrôle et de la supervision des achats et au niveau des paiements simultanément. Il s'agit donc d'améliorations apportées au processus de paiement, en plus de la caractéristique d'achats multiples. Les paragraphes suivants fournissent une analyse des principales propriétés.

5.6.1 Rôle de la protection de la vie privée

La protection des renseignements personnels des titulaires de carte est l'une de nos principales préoccupations dans notre plateforme. L'accès aux renseignements de la carte échangée est limité à l'émetteur (*Issuer*) et au détenteur de la carte (*Cardholder*). L'émetteur est l'entité unique qui peut valider les renseignements de la carte et fournir les renseignements du *VCC* qui seront attribués aux utilisateurs. Nous supposons que l'émetteur de carte de crédit (*Credit Card Issuer*) est une entité digne de confiance.

Le Système de paiement par carte de crédit (*Credit Card Payment System* ou *CCPS*) est une entité qui traite de la protection des renseignements personnels. Il aide à préserver les renseignements financiers et non financiers du titulaire de la carte. Dans la génération de carte virtuelle (*VCC Generation*), la personnalisation (*Personalization)* et les conditions privées/publiques (*Private/Public Conditions)* sont configurées par le titulaire de la carte. Ainsi, les renseignements financiers et non financiers ne sont divulgués à aucun tiers. De plus, le moteur de paiement conditionnel (*Payment Conditional Engine* ou *PC Engine*) comprend les principales tâches de base pour préserver la vie privée du titulaire de la carte et pour compiler l'opération de paiement sans révéler aucune information personnelle comme le numéro de carte, la date d'expiration de la carte, le code de vérification.

5.6.2 Rôle du processus de contrôle

En 1916, Henri Fayol formula une des premières définitions du contrôle relié à la gestion (Shafritz*, et al.*, 2015) : « Le contrôle consiste à vérifier si tout se passe conformément au plan adopté, aux instructions émises et aux principes établis… ». Dans le même contexte, notre plateforme assure le facteur de **contrôle** au détenteur de la carte. Le VCC est basé sur un ensemble de Conditions Privées/Publiques (*Private/Public Conditions)* spécifiées d'abord par le détenteur de la carte, puis par l'utilisateur de *VCC*. Le moteur de paiement conditionnel (*Payment Conditional Engine* ou *PC Engine*) veille à ce que ces conditions soient remplies par l'intermédiaire de l'évaluation et de la vérification et suite à leur harmonisation avec les conditions publiques des commerçants. Ces conditions aident les titulaires de cartes à prendre le contrôle de leurs achats.

5.6.3 Rôle du processus de supervision

La propriété **Supervision** apporte beaucoup d'améliorations à l'expérience magasinage. Il constitue plus précisément un outil efficace permettant aux titulaires de cartes de crédit de gérer leurs dépenses. Notons que le *VCC* comprend la notion de personnalisation. Dans un contexte bien défini, l'utilisateur de *VCC* est capable d'effectuer des transactions parmi les limites indiquées dans les préférences du détenteur de la carte, tout en gardant pour lui l'option d'ajouter des commentaires ou des rétroactions. Cette caractéristique, ainsi que la propriété **Contrôle** décrite précédemment, nous amène à établir une architecture de paiement qui assure une expérience de magasinage fiable pour le titulaire de la carte.

5.6.4 Rôle du processus d'achats multiples

Pour que le commerce électronique continue à s'épanouir, il est essentiel d'assurer des achats multiples dans un système de paiement électronique sain, sécuritaire et efficace. La plupart des protocoles de paiement ont certaines limites pour supporter une transaction utilisant plusieurs cartes, comme le fait que les cartes devraient être de la même banque et devraient être basées sur des transactions indépendantes (Sureshkumar*, et al.*, 2016). Cependant, notre plateforme soutient la génération de plusieurs cartes de crédit *VCC* qui peuvent appartenir à différents émetteurs. De plus, comme indiqué dans le déroulement, l'utilisateur de *VCC* est capable de faire plusieurs achats, de les ajouter à un même panier et de lancer le plan de paiement électronique (***E-Payment Plan***), qui s'occupera du processus de paiement au moyen du système de paiement automatisé (***Automated Teller Payment)***.

5.6.5 Rôle du paiement conditionnel

La dernière propriété de notre plateforme est la caractéristique du paiement **conditionnel**. Tel que décrit dans le deuxième flux de paiement, un paiement ne peut être effectué que si toutes les conditions sont remplies et satisfaites. Dans un scénario de paiement traditionnel, un certain nombre de conditions peuvent être définies telles que la limite de carte de crédit et la date d'expiration. Dans notre plateforme, des conditions

supplémentaires spécifiées par l'utilisateur peuvent être fixées en fonction des Conditions Privées/Publiques (***Private/Public Conditions)*** définies dans *VCC*.

5.7 Conclusion

Les services sécurisés de paiement en ligne ont fait l'objet d'études approfondies dans les systèmes de cartes bancaires. Néanmoins, la principale préoccupation des solutions existantes est la sécurité, alors que la supervision, le contrôle et la protection de la vie privée sont à peine abordés. Dans ce chapitre, nous avons présenté une nouvelle plateforme de paiement électronique (*E-Payment Plan*) qui, en plus de la sécurité, vise principalement à protéger la vie privée des consommateurs, tout en offrant le contrôle et la supervision, en intégrant le Plan de paiement électronique (*E-Payment Plan*) et le *VCC* (El Haddad*, et al.*, 2017).

Premièrement, cette combinaison assure la protection de la vie privée. Dans le cas des achats en ligne, l'utilisateur doit fournir des renseignements sur les paiements à divers moments. Dans la plateforme que nous proposons, il n'est pas nécessaire d'inclure des renseignements qui pourraient être piratés ou volés. Deuxièmement, la personnalisation est assurée dans la plateforme, offrant une expérience d'achat plus facile/plus flexible. Les titulaires de carte sont en mesure de définir un ensemble de conditions privées et publiques selon leur choix.

Enfin, les détenteurs de cartes de crédit obtiennent une solution efficace qui leur permet de contrôler et de superviser leurs dépenses liées aux cartes de crédit, ce qui constitue deux de nos contributions, à savoir supporter les scénarios d'achats multiples et les paiements conditionnels. Par conséquent, notre travail consiste à offrir une approche holistique qui intègre, en plus de la sécurité, la personnalisation, le contrôle et la supervision des paiements en ligne par carte de crédit tout en garantissant la confidentialité des titulaires de carte.

Chapitre 6 : La cybersécurité dans le contexte de paiement en ligne

La présente recherche explore la relation entre les connaissances en cybersécurité, le comportement de l'usager en ligne et la perception des risques. Afin d'atteindre ces objectifs, nous avons simulé une expérience de magasinage en ligne. Nous avons aussi développé un nouveau site Web « **PAYCTRI** » (*PAYment Transactions with Cybersecurity Incidents*) et invité des participants à y accéder. Selon le cheminement de l'expérience, le participant répond à une série de questions et suit des étapes bien déterminées. Les questions ont pour but d'évaluer le niveau de connaissances du participant en matière de cybersécurité. À partir de cette simulation de magasinage en ligne, nous pouvons extraire plusieurs constatations. Tout d'abord, les activités offertes en ligne sur notre site Web jouent le rôle de médiateurs qui interagissent avec l'utilisateur, par exemple il peut obtenir plus de crédits en échange de ses renseignements personnels, ou enregistrer ses renseignements sur la carte de crédit virtuelle, ou encore choisir un scénario de magasinage bien précis. Ensuite, nos résultats soulignent l'importance de sensibiliser les internautes en cybersécurité, de les rendre conscients que lorsqu'ils partagent leurs informations privées en ligne, elles deviennent publiques et de les inciter à prendre des mesures de sécurité plus efficaces pour la protection de leurs données.

6.1 Travaux en cybersécurité

L'intérêt pour le concept de la cybersécurité a augmenté ces dernières années en raison de l'énorme croissance de la technologie. Cette évolution peut être considérée comme une épée à double tranchant. Même si ceci prévoit une ère formidable et innovante de périphériques connectés et d'applications partagées et avancées, les usagers sont néanmoins exposés aux manipulateurs de données qui peuvent altérer leurs données ou aux pirates malveillants qui peuvent prendre le contrôle de leurs machines. En effet, les clients visitent souvent des sites risqués ou non protégés pour télécharger des données, de la musique ou pour magasiner en ligne.

Avec la multiplication des transactions en ligne et l'accumulation massive de données sur les utilisateurs, les risques de cyberattaques, de fraudes et de vols d'identités sont multipliés. Ces derniers sont introduits par des criminels qui usurpent l'identité de la prétendue victime. Cela est lié notamment à l'augmentation de l'espionnage industriel et à la cybercriminalité, où des logiciels malveillants sont de plus en plus utilisés pour le piratage de données à des fins lucratives. Par exemple, les usagers qui se branchent sur des connexions non sécurisées ou qui partagent volontiers leurs renseignements personnels sur des sites publics sont des victimes potentielles de vols d'identité. De même, les voleurs d'identité en ligne sont intéressés par la collecte des profils des utilisateurs et des informations personnelles tels que les informations de carte de crédit, les numéros de comptes bancaires et de permis de conduire. Ces violations de la sécurité en ligne aggravent différents problèmes de fraudes telles que les cartes falsifiées et d'autres fraudes bancaires en ligne (Levi, 2017). Malgré ces risques, les usagers ne sont pas tellement préoccupés par la cybersécurité soit parce qu'ils ne sont pas intéressés par celle-ci ou bien n'ont pas encore connu des problèmes à ce niveau (de Bruijn & Janssen, 2017). Ils supposent que leur fournisseur de service ou leur vendeur va assurer leur sécurité sur Internet.

La cybersécurité a été largement abordée dans la littérature. Des efforts considérables ont été investis dans la prévention des violations de données, et le combat pour veiller à ce qu'il existe une sécurité dans le monde digital. Des domaines variés tels que l'ingénierie sociale (Hatfield, 2018), la politique (Z. Li & Liao, 2017; H. Zhang*, et al.*, 2018), les régulateurs de la politique et l'économie (Bauer & Van Eeten, 2009; Moore, 2010), la technologie (Leszczyna, 2018; Sohal*, et al.*, 2017), les comportements humains (Anwar*, et al.*, 2017; Hadlington, 2017) et les services médicaux et sanitaires (Kruse*, et al.*, 2017; Ross, 2017) s'attaquent à la cybersécurité. Dans les systèmes de gestion, des outils de protection de données apparaissent sur le marché pour connaître, pour comprendre et pour anticiper les problèmes potentiels qui peuvent survenir (Roldán-Molina*, et al.*, 2017). La cybersécurité est également devenue un intérêt dans les systèmes infonuagiques (*info cloud*) en surveillant le trafic du réseau entrant et sortant pour déceler toute activité suspecte (Kshetri, 2017).

L'amélioration de la cybersécurité à un niveau plus large devient un défi pour les entreprises. Pour contrer les risques d'attaques, des mesures de sécurité plus efficaces doivent impérativement être mises en place, à la fois par les compagnies et par les consommateurs. Historiquement, la cybersécurité a été fortement structurée dans des arrangements réglementaires par des organismes volontaires et auto réglementés (Bauer & Van Eeten, 2009; Lewis, 2005) autres que l'application de la loi. Au fil des ans, les conséquences des cyberattaques sont devenues inévitables pour les deux secteurs publics et privés.

À cet égard, l'entreprise de télécommunications américaine **Verizon** a publié un rapport en 2017 sur les atteintes en sécurité des données. Ce rapport comprenait une analyse de 42 068 incidents et de 1 935 atteintes dans 84 pays du monde (Enterprise, 2017). Ces résultats ont donné lieu à d'autres solutions et à une plus grande sensibilisation. Les entreprises sont devenues plus conscientes des risques de perte d'informations sensibles. Elles ont investi énormément dans des solutions visant à assurer la sécurité des données personnelles comme les antivirus et les pare-feu (Kshetri, 2017), ou dans des mesures préventives comme le chiffrement du disque dur (Mulligan & Bamberger, 2007). Notons qu'une solution de cybersécurité doit être réalisable. Afin d'obtenir des résultats cohérents, la solution devrait assurer une résistance efficace contre les attaques en ligne et elle devrait aussi être efficace sur le plan opérationnel (de Bruijn & Janssen, 2017). Telles solutions reposent sur des mesures techniques sur le plan de l'infrastructure, sur le matériel et sur les logiciels (Bauer & Van Eeten, 2009).

Pour en savoir plus sur le cheminement du présent travail, nous décrivons le contexte de notre expérience d'achat dans la prochaine section.

6.2 Le contexte de l'expérience

Au cours des dernières décennies, le monde numérique a été confronté à beaucoup d'attaques et d'intrusions à la sécurité. Les résultats de telles attaques sont devenus plus dangereux et peuvent causer des dégâts catastrophiques et beaucoup plus élevés tels que montré dans la Figure 20. Ils mettent en danger un bon nombre d'intervenants qui font face à des tels incidents et menaces (de Bruijn & Janssen, 2017).

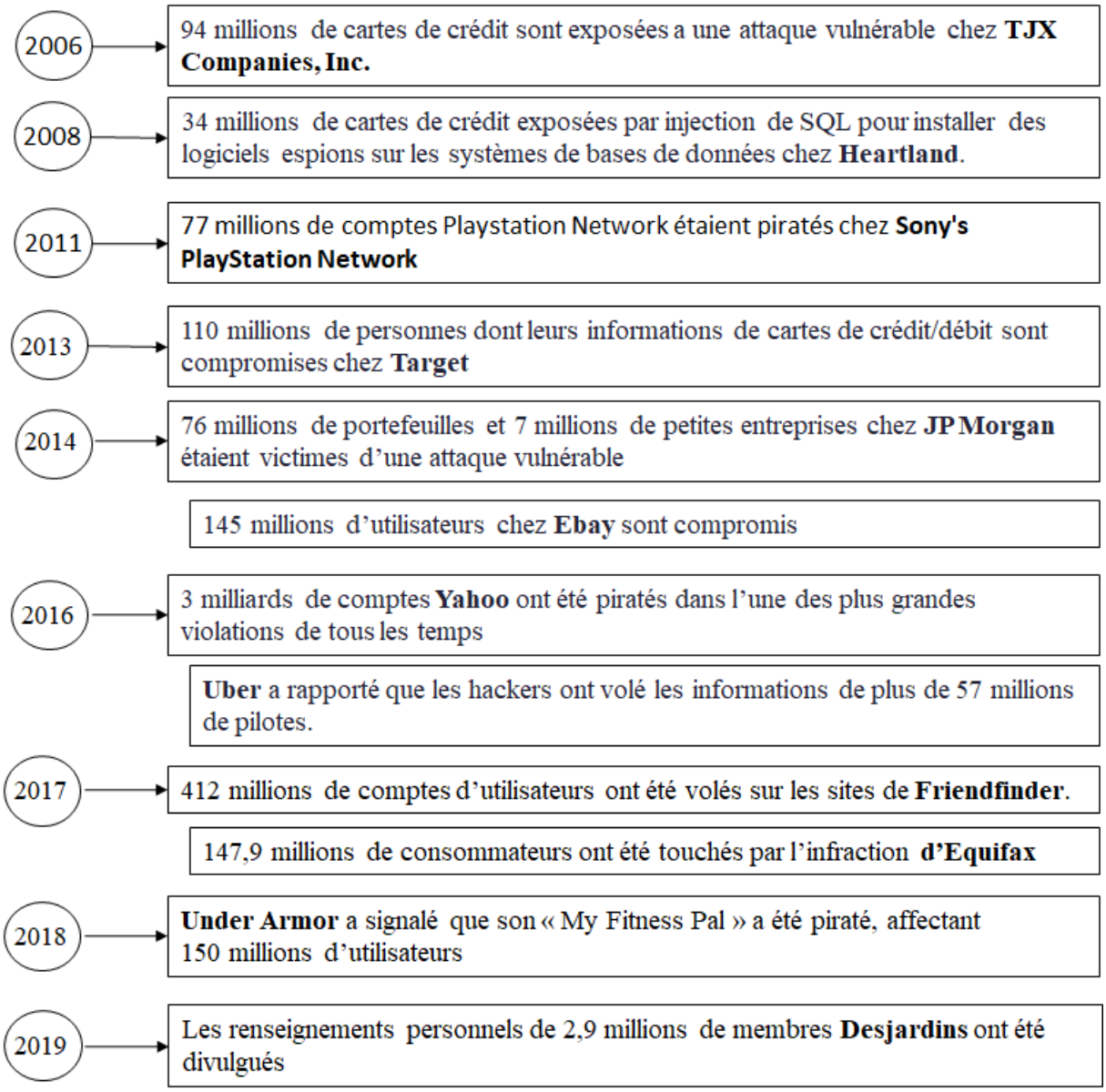

Figure 20 - Cyber attaques les plus importantes au fil des années[13,14]

Beaucoup de défis liés à la cybersécurité surviennent continuellement et restent requis dans le domaine du commerce électronique. Ce dernier, dont la subsistance dépend uniquement des transactions financières en ligne, est également affecté par les cyberattaques et les fraudes, en particulier dans les systèmes **à base de Cartes Non**

[13] https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html consulté le 22/sep/2019
[14] https://www.varonis.com/blog/cybersecurity-statistics/ consulté le 22/sep/2019

Présentes (*CNP*). Cela signifie que les transactions sont initiées par les clients à partir du site Web du marchand, par conséquent les informations de la carte sont fournies sur la page de paiement sans la machine de paiement et sans que la carte soit présentée physiquement au marchand. Les usagers sont également victimes de comportements malveillants sur internet sans jamais être au courant des accès non autorisés. Les vols d'identité et les fraudes dans les cartes continuent de croître de façon exponentielle. D'un côté, les banques et les sociétés financières doivent prendre le risque de protéger les individus contre les fraudes en ligne. D'un autre côté, les usagers doivent également prendre des initiatives afin de combattre les menaces en ligne.

En fait, la plupart des gens ont entendu parler de la cybersécurité (de Bruijn & Janssen, 2017). Le niveau de sensibilisation est encore loin de générer une perception d'urgence pour alarmer les usagers et pour prévoir le comportement approprié à la situation. La plupart du temps, les usagers ne mènent des actions préventives qu'après une violation sur leurs données. Par la suite, ils adoptent diverses mesures de prévention : révision des mots de passe, mise à jour ou installation des logiciels d'antivirus, changement de leurs informations d'identification, etc. Ce qui nous amène à déduire que les violations de vie privée forcent les usagers à effectuer des mises à jour régulières sur leurs ordinateurs (Cerdeiro, 2017).

Il serait erroné de considérer la cybersécurité uniquement comme un ensemble de mesures visant à protéger les mécanismes technologiques (matériels, logiciels et applications). Par conséquent, la prévention et la sensibilisation dans le domaine de la cybersécurité sont nécessaires pour garder les victimes en ligne au courant des comportements malveillants liés à leurs données et à leurs activités quotidiennes. Des initiatives doivent être considérées non seulement par des spécialistes ou experts, mais aussi par les utilisateurs qui doivent être motivés par la formation et l'éducation qui s'avèrent être une des méthodes à adopter pour prévenir de telles attaques (Hatfield, 2018). Notre expérience a principalement pour but de répondre aux questions de recherche suivantes. 1) Est-ce que les internautes prennent des mesures de préventions contre les problèmes de sécurité ? 2) Quel est leur comportement lorsqu'ils sont soumis à des questions personnelles ou financières ? 3) Quelle est leur perception sur la préservation de

vie privée ? 4) Quel est leur comportement lorsqu'ils achètent en ligne dans un contexte particulier de scénarios d'achats?

Nous abordons dans la section suivante la mise en application de notre expérience de magasinage en ligne.

6.3 Composants du système

Nous avons développé un nouveau site Web appelé « **PAYCTRI** » représentant quatre boutiques virtuelles en ligne : *CostKi, wemalt, Best Shop, Z-mazon*. Le site est conçu comme un système à trois composants comme indiqué à la Figure 21. Les composants du système peuvent être illustrés comme suit : l'interface utilisateur (*User Interface ou UI*), le Back-end (*Back-end*) et la Passerelle (*Gateway*).

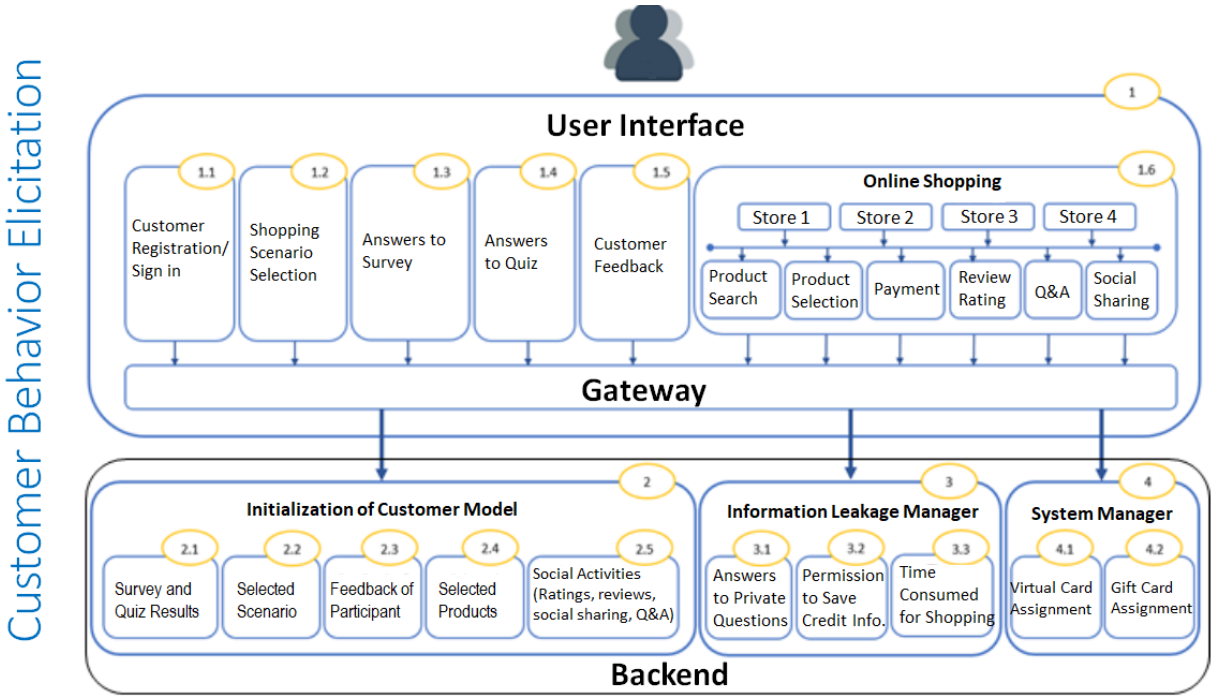

Figure 21 - Customer Behavior Elicitation

Le composant ***User Interface*** (1) est la première interface qui interagit en ligne avec le participant. Elle comprend les sous-composants suivants : inscription/ouverture de session du client (1.1), sélection du scénario d'achat (1.2), questions d'enquête avant et après l'expérience (1.3), quiz à choix multiples sur la cybersécurité (1.4), rétroaction du client (1.5). L'interface de magasinage en ligne (1.6) comprend quatre magasins en ligne

où l'utilisateur peut effectuer diverses tâches telles que la recherche et la sélection de produits, le paiement, les revues et évaluations, les Questions et Réponses (Q&A), et le partage social. Tous ces sous-composants sont ajoutés pour faciliter l'expérience.

Le deuxième composant est l'interface ***Back-end*** du système. Elle comprend l'initialisation du modèle client (2), le gestionnaire des fuites d'informations (3) et le gestionnaire du système (4).

L'initialisation du modèle client (2) comprend tous les résultats qui sont en relation avec les interactivités du participant durant l'expérience. Ceci inclut:

- Les réponses au sondage et les résultats du questionnaire (2.1).
- Les procédures de supplément pour sauvegarder le scénario sélectionné (2.2).
- Les commentaires des participants (2.3)
- Les produits sélectionnés (2.4).
- Les activités sociales sur Facebook, Twitter, Instagram et Pinterest (2.5).

Le *gestionnaire des fuites d'informations* (3) comprend tous les résultats qui sont en relation avec le comportement des participants envers les informations financières et personnelles. Ceci inclut :

- Les réponses aux questions privées (3.1).
- La permission ou le refus de sauvegarder les données de crédit (3.2).
- Le temps consacré au magasinage (3.3).

Le *gestionnaire de système* (4) comprend tous les résultats qui sont en relation avec les montants utilisés durant l'expérience, ceci inclut :

- Les montants de crédit (4.1)
- Les montants des cartes-cadeaux (4.2).

Le troisième composant, c'est le ***Gateway***. Cette partie joue le rôle d'inter logiciel (ou ***middleware***) entre les composants et est utilisée pour résoudre des problèmes liés à la

connectivité et à la traduction de protocoles pour permettre la compatibilité entre les éléments (Mukherjee*, et al.*, 2017).

Pour simuler l'expérience de magasinage en ligne, nous avons invité des participants à accéder à notre site Web, et nous les avons informés de leurs responsabilités et de leurs tâches. Nous avons permis aux participants de quitter l'expérience en tout temps à leur convenance. Dans la prochaine section, nous expliquerons plus en détail l'expérience en ligne et la méthodologie adoptée ainsi que les limites de notre travail.

6.4 Développement de l'expérience

Après avoir décrit la structure du site développé, nous avons invité les participants à magasiner et à pratiquer l'expérience en ligne. Au total, 103 participants ont accédé à notre nouveau site Web et ont expérimenté la même interface. Ils ont été exposés au même environnement en ligne et ont été invités à choisir n'importe quel scénario d'achat à partir d'une liste de quatre situations citées comme suit :

Scénario A: "*You are very busy this week, because of the biggest happening this year. You need to shop for groceries and some other necessities for the whole week. You won't have enough time during the day, so you decide to shop online*".

Scénario B: "*You receive a call from your partner. Good news. He/She is free tomorrow night. Therefore, you decide to invite him/her for dinner. There is not enough time to go shopping. You have taken time to think of what to prepare. Now, this is time to go shopping online*".

Scénario C: "*It has been long time you did not visit your family. You decide to go home to see them. Many childhood memories come to your mind. During this week, you will be surrounded by your beloved ones, and you want to bring with you some gifts. Time to go shopping online*".

Scénario D: "*Your home needs new decoration. Your budget is limited, and you cannot afford a big change. So you decide to buy online new items for your room*".

Par conséquent, nous avons différentes pratiques d'achat étant donné un scénario.

L'expérience en ligne se déroule dans un certain ordre et suit des étapes énumérées dans la Figure 22. Les tâches à accomplir varient entre répondre à un sondage, tester le niveau de connaissances en cybersécurité, interagir avec les pages Web, sélectionner un scénario, choisir un ou plusieurs magasins, chercher des produits, examiner les détails et les caractéristiques, ajouter des commentaires, poser des questions, partager des images sur les médias sociaux et ajouter, retirer des articles du panier et payer. Les objectifs sont d'abord d'initialiser le modèle client à travers les sondages (préexpérience et post-expérience) et ensuite d'observer le comportement des utilisateurs pendant le magasinage (*Information Leakage*).

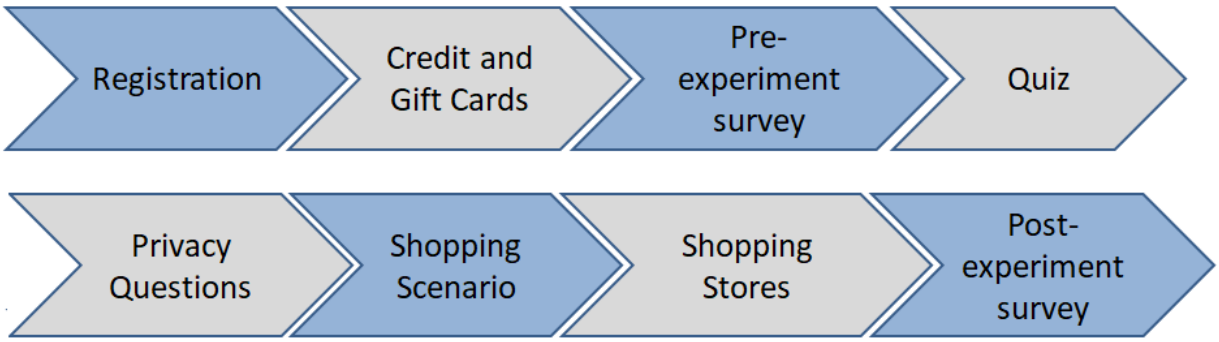

Figure 22 - Étapes de l'expérience en ligne

Au début, chaque participant s'inscrit pour la première fois. Nous avons demandé un pseudonyme et un identifiant de connexion avec un mot de passe (voir Figure 23). Une fois l'inscription terminée, le participant se connecte automatiquement au site Web en utilisant son nom d'utilisateur ou son identifiant et démarre l'expérience d'achat décrite ci-dessous.

Après s'être connecté, le participant reçoit une carte de crédit virtuelle. Aléatoirement, il peut gagner une carte-cadeau valide pour un magasin et avec un crédit initial. Sur la même page Web, le participant peut voir ses transactions et a la possibilité d'enregistrer ou non les informations de sa carte de crédit (voir Figure 24). Ensuite, il navigue sur le site Web et répond à l'enquête préexpérience sur ses informations démographiques telles que le genre, l'âge, le niveau d'éducation et l'occupation.

Let's go shopping

This work is a part of a scientific study on Online Payment Experience and Privacy. Beside shopping experience, you will learn also some potential keys about security in online browsing and online payment. Two surveys are to be responded during our journey. The first one is to be answered at the beginning of the experience and another one at the end. Be sure that all information exchanged in the website is confidential. Your identity and the collected information will not be shared with any inappropriate entity and will be stored in a secure location. Results are to be extracted anonymously and cannot in any way identify you as participant. All exchanges with *social media, online payments, comments and reviews* are exclusively restricted to our website (Not Connected to Real Social Network).
We are looking forward to learning with you in this online journey and getting innovative experiences.

Figure 23 - Page d'enregistrement

La prochaine étape consiste à répondre à un quiz avec choix multiples et comprend 16 questions qui aident à évaluer le niveau de connaissance sur la cybersécurité (navigation sécurisée, paiement en ligne, connexion Internet, etc.). Les questions sont inspirées du *questionnaire sur les aspects humains de la sécurité de l'information* (*The Human Aspects of Information Security Questionnaire* ou *HAIS-Q*)**,** qui est un instrument conçu pour mesurer la sensibilisation à la sécurité de l'information (SIA) (Y. Chen*, et al.*, 2015; Kittur*, et al.*, 2008). Notons que le HAIS-Q comprend sept domaines d'intérêt : utilisation d'Internet, utilisation des courriels, utilisation des médias sociaux, gestion des mots de passe, le signalement des incidents, le traitement de l'information, l'informatique mobile et le modèle de connaissance, d'attitude et de comportement (*Knowledge-attitude-behavior or KAB model*) (Y. Chen*, et al.*, 2015).

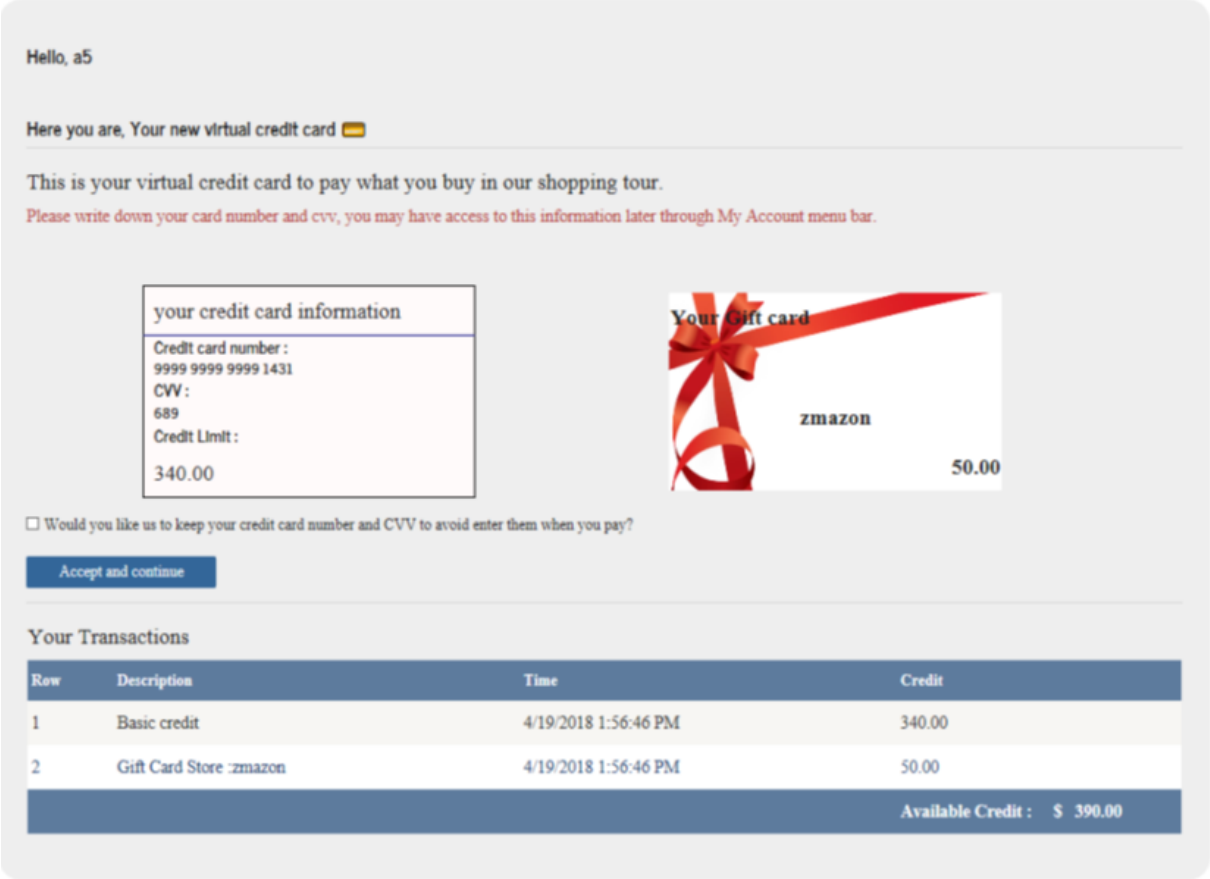

Figure 24 - Page de la carte de crédit et carte cadeau

Après le quiz, les participants ont été invités à répondre à huit questions offrant plus de crédits sur des conditions spécifiques de divulgation de la vie privée. Les questions portent sur leur adresse courriel, leur nom Facebook et Instagram, leur numéro de téléphone et les renseignements de leurs amis comme les adresses électroniques et le numéro d'identification Instagram.

En suivant les étapes ci-dessus, le participant sélectionne un scénario d'achat à partir d'une liste de quatre scénarios décrits précédemment. Après la sélection du scénario, le participant s'engage dans une pratique d'achat complète. Quatre magasins différents étaient disponibles sur le site : *CostKi, wemalt, Best Shop, Z-mazon*. La Figure 25 montre le scénario choisi et la liste des magasins disponibles.

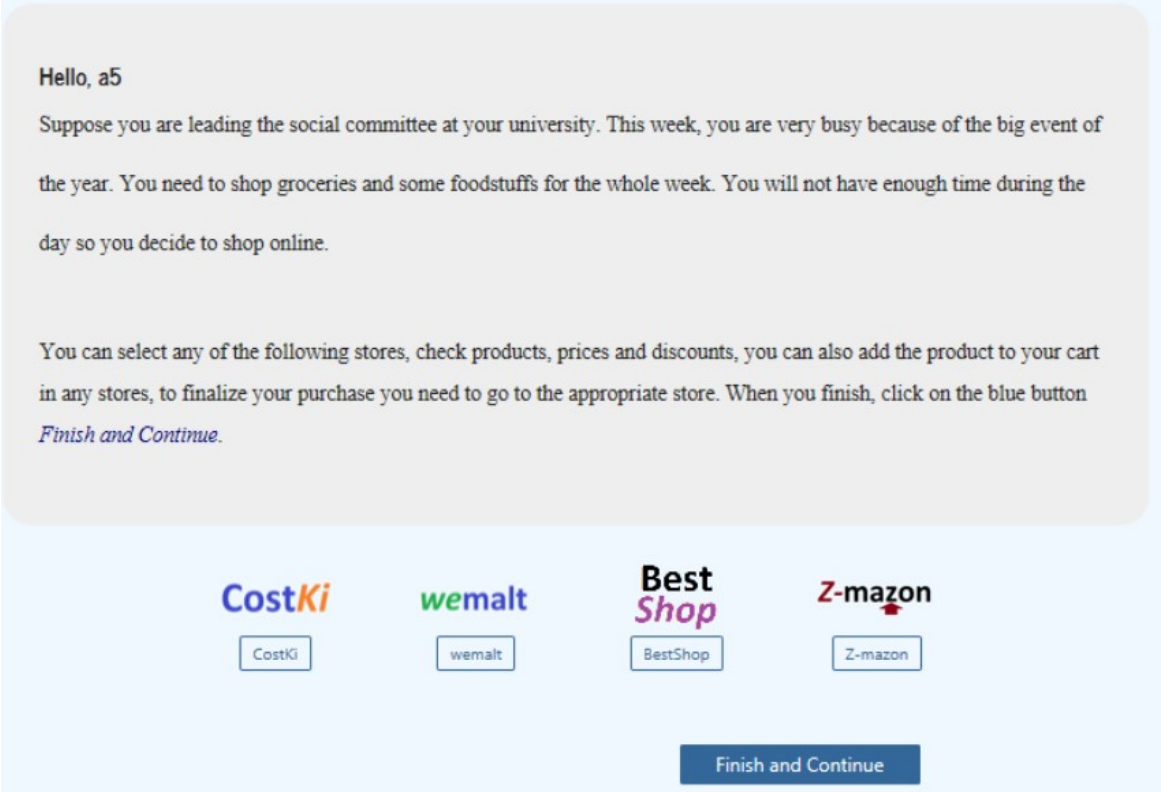

Figure 25 - Affichage du scénario et choix du magasin

Dans chaque boutique, le participant peut visualiser, rechercher, sélectionner n'importe quel produit nécessaire et l'ajouter à son panier. De plus, le participant peut voir les images, le prix, la remise, les commentaires et les rétroactions, les questions et les réponses, et les caractéristiques du produit. La Figure 26 montre l'article sélectionné du magasin *Wemalt* avec le prix et les caractéristiques. De plus, le participant peut virtuellement partager de l'information sur n'importe quel produit dans un réseau social simulé comme Twitter, Facebook et Instagram.

À la fin de l'expérience, le site Web demande au participant de conclure le paiement par carte de crédit et affiche ensuite la page du sondage. Le participant doit répondre à l'enquête post-expérience, ce qui nous a aidés à recueillir des données réelles.

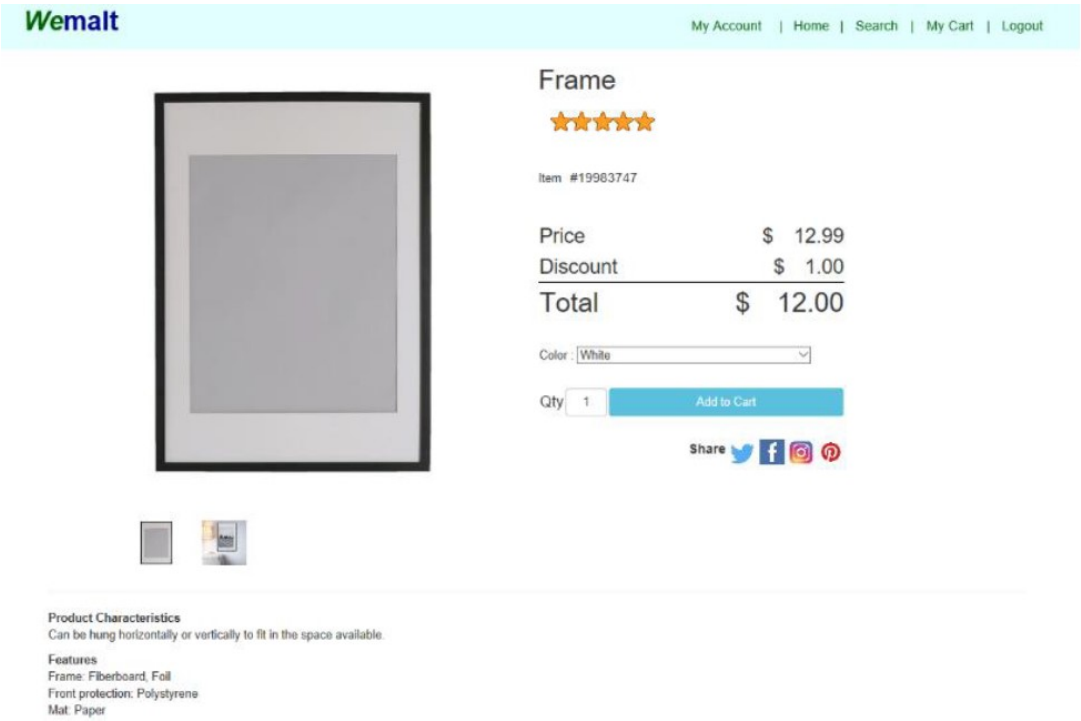

Figure 26 - Page d'affichage du produit sélectionné

Prenons l'exemple des participants **A843** (représenté par Fred) et **A940** (représenté par Bob). Au début, Fred et Bob s'inscrivent pour la première fois.

Après s'être connecté, Fred reçoit une carte de crédit virtuelle de 340$. Aléatoirement, Fred a gagné une carte-cadeau pour le magasin Costki de 70$. Sur la même page Web, Fred a vu l'historique de ses transactions et enregistre ses informations de sa carte de crédit. Ensuite, il navigue sur le site Web et répond à l'enquête préexpérience sur ses informations démographiques telles que le genre, l'âge, le niveau d'éducation et l'occupation. Arrivé au quiz, Fred l'accomplit et en conséquence 5 questions sur 16 sont correctes. Donc Fred ne possède pas un niveau de connaissance en cybersécurité assez élevé. Après le quiz, le système affiche huit questions offrant plus de crédits sur des conditions spécifiques de divulgation de la vie privée. Fred accepte de divulguer son courriel, son numéro d'identification sur Facebook. Par conséquent, Fred aura 25$ de crédits de plus. Il choisit le scénario C et s'engage dans une pratique d'achat complète.

Après s'être connecté, Bob reçoit une carte de crédit virtuelle de 260$. Aléatoirement, Fred a gagné une carte-cadeau pour le magasin Wemalt de 50$. Sur la même page Web, Fred a vu l'historique de ses transactions et enregistre ses informations de sa carte de crédit. Ensuite, il navigue sur le site Web et répond à l'enquête préexpérience sur ses informations démographiques telles que le genre, l'âge, le niveau d'éducation et l'occupation. Arrivé au quiz, Bob l'accomplit et en conséquence 13 questions sur 16 sont correctes. Donc Bob possède un niveau de connaissance en cybersécurité assez élevé. Après le quiz, le système affiche huit questions offrant plus de crédits sur des conditions spécifiques de divulgation de la vie privée. Bob n'accepte de divulguer aucune information. Par conséquent, Bob n'aura aucun crédit de plus. Il choisit le scénario D et s'engage dans une pratique d'achat complète.

Le Tableau 8 montre les deux exemples illustrés.

Tableau 8 - Exemple d'exécution de l'expérience

Participant	**Produits achetés**	**Niveau de connaissance en cybersécurité**	**Scénario choisi**	**Crédit en total**
Fred	Picture, set of 3, animals	5 sur 16 questions correctes	C	435$
	Collage frame for 8 photos			
	Picture, set of 3, animals			
	Picture, set of 3, animals			
	Zavida® - Colombian Whole Bean Coffee 2 x 5 lb Bags			
	Duvet cover and pillowcase(s)			
	Duvet cover and pillowcase(s)			
	Premium Quality Loose Leaf Green Tea			
	Premium Quality Loose Leaf Green Tea			
	Premium Quality Loose Leaf Green Tea			
	Premium Quality Loose Leaf Green Tea			
	Premium Quality Loose Leaf Green Tea			
	Floor lamp			
Bob	Tropical gold pineapple	13 sur 16 questions correctes	D	310
	Black Angus Kangaroo Ground Meat			
	Wall clock			

Avant de communiquer les résultats de la corrélation, nous décrivons d'abord les données recueillies au cours de l'expérience dans la section suivante.

6.4.1 Données collectées

Pour recueillir des données, nous avons invité les participants par courriel et dans les médias sociaux à accéder à notre site Web et à commencer l'expérience. De plus, nous avons recruté d'autres personnes grâce à la plateforme **Amazon Mechanical Turk (*MTurk*)**[15]. Au total, 103 participants ont répondu au sondage et ont complété l'expérience.

Dans le cadre de l'enquête préalable à l'expérience, les participants ont fourni des renseignements démographiques tels que le sexe, l'âge, le niveau d'éducation, la profession, le revenu annuel et le pays de résidence, en plus de la moyenne mensuelle des achats en ligne et de la fréquence des achats en ligne, comme le montre le Tableau 9.

L'âge moyen des participants se situait entre 31 et 35 ans, avec 60 hommes et 40 femmes, en plus de 3 participants qui n'ont pas répondu à la question sur le sexe. Presque tous les participants ont déclaré être très familiers avec le magasinage en ligne, 49,5 % indiquant qu'ils magasinent plus de dix fois par année et 30,1 % de 6 à 10 fois par année.

Tableau 9 - Données démographiques des participants

Demographic Information	Category	Total	%
N = 103			
Gender	Male	60	58.3
	Female	40	38.8
	I prefer not to answer	3	2.9
Age	18 – 25	13	12.6
	26 – 30	17	16.5
	31 – 35	32	31.1
	36 – 40	17	16.5
	41 – 45	10	9.7
	45 – 50	5	4.9
	Above 50	6	5.8
	I prefer not to answer	3	2.9
Education	Junior High/Middle School	0	0
	High School	20	19.4
	Technical/trade school	12	11.7

[15] https://www.mturk.com/ consulté le 26/Oct./2019

	Bachelor's degree	51	49.5
	Master's degree	11	10.7
	Doctoral degree	2	1.9
	I prefer not to answer	4	3.9
	Other	3	2.9
Occupation	Student	16	15.5
	Employee	56	54.4
	Business owner/Self-employed	9	8.7
	Manager/official	8	7.8
	Researcher	2	1.9
	Homemaker	2	1.9
	Retired	0	0
	Unemployed	1	1.0
	Other	7	6.8
	I prefer not to answer	2	1.9
Annual income (in cad $)	Less than 39,999	42	40.8
	Between 40,000 and 64,999	27	26.2
	Between 65,000 and 99,999	14	13.6
	Between 100,000 and 119,999	2	1.9
	Above 120,000	4	3.9
	I prefer not to answer	14	13.6
	Above 3500 by month	1	1.0
Living Country	Canada	19	18.4
	India	9	8.7
	Italy	1	1.0
	Sri Lanka	1	1.0
	Thailand	1	1.0
	United Kingdom	1	1.0
	The United States	63	61.2
	I Prefer not to answer	8	7.8
Online shopping monthly Average (in cad $)	I never buy online	3	2.9
	Less than 499 by month	81	78.6
	Between 500-1499 by month	17	16.5
	Between 1500-3499 by month	1	1.0
	Above 3500 by month	1	1.0
Online Shopping Frequency	Between 1 and 5 times per year	19	18.4
	Between 6 and 10 times per year	31	30.1
	More than 10 times per year	51	49.5
	Never	2	1.9

Dans l'enquête post-expérience, les questions ont été mesurées sur une échelle de Likert en 5 points, allant de fortement en désaccord (1) à fortement en accord (5), avec (3) comme pas de decision. Le Tableau 10 présente les variables, les questions des éléments, la moyenne, l'écart-type (ET) et le coefficient de cohérence interne (Alpha de Cronbach représenté par α). Selon Nunally (1978), le coefficient Alpha de Cronbach est considéré comme acceptable dépassant le 0.60 pour tous les construits. Ce qui est valide dans notre cas.

Tableau 10 - Questionnaire Post-Expérience

Constructs	**Items**	**Mean**	**SD**	α
User Trust (TR)	TR1. In general, I trust other people.	3.28	1.061	0.882
	TR2. In general, I tend to count on other people.	3.13	1.177	
	TR3. In general, I have faith in humanity.	3.47	1.065	
	TR4. In general, I trust other people unless they give me the reason not to.	3.67	1.070	
Social Behavior (SB)	SB1. In general, I do not share my location on social media.	4.06	1.083	0.598
	SB2. In general, I do not accept invitations from strangers on social media.	4.33	0.964	
	SB3. In general, I do not send personal information to strangers on social media.	4.58	0.799	
Online Trust (OT)	OT1. In general, Internet websites are safe environments in which to exchange information with others.	2.46	1.136	0.867
	OT2. In general, Internet websites are reliable environments in which to conduct transactions.	2.95	1.088	
	OT3. In general, Internet websites are trustworthy environments to handle personal information.	2.56	1.126	
	CC1. I am concerned about cybersecurity.	4.20	0.878	0.845

Cybersecurity Concern (CC)	CC2. I like to know more about cybersecurity.	4.08	0.871	
	CC3. I seek information about cybersecurity.	3.81	1.121	
	CC4. I like to know more about cybersecurity.	3.68	1.050	
Cybersecurity Awareness (CA)	CA1. I think it is difficult to spot the signs of a cyber-attack.	2.98	1.180	
	CA2. I think it is difficult to prevent a cyber-attack.	3.10	1.089	0.718
	CA3. I think it is hard to predict the consequences of a cyber-attack.	3.51	1.047	
Privacy Concern (PR)	PR1. I am concerned about my privacy over the internet.	4.26	0.700	
	PR2. I am concerned that the information I submit on the Internet could be misused.	4.13	0.836	
	PR3. I am concerned that a person can find private information about me on the Internet.	4.13	0.788	0.871
	PR4. I am concerned about submitting information on the Internet because it could be used in a way I did not foresee.	4.16	0.860	
Online Payment Trust (OP)	OP1. I pay online when I trust the website.	4.44	0.572	
	OP2. I pay online when the company/merchant on the website is trustworthy.	4.39	0.581	0.823
	OP3. I pay online when the company/merchant behind the website has a good reputation.	4.25	0.682	
Online Payment Security (PS)	PS1. I pay online when there are clear security signs on the website.	4.28	0.833	
	PS2. I pay online when the connection to the internet is secure.	4.32	0.703	0.730
	PS3. I pay online when the access to the internet is not free-to-access public Wi-Fi.	4.17	0.879	

De même, nous déterminons une statistique descriptive telle que montrée dans le Tableau 11. Ces données ont été extraites en fonction du comportement et des réponses du participant pendant l'expérience, comme le scénario sélectionné, les connaissances en cybersécurité et l'acceptation de conserver ou non les renseignements sur la carte de crédit.

Nous calculons les connaissances en cybersécurité en fonction du total des bonnes réponses (=8 ou >8). Ces résultats extraits de l'expérience enrichissent notre travail. Dans l'ensemble, ils montrent que les participants ont acheté différents types d'articles de notre site Web. De plus, il est démontré que les participants ont ajouté à leur panier un total de 392 articles appartenant à plusieurs catégories telles que lampes, viandes, meubles, décorations et autres. La Figure 27 montre une représentation graphique de cette diversité.

Tableau 11 - Statistiques descriptives

Items descriptifs	Category	Total	%
N = 103			
Shopping Scenario	Scenario A	19	18.4
	Scenario B	34	33.0
	Scenario C	10	9.7
	Scenario D	40	38.8
Cybersecurity Knowledge	<=50%	15	14.6
	> 50%	88	85.4
Save Credit Card Information	False	23	22.3
	True	80	77.7

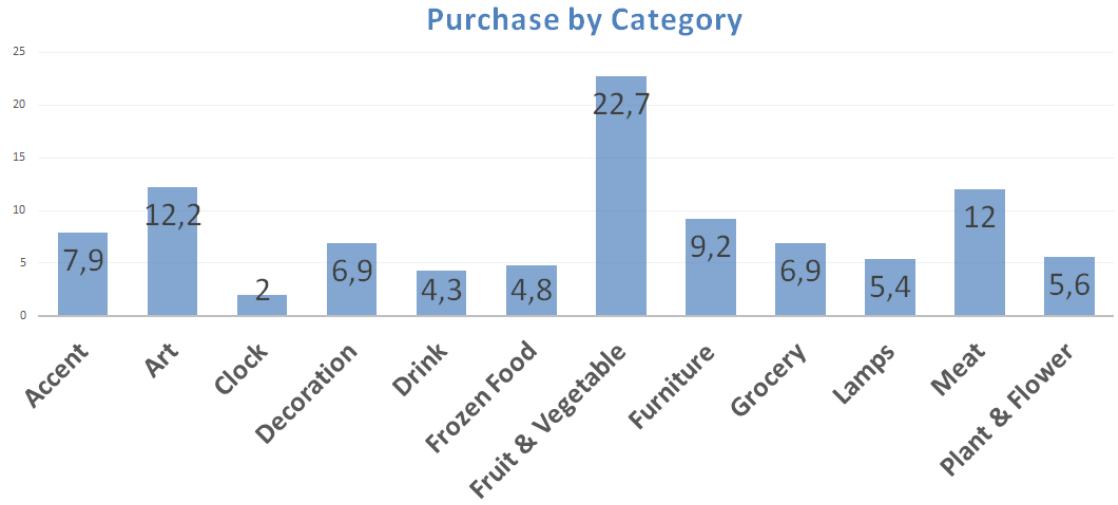

Figure 27 - Les achats par catégorie de produits

6.4.2 Limitations de la recherche

Notre recherche a certaines limites qui ne peuvent être ignorées. La première est liée à la diversité des produits. Dans notre site Web, le nombre et le type de produits sont limités, ce qui a une incidence sur les choix des participants pour réaliser le scénario choisi (A, B, C ou D). La deuxième limite est liée à notre incapacité à observer les participants pendant l'expérience et leurs réactions sur le site depuis le lancement de l'expérience sur Internet. En ce qui concerne la plateforme *Mturk*, la limite tient à la restriction de la plage de temps pour l'affectation des participants et de l'absence de soutien robuste pendant l'expérience. Néanmoins, elle peut fournir des résultats aussi pertinents que ceux des méthodes d'enquête traditionnelles (Kittur*, et al.*, 2008).

Après avoir revu le développement de l'expérience en ligne, les données collectées ainsi que les limites de notre travail, la section suivante présente les résultats et les constatations.

6.5 Résultats et constatations

Ce travail vise à renforcer la cybersécurité et à extraire des facteurs qui affectent la perception de sécurité dans un contexte de magasinage en ligne. Notre objectif est d'inciter les participants à chercher de nouvelles façons et approches pour assurer un niveau adéquat de connaissances sur la cybersécurité. Nos constatations, fondées sur le sondage post-expérience, soulignent les aspects pertinents de la perception des risques, de la confiance, du comportement social, de cybersécurité, de la vie privée et de la sécurité des paiements en ligne. *La confiance chez l'utilisateur (TR), le comportement social (SB), la confiance en ligne (OT), la préoccupation en cybersécurité (CC), la sensibilisation en cybersécurité (CA), la perception de protection de vie privée (PR), la confiance en paiement en ligne (OP) et la perception de la sécurité des paiements en ligne (PS)* représentent nos huit variables prédictives.

Dans cette expérience, notre intérêt consiste à vérifier si les connaissances en cybersécurité, le scénario choisi et la perception de protection de vie privée sont corrélés à ces facteurs déterminés. Pour atteindre ces objectifs, les données de notre expérience fournissent un résultat valide fondé sur les poids de régression extraits et normalisés avec

les valeurs estimées (**Estimate**), l'erreur-type (**S.E.**), le Critical Ratio (**C.R.**) et le niveau de probabilité (**P**). Le Tableau 12 montre ces valeurs et relie les variables prédictives aux variables dépendantes.

Tableau 12 - Regression Weights (P-value *** p< 0.001)

Construct	**Items**	**Estimate**	**S.E.**	**C.R.**	**P**
TR	TR4	1			
TR	TR1	1.07	0.103	10.359	***
TR	TR3	0.88	0.109	8.1	***
TR	TR2	1.036	0.118	8.808	***
SB	SB3	1			
SB	SB1	1.195	0.379	3.152	0.002
SB	SB2	1.077	0.341	3.155	0.002
OT	OT2	1			
OT	OT3	1.137	0.116	9.838	***
OT	OT1	0.968	0.115	8.397	***
CC	CC3	1			
CC	CC4	0.833	0.078	10.627	***
CC	CC2	0.665	0.066	10.001	***
CC	CC1	0.464	0.078	5.924	***
CA	CA2	1			
CA	CA1	1.23	0.263	4.669	***
CA	CA3	0.723	0.165	4.375	***
PR	PR4	1			
PR	PR3	0.855	0.086	9.939	***
PR	PR2	0.973	0.089	10.993	***
PR	PR1	0.597	0.085	7.051	***
OP	OP2	1			
OP	OP1	0.938	0.112	8.386	***
OP	OP3	0.968	0.133	7.292	***
PS	PS1	1			
PS	PS3	1.371	0.271	5.064	***
PS	PS2	1.61	0.309	5.208	***

Prenons l'exemple de la variable prédictive TR (*La confiance chez l'utilisateur*) avec les variables dépendantes TR1, TR2, TR3 et TR4 dont chacune représente une question dans le questionnaire Post-Expérience (voir Tableau 10). Pour mettre l'accent sur le profil des participants, notre interface en ligne offre l'option de gagner plus de crédits en répondant aux huit questions sur la divulgation de la vie privée.

Les réponses présentées au Tableau 13 reflètent également leur perception de protection de vie privée et nous donnent des résultats sur les attitudes des utilisateurs lorsqu'ils traitent des renseignements personnels. Pour simplifier, nous avons récupéré les réponses et effectué une analyse des résultats pour chaque réponse A [0, 1] où « 0 » signifie que le participant garde les huit questions sans aucune réponse (c.-à-d. qu'il n'a pas saisi aucun renseignement personnel), et « 1 » signifie que le participant a répondu au moins à une question. Ainsi, deux nouvelles variables *OPD* (Own Privacy disclosure**)** et *FPD* (Friend's Privacy disclosure**)** sont créées pour refléter respectivement la divulgation de la vie privée personnelle et celle des amis.

Tableau 13 - Réponses sur les questions de vie privée

Items Descriptive	**Response**	**#**	**%**
N = 103			
Give Email Address	False	52	50.5
	True	51	49.5
Enter Facebook Id	False	68	66.0
	True	35	34.0
Enter Instagram ID	False	80	77.7
	True	23	22.3
Enter Phone number	False	67	65.0
	True	36	35.0
Give Permission to Import Facebook contacts	False	92	89.3
	True	11	10.7
Own Privacy disclosure (OPD)	**False**	**47**	**45.6**
	True	**56**	**54.4**
Enter Some Friends Emails	False	80	77.7
	True	23	22.3
Enter Some Friends Instagram ID	False	85	82.5
	True	18	17.5
Friend's Privacy disclosure (FPD)	**False**	**80**	**77.7**
	True	**23**	**22.3**

6.6 Discussion

L'objectif de ce travail est d'élargir les constatations qui contribuent, de plusieurs façons, aux recherches dans les analyses des perceptions et des comportements des usagers en ligne. Deux analyses distinctes sont précisément interprétées. Dans la première analyse, les participants sont divisés en deux groupes en fonction de leur **divulgation sur leur vie privée** (*OPD*). Dans la deuxième analyse, les participants sont divisés en deux groupes en fonction de **leur épreuve des bonnes réponses au test de connaissance en cybersécurité**. En résumé, par l'intermédiaire de l'analyse de la variance (ANOVA), nos constatations sont les suivantes :

Notre première analyse indique que les participants, qui n'ont fourni aucun renseignement privé suite à l'échange avec des crédits (ceux qui n'ont pas coché la question dans la Figure 28) et dont la valeur de **divulgation sur leur vie privée** (*OPD*) est fausse, sont plus susceptibles de percevoir une préoccupation élevée en matière de protection de vie privée (PR) ($p = 0{,}017 < 0{,}05$). Ce résultat souligne les constatations antérieures concernant le niveau de connaissance de la cybersécurité, qui est un facteur significatif dans l'adoption du comportement des consommateurs lorsqu'ils décident du degré de risque qu'ils sont prêts à prendre (van Schaik*, et al.*, 2017). Supposons que Bob se préoccupe de sa vie privée, il va dénoncer à tout profit en échange de ses informations personnelles.

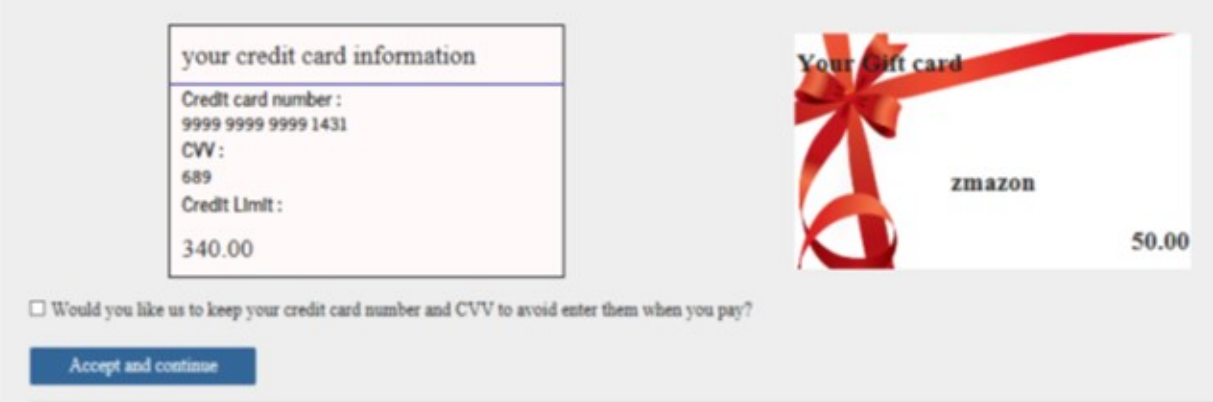

Figure 28 - Question d'échange de renseignements privés des crédits

En ce qui concerne la deuxième analyse, les résultats montrent que le niveau de connaissance en cybersécurité a un effet significatif sur **la confiance en ligne** (*OT*) ($p =$

0,001 < 0,01). Par exemple, les participants qui ont donné des réponses correctes à moins de 50 % des questions de cybersécurité sont plus susceptibles de faire confiance au site Internet et de le considérer comme un environnement sécuritaire. Nos constatations mettent l'accent sur le concept de confiance en ligne. En général, avec la confiance, les internautes ne perçoivent pas un risque élevé pendant les services en ligne et sont plus susceptibles de les utiliser (Riek*, et al.*, 2016). Prenons l'exemple de Fred qui a une confiance envers Costco comme étant un vendeur fiable en ligne. En prenant son café, Fred se connecte au Wifi du restaurant et effectue des achats en ligne par l'intermédiaire de sa carte de crédit. Vu que Fred possède un niveau de connaissance en cybersécurité qui n'est pas très élevé, il ne se rend pas compte que la connexion de Wifi n'est pas sécurisée malgré que le site de *CostKi* le soit. Ce qui expose ses informations financières à une activité vulnérable sans qu'il le sache.

En revanche, une déduction importante au sujet de la protection de la vie privée est digne d'être mentionnée. Le niveau de connaissances en cybersécurité a un effet important sur **la perception de protection de vie privée** (*PR*). Par exemple, les participants qui ont obtenu plus de 50 % de réponses correctes aux questions de cybersécurité sont plus susceptibles de percevoir une préoccupation élevée en matière de protection de vie privée (PR) (p = 0,000004 < 0,001).

Autre que la perception de protection de vie privée, le niveau de connaissance en cybersécurité a également un effet significatif sur **la préoccupation en cybersécurité** (*CC*) (p = 0,011 < 0,05). Par exemple, les participants qui ont obtenu plus de 50 % de réponses correctes sur les questions du quiz sont également préoccupés par le sujet de cybersécurité, donc il est essentiel de mentionner l'impact des cybercrimes sur la déviation des services en ligne. En effet, ce risque rend les consommateurs réticents à poursuivre leurs activités en ligne (Riek*, et al.*, 2016). Par exemple, si Bob possède un niveau de connaissance considérable en cybersécurité, il se préoccupe davantage à conserver précieusement les données de paiement et les renseignements de ses comptes.

De plus, le niveau de connaissance en cybersécurité a un effet significatif sur **la perception de la sécurité des paiements en ligne** (*PS*) (p = 0,036 < 0,05). Les signes de sécurité et les connexions sécurisées sont la principale préoccupation des organisations de

réglementation puisque les activités en ligne peuvent de plus en plus conduire à des violations de la sécurité par les criminels (van Schaik*, et al.*, 2017). Par exemple, si Bob possède un niveau de connaissance en cybersécurité assez élevé, il sera plus compétent à cerner les aspects de sécurité dont il doit se préoccuper davantage dans les paiements en ligne. Ceci dit, il pourra facilement repérer les attaquants potentiels en ligne, leurs cibles et leurs techniques telles que les courriels d'hameçonnage, les sites non sécurisés, les messages d'erreurs imprévus.

Une autre incidence de connaissances en cybersécurité doit être admise sur le **comportement social** du consommateur (*SB*) ($p = 0{,}041 < 0{,}05$). Étant donné que la sécurité de l'information et la protection de la vie privée constituent les principales préoccupations dans les réseaux sociaux (Soomro*, et al.*, 2016), la perception du risque des internautes est réduite lorsqu'ils croient comprendre les risques sous-jacents (van Schaik*, et al.*, 2017).

En ce qui concerne la confiance en général, l'analyse nous fournit la preuve que les connaissances en cybersécurité n'ont aucune incidence sur la **confiance de l'utilisateur** (*TR*) ($p = 0{,}241 > 0{,}05$). Ce résultat montre plus précisément que la confiance n'est pas affectée par le niveau de connaissance en cybersécurité.

En outre, une autre constatation très intéressante de ce travail est que les connaissances en cybersécurité n'ont aucune incidence sur **la confiance en paiement en ligne** (*OP*) de l'utilisateur ($p = 0.464 > 0.05$). À cet égard, nous différencions la confiance en ligne lorsque les utilisateurs considèrent que les sites Web pourraient être fiables et sécuritaires pour échanger de l'information avec d'autres paires, et lorsqu'ils établissent des échanges avec des commerçants ou des sites dignes de confiance. Ce résultat met également en évidence l'analyse du comportement de l'utilisateur à l'égard de l'option « **Conserver l'information de la carte de crédit** ». En fait, notre recherche confirme qu'il n'y a aucune corrélation avec les connaissances en cybersécurité.

De plus, les connaissances en cybersécurité n'ont aucune incidence sur **la sensibilisation en cybersécurité** (*CA*) ($p = 0{,}684 > 0{,}05$). Quel que soit leur niveau de connaissance en cybersécurité, les utilisateurs font toujours face à diverses sources de

cybermenaces et ne peuvent prévoir les conséquences, ils peuvent néanmoins minimiser leur impact (Reyns & Henson, 2016).

De plus, nos résultats démontrent que le scénario d'achat sélectionné n'est pas un prédicteur significatif du comportement du client ($p > 0,05$).

Les commentaires ajoutés à la fin de la session nous ont aidés à interpréter correctement le comportement de l'utilisateur pendant l'expérience. Voici quelques exemples : «L'expérience d'achat était vraiment amusante et fonctionnait très bien», «C'était amusant d'ajouter des choses à mon panier», « C'était plutôt amusant, mais la sélection de viande était horrible! », «Certaines questions ont trop peu de réponses. Parfois, il est difficile de choisir l'un des trois choix, car je pense que je ne ferais aucun des trois choix présentés. Il faudrait peut-être ajouter une option "Autre" avec une boîte de texte pour entrer une réponse personnalisée?», «Pourquoi ne puis-je pas utiliser ma carte-cadeau sans entrer d'information de crédit?», «Tout s'est bien passé», « Tout a bien fonctionné, et je n'ai eu aucun problème».

La section suivante conclut ce travail et présente des améliorations futures.

6.7 Conclusion et travaux futurs

La cybersécurité est un enjeu de plus en plus important touchant pratiquement toutes les activités et tous les domaines en raison de la numérisation croissante de nos solutions technologiques et surtout dans les paiements en ligne. Dans ce contexte, notre travail vise principalement à explorer le comportement des utilisateurs pendant les achats en ligne. Pour ce faire, nous avons mis en place un nouveau site Web appelé « PAYCTRI » stimulant une expérience de magasinage en ligne. Le déroulement de l'expérience comprend trois étapes principales. La première étape est un ensemble de questions inspirées du questionnaire sur les aspects humains de la sécurité de l'information (HAIS-Q) qui cible la sensibilisation à la sécurité de l'information. Ce questionnaire nous aide à évaluer le niveau de sensibilisation des participants à la cybersécurité. Le deuxième volet a exposé les participants à un ensemble de questions sur la divulgation de la vie privée. En faisant cela, la capacité de déduire la perception de protection de vie privée pourrait être utile pour remédier au manque de confiance qui existe dans les achats en ligne, comme la sauvegarde

du numéro de carte de crédit, l'échange de renseignements personnels pour obtenir des crédits. Le troisième composant intégrait la sélection de scénarios d'achats pour créer divers contextes d'achats en ligne. Les trois facettes mentionnées sont soutenues par une enquête (pré expérience et post-expérience) qui nous a aidés à collecter des données réelles (El Haddad, Shahab*, et al.*, 2018).

Notre recherche est utile pour les développeurs, ainsi que pour les fournisseurs qui mettent en place des solutions pour les sites d'achats en ligne. Pour résumer nos contributions, les résultats ont d'abord identifié le comportement de l'utilisateur en matière de confidentialité. Les participants qui sont très préoccupés par la protection des renseignements personnels n'ont fourni aucun renseignement personnel.

Deuxièmement, notre travail a déterminé un autre résultat qu'un niveau significatif de connaissances en cybersécurité a affecté la confiance en ligne, et a influencé le comportement social. Il a également eu une incidence positive sur la sécurité des paiements et a fait respecter les préoccupations relatives à la cybersécurité et à la protection de la vie privée. Cependant, la connaissance de la cybersécurité n'a eu aucun effet sur la confiance en général, plus explicitement dans la confiance en paiement en ligne et la sensibilisation à la cybersécurité.

Enfin, nos constatations indiquent que le scénario d'achat n'a eu aucun impact sur le comportement des utilisateurs. En conclusion, nous croyons que nos résultats suggèrent aux chercheurs de mieux comprendre la relation entre le comportement en ligne des clients, leur confiance en ligne, le sentiment de cybersécurité pour payer en ligne, ainsi que pour les praticiens pour améliorer les sites de magasinage existants.

Notre travail a plusieurs orientations futures. Premièrement, l'augmentation du nombre de participants nous aidera à valider les résultats existants et à améliorer nos constatations. Deuxièmement, notre analyse peut être améliorée en considérant d'autres caractéristiques, comme le contenu sémantique de l'information fournie dans les commentaires, dans l'examen du produit et dans la boîte questions/réponses. Adopter une autre perspective basée sur les questions de divulgation privée peut également constituer un défi pour certains travaux futurs pour conquérir le risque de manipulation en ligne et créer plus d'incitatifs pour le minimiser.

Chapitre 7 : Équilibre entre vie privée et utilité dans les systèmes de recommandation

Dans les systèmes de recommandation, les techniques de **filtrage collaboratif** (*Collaborative Filtering ou CF*) deviennent de plus en plus populaires avec l'évolution des sites d'achats en ligne (Jiang*, et al.*, 2019). Le filtrage collaboratif a pour principe d'exploiter les évaluations que des utilisateurs ont faites de certains articles, afin de recommander ces mêmes articles à des utilisateurs qui leur sont similaires, et sans qu'il soit nécessaire d'analyser le contenu de ces articles. La recommandation collaborative peut être implémentée en utilisant par exemple l'algorithme des *k* plus proches voisins. En conséquence, des questionnements au sujet de la protection de vie privée se posent : **comment protéger la vie privée des utilisateurs lorsqu'il est nécessaire de publier des données en masse pour des groupes communautaires ? Comment assurer un équilibre entre la divulgation des données et leur utilité pour le filtrage collaboratif tout en gardant une fiabilité dans les recommandations ? Comment gérer la publication des données tout en respectant la vie privée et surtout la divulgation de ces données est exigée par les systèmes de recommandation collaboratifs ?**

Afin d'adresser ces problématiques, nous proposons un nouveau modèle de protection de vie privée dans un contexte de filtrage collaboratif. Notre modèle est une extension du modèle de préservation de vie privée appelé « ***k*-coRating** » et basé sur la méthode de clustering « ***k*-means** ». Dans ce chapitre, nous évaluons premièrement le modèle *k*-coRating par rapport à la vie privée et à l'utilité des données. Ensuite, nous présentons nos solutions pour régler le problème d'équilibre entre les deux concepts. Enfin, nous comparons notre modèle à celui de « *k*-coRating » sous plusieurs aspects. Il apparait que notre modèle performe mieux que le modèle *k*-coRating existant en ce qui concerne l'utilité et la préservation de la vie privée (Xiang*, et al.*, 2019).

7.1 Systèmes de recommandation et vie privée

Parmi les innovations dans les systèmes de recommandation, nous pouvons citer les distributeurs de contenus audiovisuels, tels que Netflix, dont les services payants sont

accessibles par la diffusion en ligne sur différentes plateformes (ordinateurs, consoles de jeux vidéo, appareils mobiles, téléviseurs intelligents). Vu sa réputation, 151.5 millions d'abonnés en 2019[16], la compagnie investit des efforts considérables afin d'améliorer ses systèmes de recommandation et essaie d'atteindre un niveau de prédiction qui permettrait « *de connaître l'émission parfaitement exacte pour chaque abonné et débuter la lecture au moment où celui-ci lance Netflix* » (Amatriain & Basilico, 2016). En effet, l'historique des activités de visionnement, les habitudes de consommation de l'utilisateur (type d'appareil, moment de la journée, intensité de l'utilisation) et même les choix qui n'ont pas satisfait l'utilisateur font partie des données que recueille et analyse le système de recommandation de Netflix (Gomez-Uribe et Hunt, 2015).

En revanche, des chercheurs ont noté que les services offerts par Netflix deviennent un enjeu pour la vie privée, car ces derniers permettent l'accès en temps réel aux réactions des consommateurs devant les contenus visionnés (Keating, 2012). En septembre 2009 (Koren, 2009), l'équipe *BellKor 's Pragmatic Chaos* gagnait la compétition internationale organisée par Netflix pour avoir réussi à améliorer de 10,06 % l'efficacité de *Cinematch*, son système de recommandation[17]. À l'aide d'une attaque par inférence utilisant **Internet Movie DataBase** (*IMDB*) comme informations auxiliaires, une dé-anonymisation a été possible pour un nombre important d'enregistrements d'abonnés chez Netflix, bien qu'aucun identifiant n'ait été utilisé (Narayanan & Shmatikov, 2008). Les variables dont au moins une fonction des valeurs est connue sont alors appelées variables auxiliaires. Ce type d'information peut être donné par un recensement ou tout simplement par la base de sondage. On peut citer comme exemple d'information auxiliaire: le total d'un attribut sur la population, des sous-totaux selon des sous-populations, des proportions, des moyennes, des variances, les valeurs d'un caractère sur toutes les unités de la base de sondage. La notion d'information auxiliaire englobe donc toute donnée issue de recensements. En comparant les renseignements auxiliaires obtenus par les attaquants et les données publiées, le modèle pourrait soit réidentifier un utilisateur, soit dire qu'il ne figure pas dans les données diffusées. Dans le même contexte, un reportage a annoncé le 28 décembre 2009

[16] https://www.cnn.com/2019/07/17/media/netflix-earnings-2019-second-quarter/index.html consulté le 30/sep/2019

[17] https://www.netflixprize.com/ consulté le 06/Nov/2019

que **Netflix avait été poursuivi pour atteinte à la vie privée**. Malgré ceci, la base d'abonnés de Netflix augmente d'une façon fulgurante tous les jours.

La technologie qui consiste à extraire les données et de les partager en ligne est en plein essor. Par conséquent, l'exploration des méthodes pour assurer l'équilibre entre la vie privée et l'utilité des données est un défi permanent (F. Zhang*, et al.*, 2014).

Dans la littérature, des études scientifiques ont largement abordé les modèles de protection de vie privée (Ye*, et al.*, 2017; F. Zhang*, et al.*, 2018; Q. Zhang*, et al.*, 2017). Celles-ci ont tenté de classer les champs de l'enregistrement entre données non sensibles (loisir, travail) et données sensibles (nom, code postal, date de naissance, sexe) dans des ensembles appelés quasi identificateurs *(quasi identifié).* Par exemple, *K*-Anonymity (Sweeney, 2002) a proposé un modèle innovateur expliquant la vie privée en rendant difficile de distinguer un individu de l'autre. Ce processus d'anonymisation ou le retrait des identificateurs directs consiste à généraliser la valeur de ces champs quasi-identificateurs afin de rassembler les enregistrements en groupes dans lesquels les enregistrements sont indiscernables les uns par rapport aux autres. Le mécanisme d'anonymisation s'applique généralement sur les données avant de les publier. Toutefois, cette classification est heuristique et dépend de la **perception de vie privée de chaque utilisateur.** K-Anonymity, L-Diversity (Machanavajjhala*, et al.*, 2006) et T-Closeness (N. Li*, et al.*, 2007) ont offert une protection plus forte en tenant compte de la diversité et de la distribution des attributs des individus. Ils tentent ainsi de définir et d'étendre la protection de la vie privée sous différents aspects, mais il n'existait pas de définition officielle universelle de la vie privée avant l'apparition de la confidentialité différentielle (Dwork, 2008), qui offre un cadre théorique pour protéger la vie privée dans les bases de données statistiques.

De plus, des études antérieures ont proposé des modèles de protection de vie privée fondés sur le chiffrement (Bos*, et al.*, 2017; Raisaro*, et al.*, 2018; Wu*, et al.*, 2018), mais généralement, ces méthodes ne sont pas très pratiques si on tient compte du temps de calcul.

Cependant, ce traitement qui tente de rendre l'enregistrement de l'utilisateur anonyme implique une modification des données, ce qui conduit à une diminution de son

utilité. Par conséquent, un compromis entre la protection des renseignements personnels et l'utilité des données collectées est requis.

Dans ce contexte, des travaux ont proposé un modèle d'utilité pour le traitement des données adapté à un environnement de « **Fog computing** » (Cappiello*, et al.*, 2018). Cependant, il ne donne qu'une définition abstraite de l'utilité et n'est pas efficace dans la pratique. Dans une autre étude, les auteurs ont proposé une méthode d'anonymisation pour améliorer l'utilité des données pour la classification (Han*, et al.*, 2017), tandis que pour l'évaluation de l'utilité, ils l'évaluent en fonction du rendement de la classification, qui ne s'applique pas à tous les scénarios.

Dans le domaine des systèmes de recommandation, les données des utilisateurs sont reliées à leurs activités d'achats, à leurs préférences personnelles, à leurs historiques de navigation, et à leurs informations qui peuvent être sensibles. Idéalement, les fournisseurs comme Netflix devraient accorder une importance à la vie privée des utilisateurs autant qu'à l'utilité des données diffusées. Ainsi, nous nous intéressons dans ce chapitre à la protection de la vie privée tout en assurant l'utilité des données.

7.2 Méthodes basées sur k-coRated

Les préoccupations relatives à la protection de la vie privée dans la publication des données reçoivent de plus en plus une attention. Ces travaux ont donné lieu à plusieurs publications. Une étude de Li *et al.* (T. Li & Li, 2009) a offert une nouvelle perspective sur la publication de données. K. Chen *et al.* (K.-C. Chen*, et al.*, 2017) ont proposé une nouvelle façon d'évaluer l'utilité en fonction du cadre de protection des renseignements personnels différenciés. Johnson *et al.* (Johnson*, et al.*, 2018) ont proposé un compromis entre l'utilité des données à divulguer et les données à protéger dans le but de la protection de vie privée, sur l'ensemble des données collectées.

Le chiffrement/déchiffrement est une autre technique de préservation de la vie privée. Ce type de technique est appliqué dans un scénario de calcul distribué qui consomme beaucoup de temps. Il consiste à chiffrer les données originales avant d'être utilisées. Bien qu'une telle méthode puisse garantir l'exactitude des recommandations, son application comporte toutefois certaines limites. Il n'est pas pratique de chiffrer ou de

déchiffrer de grands ensembles de données et de nombreux calculs d'exploration de données qui ne peuvent être effectués par chiffrement ou déchiffrement. En conséquence, les périmètres d'utilisation sont restreints.

En outre, F. Zhang *et al.* (Ye*, et al.*, 2017; F. Zhang*, et al.*, 2014; F. Zhang*, et al.*, 2018) ont proposé un nouveau modèle de préservation de vie privée : ***k*-coRating,** inspiré de la technique de *k*-anonymity. Le concept du modèle consiste à remplacer certaines évaluations nulles par des scores « bien prédits » en améliorant l'utilité des données mesurées par l'exactitude des prédictions. Selon eux, les scores sont considérés « bien prédits » s'ils sont basés sur le critère de la confiance entre les utilisateurs ou la similarité selon la corrélation de Pearson. Le calcul de la moyenne des évaluations ou le choix des valeurs aléatoires pour remplir les évaluations nulles n'ont pas abouti à un résultat pertinent. Cependant, ils ont omis d'établir un équilibre entre la vie privée et l'utilité. Ce qui nous amène à présenter une amélioration du modèle ***k*-coRating.**

7.3 Méthodologie

Dans cette section, nous expliquons les étapes de notre méthodologie en commençant par une introduction du modèle ***k*-coRated**. Nous discutons ensuite ses inconvénients en ce qui concerne l'utilité et nous proposons notre modèle hybride inspirée de *k-coRated* et basée sur *k-means*. Par la suite, nous présentons plus en détail notre modèle.

7.3.1 Introduction

Le modèle *k*-coRated définit la vie privée de l'utilisateur à partir des éléments évalués sur le site Web. À la base, il est considéré empiriquement comme un modèle pour protéger les utilisateurs des attaques bien connues de Narayanan, qui ont prouvé la possibilité de réidentifier des abonnées chez Netflix suite à leur publication. Ces attaques ont montré qu'une dé-anonymisation est possible pour un nombre important d'enregistrements anonymes à l'aide du recoupement de données à partir d'autres sources d'information sur d'autres sites ou forums (Narayanan & Shmatikov, 2008). De plus, il permet de dissimuler les valeurs actuelles des appréciations dans des circonstances éventuelles. Toutefois, le modèle est adapté pour les évaluations à petite échelle, similaire au système de cotations à

5-étoiles. Ainsi, avec un système de cotations à grande échelle, il ne sera pas très efficace en ce qui concerne la protection de la vie privée. Nous montrons ci-dessous la définition de la vie privée *k*-coRated et les concepts raccordés.

Définition (Equivalence coRated) : D'après
(F. Zhang*, et al.*, 2014), deux utilisateurs $u, v \in U$ sont *coRated équivalents* si pour tout item $i \in I$, $u[i] = v[i]$ où $u[i]$ est définit comme suit :

Pour chaque utilisateur $u \in U$ et chaque item, $i \in I$, soit $R_{u,i}$ l'appréciation de l'utilisateur u pour l'item i :

$$u[i] = \begin{cases} 0, \text{ si } R_{u,i} = NULL \\ 1, si\ R_{u,i} \neq NULL \end{cases} \quad (1)$$

Cette dernière dérive une autre définition concernant la protection de la vie privée avec *k*-coRated :
Définition (k-coRated Privacy) : Une matrice d'appréciation satisfait la protection de la vie avec k-coRated, si chaque utilisateur $u \in U$ possède au moins k - 1 utilisateurs coRated Equivalence.

Dans le modèle *k*-coRated (F. Zhang*, et al.*, 2014), les auteurs ont prouvé que la manière d'établir une matrice d'appréciation afin de satisfaire la vie privée constitue un problème NP-hard et ont proposé en conséquence un algorithme heuristique nommé « *GeCom* » (voir Algorithme 1) ; nous résumons le processus en deux étapes. Afin de générer des recommandations pour un utilisateur spécifique, la première étape est de trouver ses utilisateurs similaires, qui sont collectivement appelés les voisins les plus proches (en utilisant la corrélation de Pearson pour calculer la similarité sémantique). Deuxièmement, ils remplissent pour chaque utilisateur une matrice d'appréciation contenant ses évaluations prédites pour un item non encore apprécié. De façon formelle, une matrice M des appréciations satisfait la vie privée selon *k*-coRating si chaque utilisateur $u \in U$ a au moins *k*-1 utilisateurs équivalents en coRated ($u_1, u_2, \ldots, u_{k-1} \in U$).

Le Tableau 14 illustre une matrice d'appréciation pour une base de 5 utilisateurs et 4 films. Cette matrice correspond formellement à un ensemble des appréciations $V_{i,j}$ faites par des utilisateurs i sur un film j. Par exemple, l'appréciation faite par Jill sur « Titanic » est de 3 donc $V_{3,2} = 3$. V_i correspond au vecteur décrivant l'utilisateur i. En d'autres termes, V correspond à l'ensemble de ses appréciations. Dans notre exemple, nous avons donc V_3 = [Null, 3, 1, Null]. Le Tableau 15 montre les appréciations après avoir appliqué le modèle *k*-coRated. Les valeurs Null sont remplies par des valeurs prédites pour que tous les utilisateurs évaluent les mêmes items.

Tableau 14 – Matrice des appréciations avant *k*-coRated

Film / Utilisateur	**Fast & Furious**	**Titanic**	**The Godfather**	**Star Wars**
Jeff	Null	2	4	Null
Ted	3	2	Null	Null
Jill	Null	3	1	Null
Fred	Null	Null	5	2
Kim	Null	1	2	Null

Tableau 15 - Matrice des appréciations après *k*-coRated

Film / Utilisateur	**Fast & Furious**	**Titanic**	**The Godfather**	**Star Wars**
Jeff	3	2	4	2
Ted	3	2	1	4
Jill	3	3	1	4
Fred	4	3	5	2
Kim	2	1	2	3

Comme point de départ, nous implémentons les algorithmes de *k*-coRated tel que décrit dans l'Algorithme 1 et utilisons une base de données de MovieLens 100k, afin de la traiter avec le modèle *k*-coRated. En résultat, nous constatons qu'après le traitement, la matrice des appréciations originales a augmenté. Au démarrage, la matrice contenait 80000 appréciations et après le traitement, elle augmentait jusqu'à environ 370000. Ainsi, le nombre des appréciations que la méthode a ajoutées à la matrice est considérable.

Algorithme 1 - Les algorithmes de *k*-coRated (F. Zhang*, et al.*, 2014)

Algorithm 1: sub-GeCom: k-coRating an Already Sorted Matrix M_2

input : a positive integer k; a non-k-coRated matrix M_2, treated as a set of user-item rating vectors.
output: $\overline{M_2}$, a rating matrix satisfying k-coRated privacy.

Locate first vector V in M_2
while M_2 *is NOT NULL* **do**
  Set temporary set $T \leftarrow \phi$;
  while $|T| < k$ **do**
    Append V to T;
    Delete V from M_2;
    Locate first vector V in M_2;
  end
  while M_2 *is NOT NULL and* V *is coRated equivalent to the last element in* T **do**
    Append V to T;
    Delete V from M_2;
    Locate first vector V in M_2;
  end
  if $|M_2| < k$ **then**
    Append all the remaining vectors in M_2 to T;
    Delete all the remaining vectors in M_2;
  end
  Make set I by forming the union of all the items with non-null rating values in T;
  foreach $V \in T$ **do**
    foreach $i \in I$ *and* $r_{u,i}$ *is NULL in* V **do**
      $r_{u,i} \leftarrow$ the predicted value based on different filling methods);
    end
  end
  Append T to $\overline{M_2}$;
end

Algorithm 2: GeCom: Generate k-coRated Matrix $\overline{M}$

input : rating matrix M, treated as a set of user-item rating vectors; a positive integer k; a trust matrix, tM.
output: $\overline{M}$, a rating matrix satisfying k-coRated privacy.

Sort the rating vectors in M first by ascending order of number of ratings (the smaller, the further in front), and then by lexicographic order of items;
Divide M into two parts: M_1 satisfying k-coRating, and M_2 not satisfying k-coRating;
Set $\overline{M} \leftarrow M_1$;
Invoke Algorithm 1 to k-coRate the matrix, M_2, getting a k-coRated matrix $\overline{M_2}$;
Append Matrix $\overline{M_2}$ to $\overline{M}$, forming a new rating matrix $\overline{M}$ and printing it out to a file;

7.3.2 Préoccupations et solutions relatives

Puisqu'il est impossible d'évaluer l'utilité d'une façon absolue, nous proposons un modèle qui puisse avoir une meilleure utilité. Dans le meilleur des cas, nous tentons de réaliser

notre objectif avec le moindre de modification des données. Pour cette raison, nous choisissons la méthode d'anonymisation des données en ajoutant du bruit et en essayant de faire moins de modifications. Par conséquent, s'il est inévitable d'apporter des changements aux données, nous l'espérons le moins possible. De plus, la raison pour laquelle nous évitons la modification des données est que les données originales sont parfaites et sont convenables vu que les utilisateurs les ont générées au moment de leurs activités et tout ajout de nombres à la matrice sera inadéquat au scénario. Cependant, si ce que nous ajoutons à la matrice originale correspond à ce qui va se passer ou ce qui s'est passé dans le monde réel, alors l'utilité des données devrait rester la même. Ainsi, une meilleure prédiction permettra également une meilleure utilité. En conséquence, nous établissons deux objectifs :

Moins de modifications : Nous espérons atteindre le modèle *k*-coRated avec le moins de modifications de données possibles dans le contexte de préservation de la vie privée. Pour ce faire, nous adoptons *k*-means pour améliorer le regroupement des utilisateurs en espérant que les utilisateurs dans le même groupe aient déjà apprécié ou co-rated la plupart des éléments. Ensuite, nous proposons une nouvelle méthode pour faire la modification, appelée **Delete Little to Add Less** (*L2L*).

Meilleure prédiction : Les méthodes de filtrage collaboratif (*CF*) centrées sur l'utilisateur sont généralement utilisées dans les systèmes de recommandation et c'est prouvé qu'ils présentent des avantages par rapport au filtrage fondé sur le contenu, principalement la capacité de filtrer en fonction des préférences des utilisateurs afin d'amener à des recommandations satisfaisantes (Herlocker*, et al.*, 2000). Pour ce faire, un ensemble de ***k*-proches** voisins est identifié pour chaque utilisateur, et la décision de proposer ou non un item à un utilisateur dépendra des appréciations des utilisateurs de son voisinage. Dans notre travail, un meilleur ensemble de voisins les plus proches se traduira également par une meilleure prédiction.

7.3.3 Moins de modifications : K-means

Puisque nous nous intéressons à savoir si un utilisateur a apprécié un item ou non, avant d'appliquer à notre matrice la méthode de clustering *k-means*, nous effectuons une normalisation selon la formule suivante :

Définition (Normalized Rating Matrix) : Une matrice d'appréciation *R* est normalisée si $R_{u,i}$ satisfait la formule suivante:

$$R[u,i] = \begin{cases} 1, \text{User } u \text{ has rated item } i \\ 0, \textit{otherwise} \end{cases}$$

Suite à la normalisation, nous appliquons la méthode *k*-means. Il s'agit d'une méthode qui permet de séparer les utilisateurs en *k* clusters, et où chaque utilisateur appartient au cluster dont la moyenne est la plus proche. L'une des difficultés de la présente méthode est le choix des clusters au départ, donc le choix de l'initialisation. Ce qui fait que la performance de *k*-means dépend largement de la sélection des centres initiaux. Pour ce faire, nous avons choisi d'utiliser *l'heuristique du plus proche* voisin qui représente une heuristique de construction simple et une des heuristiques les plus utilisées. L'idée principale de l'heuristique est de trouver une sélection la plus proche du vrai centre final afin de fournir de meilleurs clusters (grappes de nœuds). Afin d'obtenir une meilleure base pour mesurer l'ensemble initial de centres, nous concluons deux propriétés pour les centres qui aident à déterminer un moyen de trouver des centres initiaux, à savoir la **Distance** et la **Densité** que nous définissons ci-dessus :

Distance : les centres initiaux doivent être suffisamment éloignés les uns des autres et non situés dans le même groupe.

Densité : le centre initial doit avoir beaucoup d'autres points autour de lui.

Après avoir défini ces propriétés, nous donnons leurs définitions en nous basant sur la distance euclidienne entre utilisateurs.

Définition (dis) : Pour chaque utilisateur *u* et $v \in U$,

$$dis(u,v) = \sqrt{\sum_i (u[i] - v[i])^2} \quad (2)$$

Définition (density) : Pour chaque utilisateur $u \in U$,

$$Density(u) = \frac{1}{\sum_{v \in U} dis(u,v)} \quad (3)$$

Définition (distance) : Pour chaque utilisateur $u \in U$,

$$Distance(u) = \sum_{v \in Centers} dis(u,v) \quad (4)$$

Pour assurer un équilibre entre distance et densité, nous proposons une fonction de poids entre les résultats normalisés par la distance et de la densité

Définition (weight) : Pour chaque utilisateur $u \in U$,

$$weight(u) = \alpha * \widehat{distance}(u) + (1 - \alpha) * \widehat{density}(u) \quad (5)$$

$\widehat{distance}(u)$ et $\widehat{density}(u)$ Sont les résultats normalisés entre [0,1].

À partir de ces définitions, nous présentons l'Algorithme 2 pour trouver de meilleurs centres initiaux en nous basant sur la densité et la distance (*DD*).

Algorithme 2 - DD-Based Initial Centers

Input:

k, the number of initial centers

R, normalized rating matrix

Output:

k initial centers

1: Initialize centers as empty
2: Compute density for every user in *R*
3: Set the user with max density as the first center
4: **while** *len*(centers)! = *k* **do**
5: Compute weight for every user in *R* except those in centers
6: Add a user with max weight to centers
7: **end while**
8: **return** centers

7.3.4 Moins de modifications : L2L

Prenons l'exemple d'une matrice des appréciations (Utilisateur x Item). Telle qu'illustrée dans la Figure 29, la Table 1 représente la matrice originale. Il existe dans la matrice originale des items qui sont appréciés par la majorité des utilisateurs et des items qui sont moins appréciés. Nous appliquons une nouvelle méthode nommée **Delete Little to Add Less** (*L2L*). Cette méthode consiste à supprimer les appréciations des items qui sont moins appréciés. La Figure 29 montre les résultats avec la méthode L2L et fait une comparaison avec les résultats du modèle *k*-coRated.

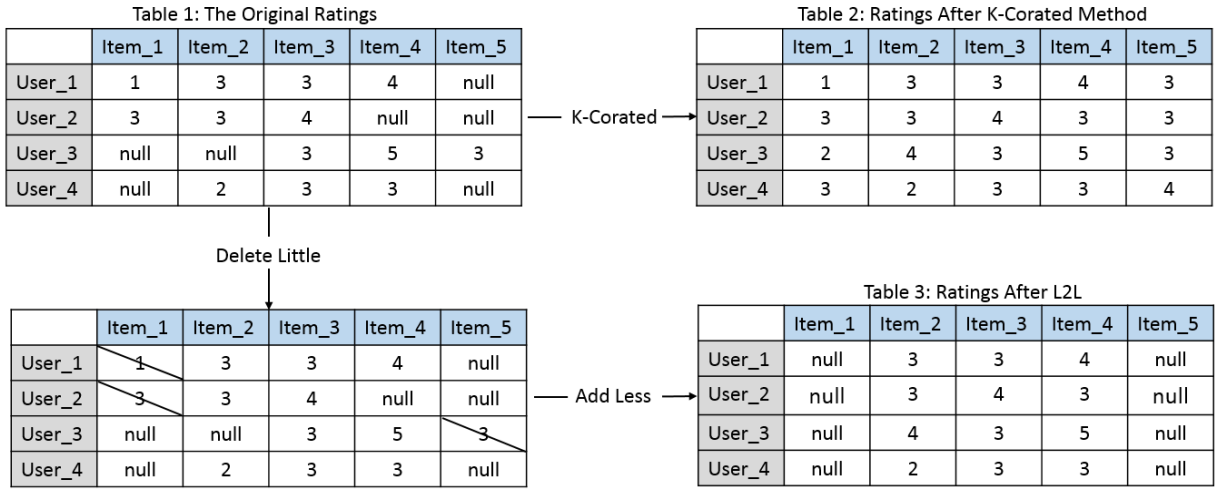

Figure 29 - Procédure de L2L

Quatre utilisateurs ont apprécié les éléments de 1 à 5. Afin de les rendre *k*-coRated, nous suivons l'ancienne méthode, puis nous ajoutons des appréciations prévues pour remplir les valeurs nulles. Le résultat de ce traitement apparait dans la Table 2. Cependant, dans la Table 1, certains éléments sont moins évalués, peu d'utilisateurs les ont évalués, comme l'item_1 et l'item_5. Selon notre approche, nous supprimons ceux qui sont appréciés par peu d'utilisateurs; ainsi, dans la Figure 29, nous supprimons les appréciations de (*User_1, Item_1*), (*User_2, Item_1*) et (*User_3, Item_5*), puis nous ajoutons les appréciations prévues pour (*User_2, Item_4*) et (*User_3, Item_2*). Cependant, comment décider quelle partie qui doit être supprimée? Quels sont les éléments qui sont appréciés par peu d'utilisateurs?

Définition (centroïde Cluster) : Ci-dessous, nous définissons ce qui est le centroïde d'un cluster C, noté comme étant *ctr*(*C*). Pour chaque utilisateur $i \in I$,

$$ctr(C)[i] = \frac{\sum_{u \in U} u[i]}{|C|} \quad (6)$$

En nous basant sur le *ctr*(*C*), nous décidons que, pour tout point i, si le *ctr(C)*[*i*] ≤ β, donc i appartient à la partie à supprimer. β est un hyperparamètre, c'est-à-dire un paramètre choisi arbitrairement avant l'entraînement et donc non optimisé lors de celui-ci.

7.3.5 Meilleure prédiction

Le calcul de la similarité est une phase indispensable dans le filtrage collaboratif. Une meilleure prédiction vient d'une meilleure définition de la similarité entre deux utilisateurs. Les mesures de similarité à tester sont appliquées pour trouver les plus proches voisins sémantiques. Finalement, tous les utilisateurs sont triés suivant leur valeur de similarité et seuls les *N* plus proches voisins sont conservés. Afin de prévoir la préférence d'un utilisateur *u* à l'item *i*, dénotée par $P_{u,i}$, les méthodes de filtrage collaboratif basées sur l'utilisateur tentent de se référer aux préférences de ***k* proches** voisins de *u* (*k-NN*) (Keller*, et al.*, 1985). Pour l'utilisateur *u,* les voisins les plus proches sont dénotés par *N Nu.* Dans notre travail, nous adoptons la formule ci-dessous pour faire la prédiction :

$$P_{u,i} = \bar{u} + \frac{\sum_{v \in NNu} \text{sim}(u,v) * R_{v,i}}{\sum_{v \in NNu} \text{sim}(u,v)} \quad (7)$$

Où $\bar{u}$ est la moyenne des appréciations de l'utilisateur *u*, sim(*u,v*) est la similarité entre deux utilisateurs *u et v*.

7.4 Expérience et résultats

Dans cette section, nous évaluons notre modèle en matière de protection de vie privée et d'utilité et le comparons avec celui de Zhang *et al.* (F. Zhang*, et al.*, 2018).

7.4.1 Réalisation de l'expérience

Nos expériences sont réalisées en utilisant la base de films **MovieLens 100k** (Harper & Konstan, 2016), qui se compose de 100000 appréciations de 943 utilisateurs sur 1682 articles. Nos algorithmes sont implémentés en python sur un ordinateur équipé de Windows 10.

7.4.2 Protection de la vie privée

Dans un contexte de publication des données, la littérature relative à la protection de la vie privée souligne qu'en règle générale, un attaquant, pour accéder à l'information sensible, utilise des stratégies fondées avant tout sur sa connaissance du contexte. Dans ces stratégies, nommées aussi modèles d'attaques, l'adversaire déduit des informations sensibles sur sa victime en établissant des liens tels que : liens par *homogénéité*, liens par *similarité*, liens par *attribut*, liens par *dissymétrie* ou encore en procédant à des *inférences probabilistes* suivant des croyances probabilistes avant et après l'analyse des valeurs des attributs sensibles telle que distribuée dans la table publiée.

Pour ce faire, nous évaluons notre travail en matière de la protection de la vie privée en nous appuyant sur le modèle d'attaque proposé par (Narayanan & Shmatikov, 2008). Le modèle est appliqué à l'ensemble de données de Netflix, qui contient les appréciations anonymes des films de 500000 abonnés. L'attaque démontre qu'un adversaire qui ne connaît que peu d'informations à propos d'un abonné peut facilement identifier l'enregistrement de cet abonné dans l'ensemble des données. Ce modèle, nommé aussi *modèle d'attaque de Natayanan et Shmatikov ou NS*, suppose que les attaquants peuvent obtenir des informations auxiliaires des utilisateurs. Par exemple, si l'adversaire connait 8 appréciations sur des films avec leurs dates d'appréciations effectuées par les abonnés, ces derniers peuvent être identifiés. Le modèle définit une fonction appelée *Score*, qui considère comme paramètres l'enregistrement de l'utilisateur dans la base de données et l'information auxiliaire que les attaquants ont connue. La fonction extrait un indicateur pour mesurer à quel point l'enregistrement correspond à l'information auxiliaire et par conséquent l'utilisateur est ciblé.

$$Score(Rec,Aux) = \sum_{i \in supp(Aux)} wt(i) \ * \ Sim(Rec_i, Aux_i) \qquad (8)$$

Où *Rec* est l'enregistrement de l'utilisateur dans la base de données, *Aux* représente l'information auxiliaire.

Pour chaque utilisateur concerné par les données publiées, une liste de scores est extraite en appliquant la formule 8. Soit **Max1** et **Max2** respectivement le premier score le plus élevé, le deuxième score le plus élevé, **σ** l'écart-type des scores et **ϕ** paramètre fixe

appelé excentricité. La valeur de $\frac{Max_1 - Max_2}{\sigma}$ indique à quel point le meilleur enregistrement surpasse les autres et ϕ est un seuil. Si $\frac{Max_1 - Max_2}{\sigma} < \phi$ alors il n'y a pas de correspondance entre *Rec* et *Aux*, sinon l'ensemble de correspondance se compose de l'enregistrement ayant le score le plus élevé. Par conséquent, le modèle exige non seulement que l'enregistrement de l'utilisateur cible soit celui qui a le score le plus élevé, mais aussi qu'il surpasse les autres enregistrements. L'Algorithme 3 explique le *modèle d'attaque NS* étape par étape.

Algorithme 3 - Scoreboard-RH (Narayanan & Shmatikov, 2008)

Input:

Aux, the auxiliary information gained by attackers

D, the rating dataset ϕ, eccentricity

Output:

the match record or empty set

1: For each record $Rec \in D$, compute $Score(Rec, Aux)$

2: Compute $Max_1 = Max_1(S)$, $Max_2 = Max_2(S)$, $\sigma = std(S)$,

where $S = (Score(Rec,Aux), Rec) \in D$

3: **If** $\frac{Max_1 - Max_2}{\sigma} < \phi$, **then**

4: **return** an empty set

5: **else**

6: **return** the match record with the highest

7: **endif**

Nous avons simulé le *modèle d'attaque NS* en supposant que les attaquants ont obtenu 8 et 16 éléments d'information au total. La Figure 30 compare le rendement de la préservation de la vie privée entre notre modèle et celui de *k*-coRated. L'axe des y indique la probabilité d'être réidentifié pour les utilisateurs des données, tandis que l'axe des x indique l'information recueillie par les attaquants. À partir des deux graphiques, nous pouvons voir que, bien qu'il y ait peu de différence entre notre modèle et *k*-coRated lorsque les attaquants gagnent peu d'éléments d'information, notre modèle surpasse presque de deux fois le modèle *k*-coRated concernant la possibilité d'être réidentifié quand les attaquants en savent plus.

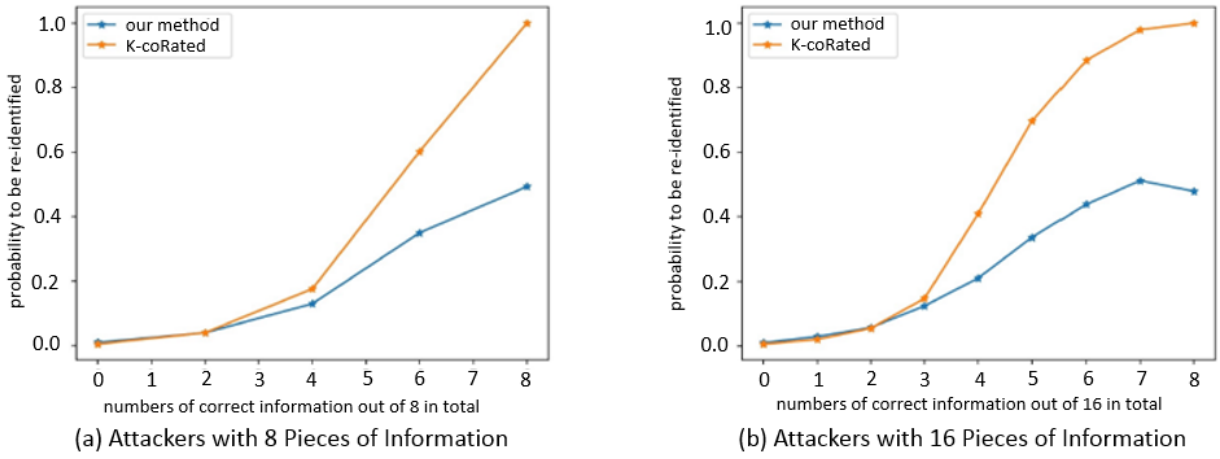

Figure 30 - Comparaison de vie privée

7.4.3 Utilité : Nombre de ratings

Étant donné qu'il n'existe pas de norme universelle d'évaluation de l'utilité, nous construisons notre évaluation en comparant le nombre d'appréciations dans la matrice et en évaluant le rendement des données concernant le filtrage collaboratif. Nous comparons le nombre d'appréciations dans la matrice, ce qui reflète la modification des données. Afin de rendre les deux méthodes comparables, nous faisons en sorte qu'elles aient le même nombre de clusters. La Figure 31 présente les résultats de deux méthodes pour regrouper les utilisateurs en 10, 20 et 30 groupes. À partir de la Figure 31, nous pouvons déterminer qu'après avoir été traité par notre modèle, le nombre des appréciations dans la matrice demeure autour de 260000 alors qu'après avoir été traités par le modèle *k*-coRated, il est passé de 400000 environ à 600000 à mesure que le nombre de grappes d'utilisateurs augmente. Par conséquent, notre modèle réduit considérablement la modification des données et fournit une meilleure utilité des données.

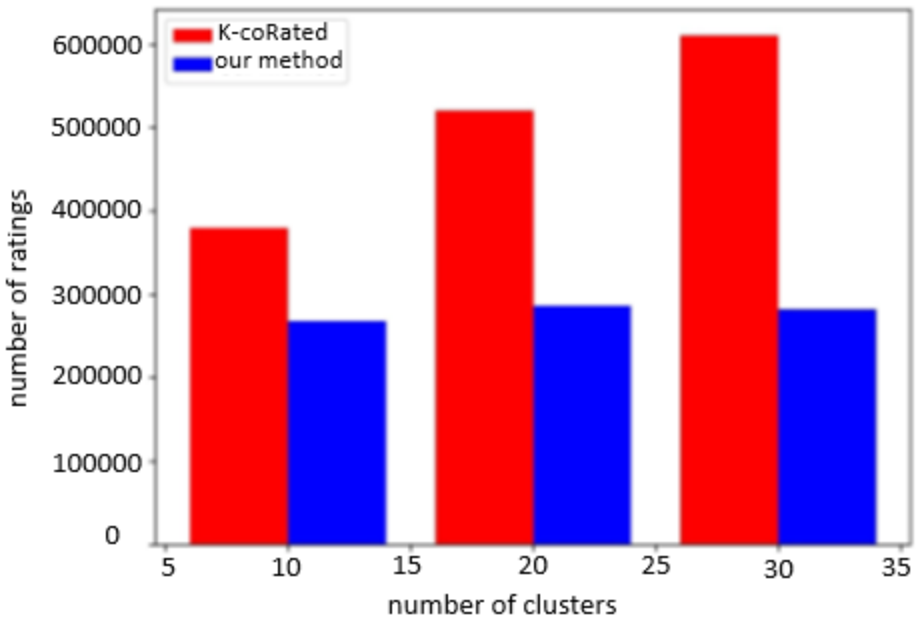

Figure 31 - Comparaison de nombre de Ratings

7.4.4 Utilité : Performance du filtrage collaboratif

Puisque nos données portent sur le système de recommandation et que le filtrage collaboratif est couramment utilisé sur le terrain, nous avons donc décidé de tester l'utilité des données en fonction de la performance du filtrage collaboratif. Nous mettons en œuvre différentes stratégies de prédiction proposées par (F. Zhang*, et al.*, 2018) et utilisons *la moyenne des erreurs quadratiques* (*Root Mean Square Error* ou **RMSE**) entre la note prédite et la note réelle pour évaluer la performance des CF. Nous expliquons ci-dessous ce qu'est RMSE.

Compte tenu des N paires réelles/prévues ($R_{u,\,i}$, $P_{u,\,i}$), le RMSE des paires N est calculé comme suit :

$$RMSE = \sqrt{\frac{\sum(Ru,i - Pu,i)^2}{N}} \tag{9}$$

Où $R_{u,i}$ est la note réelle attribuée par l'utilisateur u à l'item i, $P_{u,i}$ est la note prédite.

La Figure 32 montre la performance de notre modèle par rapport au modèle *k*-coRated. Dans chaque cas, nous utilisons les mêmes définitions de similarité selon l'équation 7 pour faire la prédiction, et nous choisissons les voisins les plus proches des 5 à 100 utilisateurs les plus semblables.

À partir de la Figure 32(a), la meilleure *RMSE* est d'environ 0,98 lorsque l'on adopte la définition de la similitude fondée sur la corrélation et que l'on choisit les voisins les plus proches dans le top 80, tandis que, d'après la Figure 32(b), la meilleure *RMSE* est d'environ 0,94 lorsque l'on adopte la définition de la similitude fondée sur la corrélation et que l'on choisit les voisins les plus proches dans le top 40. Par conséquent, notre modèle augmente l'utilité des données compte tenu de la performance des CF.

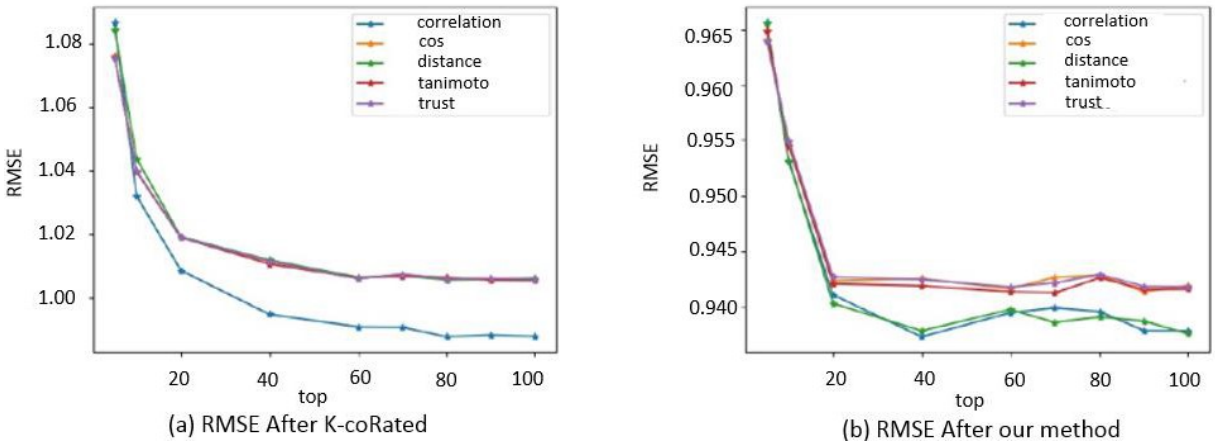

Figure 32 - Comparaison de l'utilité

7.5 Conclusions et travaux futurs

F. Zhang *et al.* (F. Zhang*, et al.*, 2018) ont proposé un modèle novateur pour protéger la vie privée des utilisateurs lorsque des données sont sur le point d'être diffusées. Cependant, ils ont omis de pondérer l'équilibre entre la vie privée des utilisateurs et l'utilité des données. Sur la base des inconvénients de leur modèle, nous proposons un nouveau modèle impliquant moins de modifications de données et offrant une meilleure prédiction. En appliquant les méthodes de *k-means* et de **Delete Little to Add Less** (*L2L)*, nous obtenons une réduction significative de la modification des données. Ceci dit, une constatation que nous pouvons relever de notre modèle est qu'il nous permet d'affirmer que moins de modifications conduisent à une meilleure utilité comme, de notre point de vue, il n'existe pas de norme universelle pour évaluer l'utilité. Entre-temps, dans le cadre de l'évaluation des attaques NS, nous offrons un meilleur degré de protection de la vie privée.

En outre, nous avons implémenté et testé nos travaux sur l'ensemble des données de **MovieLens 100k**. Dans les travaux futurs, nous prévoyons de prendre en considération d'autres ensembles de données comme MovieLens 10M, Epinions ou Netflix. L'expérience sur ces ensembles de données nécessite d'autres considérations, et puisque MovieLens 100k n'est pas un grand jeu de données, nous ne mettons pas l'accent sur le temps de calcul. Un autre travail futur consiste à concevoir un modèle pour évaluer l'utilité des données dans différents domaines.

Chapitre 8 : Stabilité des préférences dans les systèmes de recommandation

Les systèmes de recommandation visent à mettre en place des options plus personnalisées pour les utilisateurs et donc à offrir une intégration vitale dans le commerce électronique. Comme objectifs, ces systèmes essaient de modéliser les intérêts des utilisateurs en fonction des données historiques afin de prévoir finalement des recommandations qui répondent à leurs besoins.

Cependant, cela néglige les utilisateurs qui sont flexibles dans leurs préférences et qui sont plus prêts pour essayer des avis différents ou nouveaux. Cette diversification implique que dans de prochaines sélections, les préférences ou les goûts des utilisateurs peuvent s'écarter de ce que les systèmes de recommandation prédisent. Pour cette raison, il est nécessaire de formuler des recommandations pour les utilisateurs en fonction de leurs goûts modélisés.

Dans cette direction, nous mesurons la stabilité de l'intérêt des utilisateurs en calculant la variation des données récentes de l'utilisateur. Nous proposons un réseau neuronal pour prédire le goût de l'utilisateur en fonction de la séquence des éléments sélectionnés par les utilisateurs et les caractéristiques des éléments en supposant que le goût de l'utilisateur ne change pas radicalement. La méthode de prédiction proposée implique la génération de recommandations qui fournissent des éléments innovants et différents aux utilisateurs qui sont instables dans leurs préférences à une probabilité plus élevée et aux utilisateurs qui sont stables avec une probabilité inférieure.

8.1 Préférences des usagers dans les systèmes de recommandation

Devant l'augmentation explosive du nombre de produits et d'informations sur Internet, les gens ont tendance à être perplexes et n'ont pas le temps de trouver ce qui leur convient le mieux et ce qui pourrait les intéresser. Des systèmes de recommandation sont développés pour leur offrir des options moins nombreuses, mais plus personnalisées qui peuvent améliorer leur expérience. Les systèmes de recommandation sont essentiels non seulement

pour les sites Web commerciaux comme Amazon et Taobao, mais aussi pour les sites Web de divertissement comme Netflix, YouTube et CBS. Habituellement, les utilisateurs se sentent mieux s'ils peuvent obtenir rapidement ce qu'ils veulent. La stabilité des intérêts des utilisateurs doit être prise en considération lorsque les systèmes de recommandation présentent certains éléments aux utilisateurs.

Dans le but de mieux comprendre le contexte de notre travail, nous prenons comme exemple quatre usagers avec sept films : *the Godfather* (M_1), *Underground* (M_2), *James and the Giant Peach* (M_3), *the Phantom of the Opera* (M_4), *Home Alone* (M_5), *the Insider* (M_6), et *Othello* (M_7). Comme indiqué dans le Tableau 16, U_1 et U_4 ont marqué M_1 avec une appréciation égale à « 5 », M_4 avec « 3 », M_6 avec « 4 ». M_1, M_4 et M_6 avec M_7 appartiennent à la même catégorie des films tragiques (*"Drama Movies"*).

Tableau 16 - Exemples de films appréciés par les usagers

User	Movie	Rating
U_1	M_1	5
	M_4	3
	M_6	4
U_2	M_2	1
	M_5	2
	M_7	5
U_3	M_3	2
	M_6	4
U_4	M_1	5
	M_2	3
	M_3	4
	M_4	3
	M_5	2
	M_6	4

Les méthodes de recommandation existantes utiliseraient le filtrage basé sur le contenu et regarderaient les similitudes des propriétés des films pour recommander M7 à l'utilisateur U_1 puisqu'il appartient à la même catégorie des films bien appréciés précédemment. Alternativement, les systèmes de recommandation de filtrage collaboratifs basés sur les similitudes entre les utilisateurs trouveraient par exemple une similitude entre U_1 et U_4 puisque les deux usagers ont bien apprécié M_1, M_4 et M_6, donc le système recommanderait M_3 à l'utilisateur U_1 puisque U_4 l'a évalué avec « 4 ». Cependant, que se passerait-il si l'utilisateur U_1 changeait ses préférences et décidait aujourd'hui de rejeter ce qu'il a préféré dans le passé ? Ou s'il préfère une sélection qui n'était pas dans ses listes? Ou bien si son appariement avec l'utilisateur U_4 n'est plus valide ? Dans ce cas, l'utilisateur U_1 est moins satisfait, ignore les recommandations et procède à de nouvelles recherches dans les sites Web.

Dans ce chapitre, nous proposons un réseau neuronal pour nous attaquer à ce problème. La stabilité des intérêts des utilisateurs consiste notre point de départ. Notre objectif est de fournir des recommandations plus personnalisées et mieux répondre aux besoins des utilisateurs. Prenons l'exemple de Bob qui apprécie beaucoup les films d'horreur. À la période d'Halloween, il se fait recommander un nouveau film d'horreur sorti récemment. Cependant, Bob regarde les films récents et voit « Under the Skin » un film de science-fiction tournant autour d'une aventure d'horreur. Bob n'a pas l'habitude de regarder de la science-fiction mais cette fois-ci, il change son avis et le choisit.

Pour ce faire, nous procédons aux étapes suivantes :

- Nous transformons les entrées précédentes des utilisateurs en données numériques via l'encodage linéaire (one-hot) (Beck & Woolf, 2000). Cette méthode produit des vecteurs de données dans lesquels seul un bit est mis à 1, le reste est à 0. Ces vecteurs sont ensuite stockés dans les registres d'états des neurones de la couche d'entrée.
- Nous analysons les données séquentielles et les fonctionnalités des éléments sélectionnés par les utilisateurs (Brafman*, et al.*, 2003; Sachdeva*, et al.*, 2018) pour modéliser leurs intérêts.

- Nous supposons que les goûts des utilisateurs ne changent pas radicalement.
- Nous mesurons la stabilité des intérêts des utilisateurs en utilisant la variation de la séquence des données et l'ajoutons à la couche neuronale dans notre réseau (Chapelle & Wu, 2010) qui donne la probabilité d'occurrence de chaque élément.
- Nous adoptons la méthode d'échantillonnage (Bengio & Senécal, 2008) pour générer les K recommandations finales.
- Nous évaluons notre nouveau modèle. Les utilisateurs qui ont une stabilité d'intérêt faible reçoivent, à une forte probabilité, des recommandations différentes de leurs items choisis récemment. Tandis que les utilisateurs qui ont une stabilité d'intérêt élevée, ils reçoivent, à une forte probabilité, des recommandations semblables à leurs items récents.

8.2 Réseaux de neurones dans les systèmes de recommandation

De nombreuses méthodes sont proposées pour améliorer la performance des systèmes de recommandation, y compris les méthodes traditionnelles, les méthodes de factorisation matricielle (Su & Khoshgoftaar, 2009; Xiao*, et al.*, 2018), les méthodes basées sur l'apprentissage automatique et les réseaux neuronaux profonds (X. He*, et al.*, 2017; S. Zhang*, et al.*, 2017; X. Zhao*, et al.*, 2018; Zheng*, et al.*, 2017). Ces derniers sont inspirés des systèmes nerveux biologiques dans le sens où ces modèles, capables de modéliser des tâches complexes, sont composés d'une grande quantité d'unités de calcul plus basiques, appelées neurones. Ils ont apporté des succès dans différents domaines tels que la génération d'images, la vision informatique (Hinton*, et al.*, 2012; Russakovsky*, et al.*, 2015), le traitement du langage naturel et de la parole (X. He*, et al.*, 2017). Leurs capacités à intégrer des sources multiples d'information et à tirer profit d'importants volumes de données ont également permis leur application aux systèmes de recommandation.

Dans les systèmes de recommandation, Wang *et al.* (H. Wang*, et al.*, 2015) proposent une des premières méthodes alliant les systèmes de recommandations avec les réseaux neuronaux. À titre d'exemples, mentionnons la mise en œuvre des réseaux profonds dans

le système de recommandation de *YouTube* (Covington*, et al.*, 2016) qui présente une architecture à deux niveaux, la recommandation intra-session et la connexion inter-sessions utilisant des réseaux de neurones récurrents hiérarchiques (Quadrana*, et al.*, 2017).

D'autres approches utilisent des *autoencodeurs.* Ceux-ci peuvent être utilisés de deux façons : en utilisant une couche intermédiaire plus petite comme représentation latente ou en reconstruisant une matrice de scores[18]. À titre d'exemple, (Ying*, et al.*, 2016) utilise un modèle alliant une approche bayésienne avec un *autoencodeur* pour créer une liste ordonnée de recommandations basée sur les différences de préférence entre items dans une paire.

D'autres approches utilisent des réseaux de neurones *convolutionnels* (*CNN*) pour encoder les attributs des items et le comportement des utilisateurs en se basant sur le texte de commentaires avant de les combiner par une machine de factorisation à la dernière couche (Zheng*, et al.*, 2017). À titre d'exemple, Gong *et al.* (Gong & Zhang, 2016) présentent un système de recommandation des hashtags en utilisant le texte d'un tweet comme données. L'attention est utilisée pour seulement donner de l'importance aux mots les plus informatifs.

D'autres approches sont inspirées des modèles à base de représentations vectorielles de mots utilisant une factorisation de matrices. Cette factorisation (Ricci*, et al.*, 2015; X. Zhang*, et al.*, 2017) est une amélioration des méthodes de filtrage collaboratives pour mieux modéliser les caractéristiques des utilisateurs et des éléments. Elle consiste à décomposer la matrice de scores en un produit de facteurs latents pour les utilisateurs et les items.

Le réseau neuronal récurrent (*RNN*) (Y. Zhang*, et al.*, 2014) qui fonctionne bien sur les problèmes de séquence tels que le traitement du langage naturel et la reconnaissance vocale est également appliqué aux problèmes de prédiction des éléments. Il traite le score donné par un utilisateur à un item, en prenant compte que l'attrait d'un item et les préférences d'un utilisateur évoluent au fil du temps. À titre d'exemple, Li et al. (Yang Li,

[18] https://www.deeplearningbook.org/contents/autoencoders.html consule le 05/Nov/2019

et al., 2016) présentent un mécanisme d'attention avec un *RNN* pour prédire les *hashtags* à partir d'un texte.

Ces approches font un excellent travail de modélisation des intérêts des utilisateurs en fonction des éléments qui sont recommandés. Cependant, ils ont négligé la variation de l'intérêt des utilisateurs et n'ont pas tiré parti de la stabilité de leurs préférences, ce qui peut mener à une problématique dans le processus de recommandation.

8.3 Méthodologie

Nous proposons un réseau envisageant la stabilité des intérêts des utilisateurs (*User Interest Stability ou UIS*) pour résoudre le problème de recommander *k*-éléments aux utilisateurs. Ce réseau peut analyser les caractéristiques des éléments et des articles eux-mêmes pour cerner l'intérêt des utilisateurs. Après les représentations distribuées des éléments et des fonctionnalités de l'élément, la stabilité de l'intérêt de l'utilisateur est analysée et ajoutée à la couche de sortie. En fonction des résultats, la méthode d'échantillonnage est également adaptée pour générer *K* éléments recommandés. Nous présentons ici l'énoncé formel de notre problème. Il s'agit de générer *K* recommandations en tenant compte de l'ensemble des éléments que l'utilisateur a choisis dans l'ordre $Ii = (item_1, item_2, \ldots, item_{i-1})$ et les caractéristiques des articles $Fi = (fi_1, fi_2, \ldots, fi_j)$, ainsi que de générer *K* recommandations qui tiennent compte de l'intérêt des utilisateurs et de la stabilité de leurs intérêts.

8.3.1 Solution proposée

Notre modèle *UIS* est basé sur les réseaux de neurones récurrents (*Recurrent Neural Network ou RNN*) puisque ces derniers peuvent traiter des données de taille variable. La Figure 33 illustre l'architecture des réseaux récurrents.

De même, le *Gated Recurrent Units* (*GRU*) (K. Cho*, et al.*, 2017; Chung*, et al.*, 2014) est une autre architecture, illustrée à la Figure 34, qui permet d'entraîner correctement des réseaux récurrents. *GRU* est également utilisé intensivement dans la modélisation du texte, due à son excellente performance dans la modélisation des séquences (Xing*, et al.*, 2019) et dans la prédiction de séries temporelles.

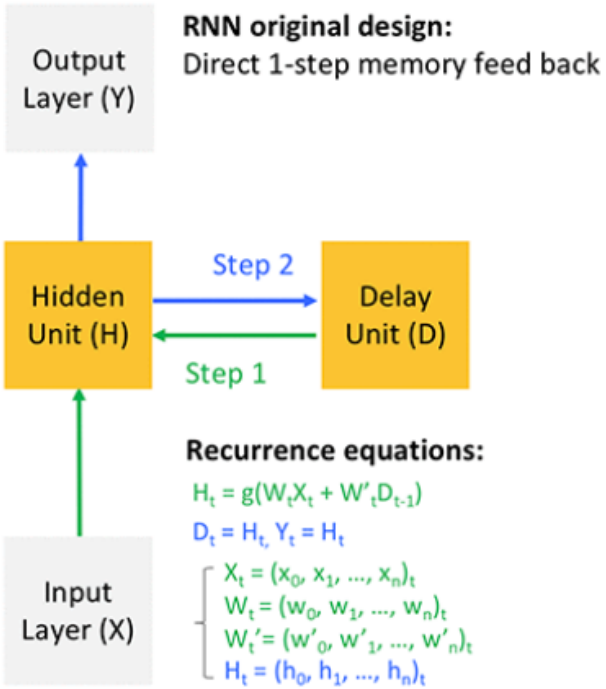

Figure 33 - Architecture d'un réseau récurrent[19]

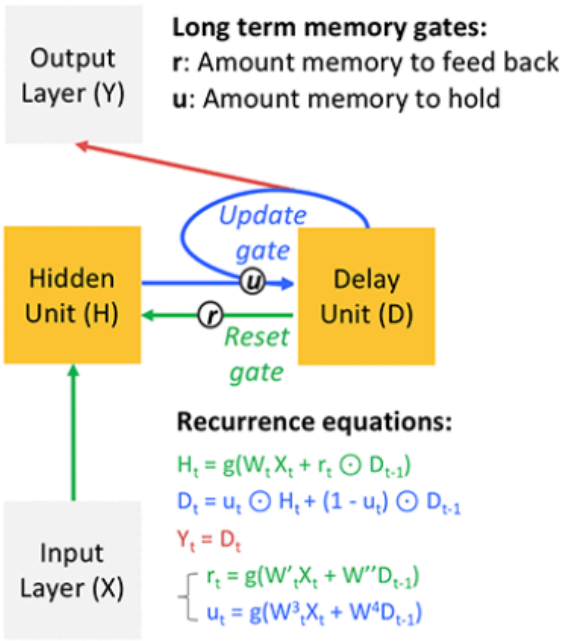

Figure 34 - Architecture d'un GRU[18]

[19] https://aws.amazon.com/blogs/machine-learning/forecasting-time-series-with-dynamic-deep-learning-on-aws/ consulte le 08/Nov/2019

Par ailleurs, le modèle *UIS* comprend deux couches principales : une couche des items précédents de l'utilisateur et une couche des caractéristiques. Nous transformons les entrées précédentes des utilisateurs en données numériques via encodage linéaire (one-hot) (Beck & Woolf, 2000). Cette étape est effectuée, car les encodages linéaires sont simples à calculer et à comprendre, et sont souvent utilisés lorsqu'il est nécessaire de représenter une variable catégorique dans un réseau de neurones (Buckman*, et al.*, 2018).

De plus, cette méthode utilise effectivement un vecteur d'états de taille |Q| où seulement un élément est "à chaud" (one-hot) et produit des vecteurs de données dans lesquels seul un bit est mis à 1, le reste est à 0 comme dans [00001, 00010, 00100, 01000,10000]. Ces vecteurs sont ensuite stockés dans les registres d'états des neurones de la couche d'entrée. Prenons l'exemple de la matrice d'appréciations M, illustrée dans le Tableau 17. Suite à l'encodage linéaire, le résultat devient tel que présenté dans le Tableau 18.

Tableau 17 – Matrice M des appréciations des films

Utilisateurs	**Films**	**Appreciations**
Alice	The Godfather	5
Alice	Home alone	3
Bob	The Phantom of the Opera	1
Bob	The Insider	4
Bob	Home alone	5
Jill	The Godfather	1
Jill	The Phantom of the Opera	5

Tableau 18 - Encodage "One-hot" de la matrice M

Utilisateurs			**Films**				**Appréciations**
Alice	Bob	Jill	The Godfather	Home alone	The Phantom of the Opera	The Insider	
1	0	0	1	0	0	0	5
1	0	0	0	1	0	0	3
0	1	0	0	0	1	0	1
0	1	0	0	0	0	1	4
0	1	0	0	1	0	0	5
0	0	1	1	0	0	0	1
0	0	1	0	0	1	0	5

UIS lit les entrées au fur et à mesure et les sorties sont traitées par le GRU. Cette étape est nécessaire pour analyser l'information en séquence et pour comprendre la stabilité des intérêts des utilisateurs. Les variations de ces sorties sont regroupées pour mesurer la stabilité des intérêts des utilisateurs qui seront ajoutées à la sortie du modèle final. Dans la plupart des réseaux de neurones, ces couches suivent toutes le même schéma, soit une transformation linéaire suivie d'une fonction appliquée par élément. Plus concrètement, pour un vecteur de données d'entrées $x \in R^p$, une matrice de poids $W \in R^{k \times p}$, un vecteur de biais $b \in R^k$ et une sortie $\hat{y} \in R^k$, on aura :

$$z = W_x + b$$

$$y = \sigma(z)$$

où σ représente n'importe quelle fonction d'activation appliquée par élément. Dans notre modèle *UIS*, ReLU (*Rectified Linear Unit*) est utilisée comme fonction d'activation. ReLU est choisie dans la sortie de la couche cachée (*hidden layer*) pour sa performance, pour son efficacité dans le calcul et pour son adaptation pour les modèles profonds plus que sigmoïde (*sigmoid*) (H. Guo*, et al.*, 2017; Qu*, et al.*, 2016). Pour un problème de

classification, la fonction typiquement utilisée à la dernière couche est le *Soft-argmax* (Honari*, et al.*, 2018). Cette dernière fait en sorte que le l'ensemble du réseau soit entièrement différenciable pour améliorer la performance de l'entraînement du modèle, c'est-à-dire donner des paires de données d'entrée et de sortie justes et faire en sorte que le modèle fasse les meilleures prédictions possibles et donne les probabilités des éléments suivants tout en tenant compte des intérêts de l'utilisateur. Pour ce faire, la méthode d'échantillonnage est adaptée pour générer *K* recommandations suivant les probabilités calculées.

Afin de comprendre la notion de couches d'un réseau de neurones, prenons l'exemple du graphique, illustré dans la Figure 35. Nous distinguons 3 nœuds d'entrée, 4 nœuds dans la couche cachée et 2 nœuds de sortie. Chaque nœud d'entrée est associé à une variable à analyser par utilisateur. Ainsi dans l'exemple, il y a 3 variables donc les utilisateurs sont représentés par un vecteur à 3 dimensions. Pour les nœuds de la couche de sortie, ceux-ci correspondent aux valeurs de sortie ou plus généralement à une *classe*. Autrement dit, en entrée, l'utilisateur est décrit par 3 variables, le traitement de ces variables se fait avec les nœuds de la couche cachée et en sortie, on obtient la classe d'affectation de cet utilisateur. À noter qu'il est possible d'avoir plusieurs couches cachées. Un nœud de la couche cachée a deux fonctions. La première consiste à « résumer » les infos qui lui arrivent en entrée. En règle générale, il s'agit de la somme des produits n_i*p_i (ou n_i est la valeur du nœud i et p_i la probabilité associée au nœud). La seconde consiste à appliquer une fonction de transfert à cette somme et ainsi fournir ce résultat aux nœuds de sortie (ou au nœud d'une autre couche cachée s'il y en a une).

Pour clarifier davantage notre solution, la section suivante décrit notre modèle avec plus de détails.

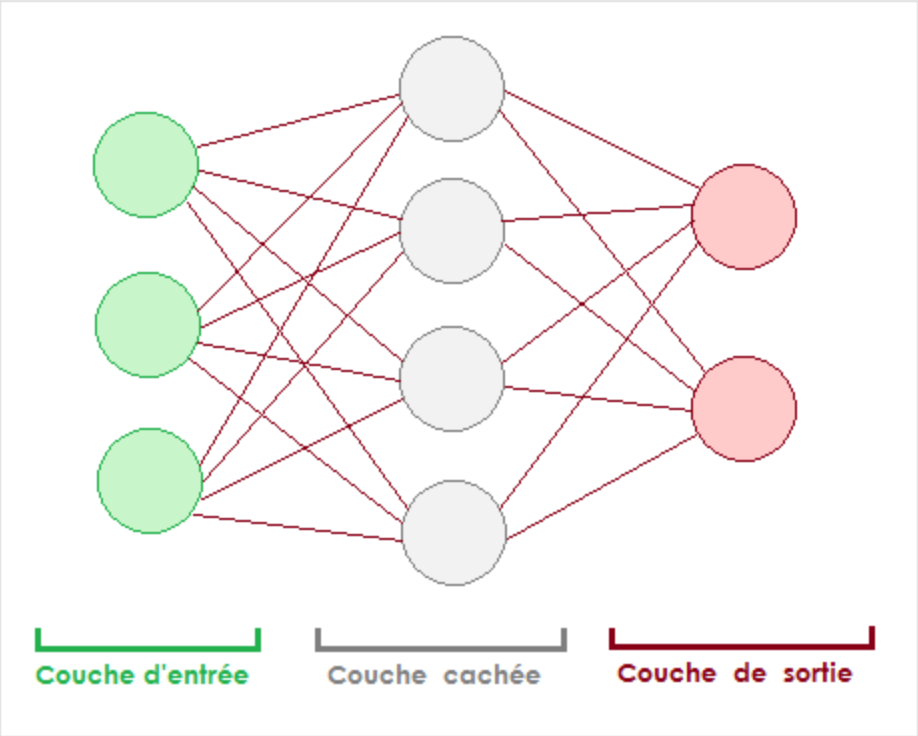

Figure 35 - Réseau de neurones avec couche de nœuds d'entrée, couche de nœuds de sortie et couche cachée[20]

8.3.2 Description du modèle

Les préférences des utilisateurs sont considérées comme l'un des facteurs importants dans les systèmes de recommandation. Le fait de découvrir et d'exploiter leurs changements de manière efficace consiste un défi dans le processus de recommandation.

Plus concrètement, soit Item = ($item_1$, $item_2$, …, $item_{|item|}$) l'ensemble de tous les articles.

$$m'_i = E_1 * m_i \quad (10)$$

où m_i est la seule représentation *One-Hot* de l'article, $E_1 \in R^{d*|I|}$ est la couche d'intégration des éléments, d est la longueur du vecteur de l'élément embarqué et $|I|$ est l'ensemble de tous les éléments.

$$f'_j = E_2 * f_i \quad (11)$$

[20] https://jcrisch.wordpress.com/2015/04/02/les-reseaux-de-neurones/ consulté le 08/Nov/2019

où f_i^j est la seule représentation *OneHot* de la fonctionnalité $j^{ème}$ de l'élément $i^{ème}$, $E_2 \in R^{d'*|F|}$ est l'intégration de la couche de fonctionnalités, d est la longueur du vecteur embarqué et $|F|$ est l'ensemble de toutes les caractéristiques.

$$f'_i = \frac{1}{n_i} \sum_{j=1}^{n_i} f'_{ij} \quad (12)$$

Où n_i est le nombre de fonctionnalités associées à l'article $i^{ème}$ et f'_i est la moyenne du vecteur d'intégration de toutes les fonctionnalités associées au $i^{ème}$ article.

$$V = V_i + V_f \quad (13)$$

Où V_i représente la variation entre les vecteurs d'éléments embarqués et V_f se réfère à la variation entre les vecteurs de fonctionnalités intégrées. Ils sont simplement ajoutés pour représenter la stabilité des intérêts des utilisateurs.

Les composants *GRU* (définis dans la section 8.3.1) analysent les vecteurs embarqués pour obtenir les vecteurs contextuels C_i et C_f qui sont ensuite concaténés pour générer le vecteur contextuel final *C.* Le vecteur final est ensuite alimenté par 4 couches denses. Dans les trois premières couches non linéaires, le vecteur sera traité dans l'équation suivante :

$$C_i = (W_i C_{i-1} + b_i) \quad (14)$$

$i \in (1, 2, 3)$ se réfère au numéro de couche non linéaire. La couche finale dense C_4 partage la même taille que le nombre total d'articles suivis d'une couche Soft-argmax qui donne aux utilisateurs la préférence possible pour chaque élément.

$$O = W_4 C_3 + b_4 \quad (15)$$

$$\beta_u = \frac{2}{1+e^{V_u}} \quad (16)$$

$$(u_l = i_i | i_{i-1}, i_{i-2}, \ldots, s_{i-m}) = \frac{e^{\beta_u o_l}}{\sum_{k=1}^{|item|} e^{\beta_u o_k}} \quad (17)$$

V_u est la variation de User u obtenue à partir de l'équation (13). β_u est calculée pour modifier la distribution de probabilité pour chaque utilisateur o_i se réfère à l'article $i^{ème}$ dans O.

Après cette couche, l'échantillonnage est adapté pour générer K recommandations. Nous exécutons la technique d'échantillonnage décrite dans l'Algorithme 4. Les recommandations générées par cette technique et la Soft-couche argmax assurent l'intégration du principe central des algorithmes de recommandation et la prise en compte de la stabilité de l'intérêt de l'utilisateur.

Algorithme 4 - Échantillonnage pour générer K recommandations

Input: Probability distribution of all items: P_u and
the user is previously select item set:U_I.
Output: K recommendations sampled from all items.
$RecommendationSet$ = ()
repeat
P_{sum} = $sum(P_u)$;
$Random_P$ = (0, P_{sum});
P_{add} = 0;
for i = 1 to $P_{u.Size}$ do
P_{add} + = $P_u[i]$;
if P_{add} ≥ Random$_P$ then
$RecommendedItem$ = i;
$[i]$ = 0;
break;
end
end
if $RecommendedItem$ U_I then
$RecommendationSet.append(RecommendedItem)$;
end
until $RecommendationSet.Size \geq K$;

Dans notre méthode, les utilisateurs instables dans leurs préférences auront des valeurs de βu plus petits et également des distributions de probabilité plus adéquates. Ceci

signifie qu'ils se feront recommander, avec une probabilité plus élevée, des choses différentes de leurs intérêts à court terme. Cependant, les utilisateurs qui sont stables dans leurs goûts, auront des valeurs de βu plus grandes et également une distribution de probabilité plus approximative. Ceci signifie qu'ils se feront probablement recommander des choses similaires à leurs intérêts récents. En conséquence, notre méthode assure une recommandation plus personnalisée.

8.3.3 Exemple d'application

Afin de mieux comprendre le modèle proposé, prenons un exemple concret. Soit Bob un utilisateur avec huit articles en entrée. La méthode d'échantillonnage pour générer K recommandations est utilisée.

Pour ce faire, la tendance consiste à choisir les Top k articles qui ont les probabilités prévues les plus élevées. Dans ce cas, Bob reçoit des recommandations qui satisfont ses intérêts précédents. Dans cet exemple, si k = 3, les articles *Item2, Item3 and Item4* sont recommandés à Bob parce que ces trois items partagent la plus grande similarité avec ses intérêts récents. Toutefois, ceci néglige le fait que ses prochains intérêts pourraient être ou non semblables à ses intérêts précédents. En se basant sur les données historiques, si Bob change ses intérêts ou modifie ses choix, il ne sera pas satisfait des recommandations du système.

Dans la Figure 36, nous présentons un graphique décrivant les prédictions. Les méthodes de la littérature peuvent prédire les distributions de probabilité comme le montre la barre rouge de la même figure. Regardons l'historique des préférences de Bob. Si la variation est faible, nous supposons que Bob est stable dans ses préférences et préfère des éléments similaires aux précédents.

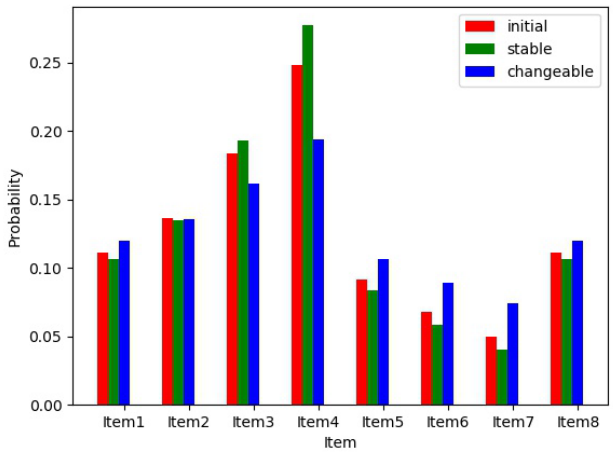

Figure 36 - Distribution de la probabilité

Comme le montre la barre verte de la Figure 36, comparativement au résultat initial, les éléments similaires aux éléments précédents ont plus de probabilité d'être recommandés comme $Item3$, $Item4$. Tandis que les éléments différents des articles précédents peuvent être moins recommandés. Si $K = 3$, dans notre méthode d'échantillonnage, il est fort possible que $Item3$, $Item4$ soient recommandés. $Item1$ ou $Item2$ peuvent également être recommandés tandis que d'autres articles n'ont presque aucune chance d'être recommandés. Ce qui est intéressant c'est que les 3 recommandations peuvent satisfaire Bob parce qu'elles correspondent à ce que le réseau prédit.

Cependant, si la variation des éléments de l'historique de Bob est élevée, ceci signifie que Bob a tendance à aimer des choses différentes de ses éléments précédents. Dans ce cas, les recommandations doivent être en mesure de satisfaire ses préférences selon lesquelles il va aimer quelque chose de différent et nouveau. Comme le montre la barre bleue de la Figure 36, par rapport au résultat initial, les éléments similaires aux éléments précédents ont une faible probabilité d'être recommandés comme $Item3$, $Item4$. D'autres éléments qui peuvent être différents de ses intérêts précédents peuvent avoir une grande probabilité d'être recommandés. En effet, des éléments comme $Item5$, $Item6$, $Item7$, dans les algorithmes de recommandations existants, peuvent ne pas être recommandés, alors qu'ils pourraient avoir une haute probabilité d'être recommandés pour Bob dans notre méthode d'échantillonnage, où la distribution de probabilité prédite devient plus adéquate. Finalement, il y aura une probabilité que $Item4$, $Item1$, $Item5$ puissent également être

recommandés. Dans ce cas, il se peut que $Item4$ et $Item5$ soient différents et nouveaux, avec une probabilité de pouvoir satisfaire Bob par rapport à ce qu'il désirait.

En conséquence, dans notre modèle, les utilisateurs avec une variance élevée dans leurs intérêts appartiennent au groupe qui reçoit à une grande probabilité des recommandations avec différents nouveaux items.

Nous utilisons la probabilité pour évaluer le rendement du modèle. Par commodité, nous utilisons la log-vraisemblance négative (*Negative Log-Likelihood ou NLL*) comme fonction de perte (P. Li*, et al.*, 2017), nous définissons l'objectif d'optimisation comme suit.

$$argmin_{E_{k,}\ G_{p,}\ W_{l,}\ b_l} - \sum_u \sum_l logP(u_l = i_i |\ i_{i\text{-}1}, i_{i\text{-}1}, \ldots, i_{i\text{-}m}) \qquad (18)$$

Où u se réfère à des utilisateurs spécifiques, l se réfère à des éléments spécifiques. u_l est l'élément réel se produisant après le m éléments donnés. $E_{k,\in 1,2}$ est la matrice d'intégration des éléments et des caractéristiques de l'article respectivement. GP est les paramètres en *GRU*. $W_{l,\in 1,2,3,4}$ et $b_{l,l\in 1,2,3,4}$ sont les paramètres de poids et les paramètres de biais dans les couches denses. L'ensemble de données d'entraînement pour entraîner le modèle est réitéré.

8.4 Expérience

Dans cette section, l'expérience menée avec l'ensemble de données est présentée. De plus, nous décrivons la mise en œuvre et la façon dont nous menons l'entraînement du modèle. À la fin de la section, nous évaluons les résultats et en discutons.

8.4.1 Groupe de données

Les expériences sont réalisées sur la base de données des films $MovieLens1M$[21] parce que la recommandation de films ressemble à des problèmes que nous essayons de résoudre. Le Tableau 19 présente les statistiques de cet ensemble de données.

[21] MovieLens1M 2003. MovieLens1M Dataset. Retrieved Feb, 2003 from https://grouplens.org/datasets/movielens/1m/

Cette base de données contient 6040 utilisateurs et 3883 films. Chaque film a une étiquette décrivant son « Genre ». Le *Genre* décrit les caractéristiques du film telles qu'action, aventure, horreur, romantique ou autre. Le total des genres est 18. Pour un film en particulier, le nombre maximum de genres auxquels il appartient est de 6, et le nombre minimum est de 1. Le nombre moyen de films qu'un utilisateur a vus une fois est de 165,60 et le nombre moyen de genres par film est de 1,65.

Tableau 19 - Statistiques de la base de données

Description	**Value**
Total Users	6040
Total Movies	3883
Total Features(Genres)	18
Average Movies per Person	165.60
Average Features(Genres) per Movie	1.65

En nous basant sur cette base de données, la tâche de recommandation est transformée en un problème de séquence qui intègre l'analyse des caractéristiques des éléments. Dans notre méthode, la taille de la fenêtre est réglée à 6 pour analyser les données de séquence. Nous avons utilisé tous les utilisateurs et les films de la base de données pour entraîner le modèle et évaluer notre travail.

8.4.2 Implémentation

Nous utilisons 80 % des données comme l'ensemble de données d'entraînement; le reste des 20 % constituent l'ensemble de données de test. Dans nos expériences, la performance de notre méthode est évaluée, elle mesure la stabilité de l'intérêt de l'utilisateur et l'examine lors de la formulation des recommandations pour mieux servir les utilisateurs. Nous avons mis en œuvre notre méthode à l'aide de PyTorch[22] utilisé avec Adam Optimizer (Ketkar, 2017), avec un taux d'apprentissage de 0,001. La taille de la fenêtre de séquence d'entrée a été réglée à six. Item (Movie) et Feature (Genre) taille d'intégration

[22] Pytorch [n. d.]. Pytorch. https://pytorch.org/ consulted on 16/Jan/2019

ont été fixés à 50. Dans notre réseau, nous utilisons la régularisation de l'abandon avec une probabilité d'écartement de 0,1 pour éviter les problèmes de surcharge.

8.4.3 Évaluation et Discussion

Nous avons inclus tous les utilisateurs de $MovieLens1M$ et avons évalué notre méthode en nous basant sur les métriques d'évaluation suivantes : $Recall@k$ (noté par $Accuracy@k$) et $MeanReciprocalRank$ (noté par $MRR@k$), en considérant k=10 (Shani & Gunawardana, 2011). Notons que :

$Recall@k$ ou le rappel à k calcule la proportion des éléments pertinents trouvés dans les k premières recommandations (S. Wang*, et al.*, 2018).

$MRR@k$ ou Classement réciproque moyen à k calcule le classement moyen de la première recommandation pertinente dans les k premières recommandations (G. Guo*, et al.*, 2015).

Notre méthode est comparée à certains modèles de base et méthodes de pointe (Hadash*, et al.*, 2018). Les résultats sont présentés dans le Tableau 20 et montrent que notre méthode surpasse ces méthodes en $Recall@10$, mais n'atteint pas les meilleures performances en $MRR@10$. L'excellente performance sur $Recall@10$ illustre l'importance de prendre en considération la stabilité des intérêts des utilisateurs parce que nos recommandations peuvent mieux correspondre aux choix réels des utilisateurs. En d'autres termes, une performance au niveau de Recall@k signifie un meilleur résultat des éléments pertinents recommandés dans les premiers éléments. Toutefois, la caractéristique aléatoire de la méthode d'échantillonnage n'a pas pu garantir des prédictions de séquences précises qui sont mesurées par $MRR@k$.

Tableau 20 - Résultats de l'expérience

Algorithm	***Recall*@10**	**MRR@10**
Popularity	0.0278	0.0035
SVD	0.0673	0.0120
CDAE	0.0926	0.0146
BPR	0.0659	0.0222
RnR(CDAE, SVD)	0.1236	0.0497

UIS	**0.1251**	**0.0347**

8.5 Conclusion

Dans cette recherche, nous utilisons un réseau de neurones qui non seulement modélise les intérêts des utilisateurs, mais tient compte également de leur stabilité d'intérêt. Notre performance sur $MovieLens1M$ dépasse les modèles de base et certaines méthodes de pointe qui considèrent la stabilité de l'intérêt des utilisateurs. Notre travail est de donner aux utilisateurs des options par rapport à ce qu'ils veulent vraiment à l'heure actuelle plutôt que ce qu'ils peuvent vouloir uniquement en fonction de leurs historiques. Dans nos travaux futurs, nous intégrerons ce travail dans de vrais sites Web. Les commentaires des utilisateurs nous aideront à mieux mesurer et améliorer notre travail. Nous chercherons des façons plus variées et efficaces de modéliser la stabilité des intérêts des utilisateurs. De plus, la stabilité des intérêts n'est qu'une des caractéristiques des intérêts des utilisateurs. Nous investiguerons sur la façon de trouver plus de caractéristiques reliées à l'intérêt de l'utilisateur.

Chapitre 9 : Conclusions et travaux futurs

Le fait que les services en ligne envahissent nos vies quotidiennement ne peut pas être négligé. Dans le commerce électronique, deux domaines de services en ligne nous intéressent : les paiements en ligne et les systèmes de recommandation. Vu leur facilité d'utilisation et leur nécessité, le nombre de transactions et des sites d'achats augmentent exponentiellement. Cependant, différents enjeux s'interpellent dans ces domaines au sujet de la préservation de la vie privée, de la confiance en ligne et de la prise de décision.

Au sujet des paiements en ligne, notre objectif dans cette thèse est d'identifier les caractéristiques du site d'achat qui influencent la prise de décision de payer en ligne. Dans le même contexte, nous nous sommes concentrés sur les préoccupations des usagers au sujet des craintes en ligne (*OCF*) et avons examiné les facteurs par rapport à la confiance, à la perception de la sécurité des paiements ainsi qu'à leur effet conjoint. À savoir *la facilité d'utilisation, la qualité des informations, et les signes de sécurité*. Deux aspects fondamentaux, qui sont les préoccupations des clients en matière de vie privée et leur perception envers la crainte de perte financière ont été considérés.

Partant de cet objectif, nous avons proposé une plateforme holistique « *E-PPSM* » qui, à la fois, assure le contrôle des transactions, la supervision des achats en ligne et la protection des informations personnelles. De plus, notre plateforme supporte les achats multiples en intégrant le principe du plan de paiement conditionnel. À partir de cette plateforme, nous visons à fournir un environnement de paiement en ligne par l'intermédiaire de cartes de crédit virtuelles incluant toutes les étapes qui mènent à compléter un achat en ligne. Cela dit, le détenteur de la carte de crédit est capable de configurer des conditions publiques et privées sans obligation de divulguer les informations personnelles et financières. Une configuration similaire est ajoutée au niveau des usagers détenteurs de la carte de crédit virtuelle, mais cette fois-ci en assurant la protection des informations personnelles et financières envers le marchand. Les détenteurs de carte de crédit sont capables de définir leurs préférences et de fournir leurs commentaires.

Dans *E-PPSM*, nous avons considéré la personnalisation des sites en commerce électronique tout en sensibilisant les usagers au sujet de la protection de vie privée et de la

sécurité de leurs informations financières. Pour cet objectif, nous avons développé un nouveau site Web « **PAYCTRI** » et simulé une expérience de magasinage en ligne avec un questionnaire et un quiz pour vérifier le niveau de connaissances sur les vulnérabilités et les mesures de précautions à prendre. L'importance de sensibiliser les personnes à la cybersécurité est cruciale. Nos constatations nous ont menés à deux ensembles d'actions : réduire le risque perçu de cybercriminalité dans les activités en ligne tout en augmentant le niveau de connaissance en cybersécurité.

Au sujet des recommandations en ligne, de nombreux sites de commerce électronique personnalisent leur contenu, notamment Netflix (recommandations de films), Amazon (suggestions de produits) et Yelp (critiques d'entreprises), mais occasionnent de sérieux risques concernant la vie privée des utilisateurs. Les préoccupations en matière de protection de vie privée sont dues aux recommandations de filtrage collaboratif visant à préserver la vie privée. Ainsi, du fait d'un manque d'équilibre avec l'utilité des données, nous avons proposé un nouveau modèle qui, à la fois, préserve la vie privée et garde l'utilité des données partagées et publiées en ligne. Notre modèle est basé sur l'algorithme « *k*-means » et sur le modèle « *k*-coRating ». Nous avons démontré que notre modèle performe mieux avec moins de modifications et une meilleure prédiction.

Toujours dans le cadre des systèmes de recommandation, d'autres contributions sont mises en relief dans cette thèse. Nous avons proposé un nouveau modèle à base de réseaux de neurones pour prédire les prochaines suggestions/recommandations en nous basant sur un ensemble d'informations déjà acquises sur cet utilisateur et sur ceux qui lui sont similaires. Le nouveau modèle traite la stabilité des préférences des utilisateurs, ceci consiste à générer des recommandations innovantes et différentes aux utilisateurs dont les préférences peuvent varier avec le temps. Toutefois, notre modèle fournit des recommandations similaires à celles du passé pour les usagers dont les préférences sont plus stables.

Quant aux travaux futurs au sujet des multi-craintes, notre thèse s'est intéressée aux attributs du site Web dans le contexte de la confiance électronique et de la prise de décision. Un travail plus complet intégrant à la fois d'autres facteurs avec leurs déterminants et conséquences reste à mener. Par exemple, le fait de s'intéresser au rôle des tiers dans les paiements en ligne.

Dans notre plateforme proposée (E-*PPSM*), nous avons centré notre réflexion sur une vue globale qui supporte à la fois des achats multiples ainsi que des paiements conditionnels et conserve la vie privée. Une vue plus technique pourrait permettre dans le futur une amélioration de la plateforme. D'autres travaux peuvent approfondir ce sujet en intégrant l'impact de l'expertise de l'internaute : il s'agit ici de l'aptitude à réaliser, avec plus ou moins d'aisance, des tâches sur Internet (par exemple chercher une information spécifique, faire une commande, réaliser un achat, etc.). Bien que les recherches intégrant l'expertise par rapport à Internet soient de plus en plus nombreuses, curieusement, la relation entre l'expertise et la confiance n'a pas fait l'objet de beaucoup de travaux. Des recherches ultérieures pourraient tenter d'étudier la question.

Aux dépens de la simulation de l'expérience en ligne, il convient de souligner quelques limitations que nous aimerions résoudre dans un futur proche. La première limitation inhérente à notre recherche est celle de ne pas prendre en considération la possibilité d'interaction directe avec les participants de (*MTURK*). Une seconde limitation réside dans les commentaires des participants qui peuvent être considérés en utilisant le traitement du langage naturel afin d'extraire des remarques plus pertinentes qui peuvent enrichir les résultats. Ces deux aspects non soulevés dans notre thèse pourront être l'objet de travaux futurs.

Bibliographie

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2018). Privacy and Human Behavior in the Information Age. *The Cambridge Handbook of Consumer Privacy*, 184.

Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior *Economics of information security* (pp. 165-178): Springer.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*(2), 249-274.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442-492.

Adomavicius, G., Bockstedt, J. C., Curley, S. P., & Zhang, J. (2017). Effects of online recommendations on consumers' willingness to pay. *Information Systems Research, 29*(1), 84-102.

Adomavicius, G., & Gupta, A. (2005). Toward comprehensive real-time bidder support in iterative combinatorial auctions. *Information Systems Research, 16*(2), 169-185.

Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE Transactions on Knowledge & Data Engineering*(6), 734-749.

Ahn, H. J. (2008). A new similarity measure for collaborative filtering to alleviate the new user cold-starting problem. *Information Sciences, 178*(1), 37-51.

Aïmeur, E. (2014). Online Privacy: Risks, Challenges, and New Trends *Risks and Security of Internet and Systems* (pp. 263-266): Springer.

Aladwani, A. M. (2018). A quality-facilitated socialization model of social commerce decisions. *International Journal of Information Management, 40*, 1-7.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: a survey. *Computers & Security, 68*, 160-196.

Alese, B., & Ayeni, O. (2013). Consumer Trust Model in Online Transaction. *International Journal of Computer Applications, 72*(17).

Amatriain, X., & Basilico, J. (2016). *Past, present, and future of recommender systems: An industry perspective.* Paper presented at the Proceedings of the 10th ACM Conference on Recommender Systems.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly, 34*(3), 613-643.

Andrade, A. A., Lopes, V. V., & Novais, A. Q. (2012). *Quantifying the impact on distrust of e-commerce trust factors: A non-parametric study.* Paper presented at the Internet Technology And Secured Transactions, 2012 International Conference for.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin *Financial Cryptography and Data Security* (pp. 34-51): Springer.

Antoniou, G., & Batten, L. (2011). E-commerce: protecting purchaser privacy to enforce trust. *Electronic commerce research, 11*(4), 421-456.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443.

Arora, A., Nandkumar, A., & Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers, 8*(5), 350-362.

Ashrafi, M. Z., & Ng, S. K. (2009). Privacy-preserving e-payments using one-time payment details. *Computer Standards & Interfaces, 31*(2), 321-328. doi: http://dx.doi.org/10.1016/j.csi.2008.04.001

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., & Starin, D. (2009). *Persona: an online social network with user-defined privacy.* Paper presented at the ACM SIGCOMM Computer Communication Review.

Bagherifard, K., Rahmani, M., Nilashi, M., & Rafe, V. (2017). Performance improvement for recommender systems using ontology. *Telematics and Informatics, 34*(8), 1772-1792.

Bai, Y., Yao, Z., & Dou, Y.-F. (2015). Effect of social commerce factors on user purchase behavior: An empirical investigation from renren. com. *International Journal of Information Management, 35*(5), 538-550.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency *Financial cryptography and data security* (pp. 399-414): Springer.

Barth, S., & de Jong, M. (2017). The Privacy Paradox–Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior–A Systematic Literature Review. *Telematics and Informatics*.

Bauer, J. M., & Van Eeten, M. J. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy, 33*(10-11), 706-719.

Beach, L. R. (1993). Broadening the definition of decision making: The role of prechoice screening of options. *Psychological Science, 4*(4), 215-220.

Beck, J. E., & Woolf, B. P. (2000). *High-level student modeling with machine learning.* Paper presented at the International Conference on Intelligent Tutoring Systems.

Bella, G., Giustolisi, R., & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *computers & security, 30*(8), 705-718.

Bella, G., Massacci, F., Paulson, L. C., & Tramontano, P. (2001). *Making sense of specifications: the formalization of set.* Paper presented at the Security Protocols.

Beltramo, T., Blalock, G., Levine, D. I., & Simons, A. M. (2015). The effect of marketing messages and payment over time on willingness to pay for fuel-efficient cookstoves. *Journal of Economic Behavior & Organization, 118*, 333-345. doi: http://dx.doi.org/10.1016/j.jebo.2015.04.025

Bengio, Y., & Senécal, J.-S. (2008). Adaptive importance sampling to accelerate training of a neural probabilistic language model. *IEEE Transactions on Neural Networks, 19*(4), 713-722.

Bettini, C., & Riboni, D. (2015). Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing, 17*, 159-174.

Bichler, M., Gupta, A., & Ketter, W. (2010). Research commentary—designing smart markets. *Information Systems Research, 21*(4), 688-699.

Bos, J. W., Castryck, W., Iliashenko, I., & Vercauteren, F. (2017). *Privacy-friendly forecasting for the smart grid using homomorphic encryption and the group method of data handling.* Paper presented at the International Conference on Cryptology in Africa.

Brafman, R. I., Heckerman, D., & Shani, G. (2003). *Recommendation as a Stochastic Sequential Decision Problem.* Paper presented at the ICAPS.

Buckman, J., Roy, A., Raffel, C., & Goodfellow, I. (2018). Thermometer encoding: One hot way to resist adversarial examples.

Burke, R. (2002). Hybrid recommender systems: Survey and experiments. *User modeling and user-adapted interaction, 12*(4), 331-370.

Burke, R. R. (2002). Technology and the customer interface: what consumers want in the physical and virtual store. *Journal of the academy of Marketing Science, 30*(4), 411-432.

Byrne, B. M. (2013). *Structural equation modeling with Mplus: Basic concepts, applications, and programming*: Routledge.

Camenisch, J., & Stadler, M. (1997). Efficient group signature schemes for large groups *Advances in Cryptology—CRYPTO'97* (pp. 410-424): Springer.

Cappiello, C., Plebani, P., & Vitali, M. (2018). A data utility model for data-intensive applications in fog computing environments *Fog Computing* (pp. 183-202): Springer.

Carbonell, M., Sierra, J. M., & Lopez, J. (2009). Secure multiparty payment with an intermediary entity. *computers & security, 28*(5), 289-300.

Carminati, B., Ferrari, E., & Tran, N. H. (2016). Trustworthy and effective person-to-person payments over multi-hop MANETs. *Journal of Network and Computer Applications, 60*, 1-18. doi: http://dx.doi.org/10.1016/j.jnca.2015.11.011

Casado-Aranda, L.-A., Liébana-Cabanillas, F., & Sánchez-Fernández, J. (2018). A Neuropsychological Study on How Consumers Process Risky and Secure E-payments. *Journal of Interactive Marketing, 43*, 151-164.

Cellary, W., & Rykowski, J. (2015). Challenges of Smart Industries–Privacy and payment in Visible versus Unseen Internet. *Government Information Quarterly*.

Cerdeiro, D. A. (2017). Contagion exposure and protection technology. *Games and Economic Behavior, 105*, 230-254.

Chang, Y.-S., & Fang, S.-R. (2013). Antecedents and distinctions between online trust and distrust: Predicting high-and low-risk internet behaviors. *Journal of Electronic Commerce Research, 14*(2), 149.

Chapelle, O., & Wu, M. (2010). Gradient descent optimization of smoothed information retrieval metrics. *Information retrieval, 13*(3), 216-235.

Chase, R. B., & Dasu, S. (2001). Want to perfect your company's service? Use behavioral science. *Harvard business review, 79*(6), 78-84, 147.

Chatterjee, P., & Rose, R. L. (2012). Do payment mechanisms change the way consumers perceive products? *Journal of Consumer Research, 38*(6), 1129-1139.

Chaum, D. (1983). *Blind signatures for untraceable payments.* Paper presented at the Advances in cryptology.

Chaum, D., & Van Heyst, E. (1991). *Group signatures.* Paper presented at the Advances in Cryptology—EUROCRYPT'91.

Chen, A., Lu, Y., & Wang, B. (2017). Customers' purchase decision-making process in social commerce: A social learning perspective. *International Journal of Information Management, 37*(6), 627-638.

Chen, J. V., Yen, D. C., Kuo, W.-R., & Capistrano, E. P. S. (2016). The antecedents of purchase and re-purchase intentions of online auction consumers. *Computers in Human behavior, 54*, 186-196.

Chen, K.-C., Yu, C.-M., Tai, B.-C., Li, S.-C., Tsou, Y.-T., Huang, Y.*, et al.* (2017). *Data-Driven Approach for Evaluating Risk of Disclosure and Utility in Differentially Private Data Release.* Paper presented at the Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on.

Chen, X., Li, J., Ma, J., Lou, W., & Wong, D. S. (2014). New and efficient conditional e-payment systems with transferability. *Future Generation Computer Systems, 37*, 252-258.

Chen, X., Zhang, F., & Liu, S. (2007). ID-based restrictive partially blind signatures and applications. *Journal of Systems and Software, 80*(2), 164-171.

Chen, Y.-C., Horng, G., & Huang, C.-C. (2009). *Privacy protection in on-line shopping for electronic documents.* Paper presented at the Information Assurance and Security, 2009. IAS'09. Fifth International Conference on.

Chen, Y.-C., Horng, G., & Huang, C.-C. (2014). Privacy protection in on-line shopping for electronic documents. *Information Sciences, 277*, 321-326.

Chen, Y., Yan, X., Fan, W., & Gordon, M. (2015). The joint moderating role of trust propensity and gender on consumers' online shopping behavior. *Computers in Human Behavior, 43*, 272-283.

Chiu, C. M., Wang, E. T., Fang, Y. H., & Huang, H. Y. (2014). Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information Systems Journal, 24*(1), 85-114.

Cho, J., Aribarg, A., & Manchanda, P. (2017). The value of measuring customer satisfaction.

Cho, K., Merrienboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H.*, et al.* (2017). Learning phrase representations using rnn encoder-decoder for statistical machine translation. Comput Sci. 2014.

Choi, M., Law, R., & Heo, C. Y. (2016). Shopping destinations and trust–tourist attitudes: Scale development and validation. *Tourism Management, 54*, 490-501.

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J. C. (2004). *Client-Side Defense Against Web-Based Identity Theft.* Paper presented at the NDSS.

Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. J. a. p. a. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling.

Commission, F. T. (2018). Consumer sentinel network data book 2017. *Retrieved from*.

Covington, P., Adams, J., & Sargin, E. (2016). *Deep neural networks for youtube recommendations.* Paper presented at the Proceedings of the 10th ACM conference on recommender systems.

Cui, F., Lin, D., & Qu, H. (2018). The impact of perceived security and consumer innovativeness on e-loyalty in online travel shopping. *Journal of Travel & Tourism Marketing*, 1-16.

Cui, M., & Pan, S. L. (2015). Developing focal capabilities for e-commerce adoption: A resource orchestration perspective. *Information & Management, 52*(2), 200-209.

Dahlberg, T., Bouwman, H., Cerpa, N., & Guo, J. (2015). *M-Payment-How Disruptive Technologies Could Change The Payment Ecosystem.* Paper presented at the ECIS.

Das, M. L., & Samdaria, N. (2014). On the security of SSL/TLS-enabled applications. *Applied Computing and informatics, 10*(1-2), 68-81.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7.

Dixon, C. J., & Pinckney, T. (2013). Indicating website reputations during website manipulation of user information: Google Patents.

Dunn, J. (2004). Survey shows online security perception gap between experts, users. *Knight Ridder Tribune Business News, 17*(1).

Dwork, C. (2008). *Differential privacy: A survey of results.* Paper presented at the International Conference on Theory and Applications of Models of Computation.

Eagly, A. H., & Chaiken, S. (1993). The nature of attitudes. *The psychology of attitudes*, 1-21.

Eisenstein, E. M. (2008). Identity theft: an exploratory study with implications for marketers. *Journal of Business Research, 61*(11), 1160-1172.

El Haddad, G., Aïmeur, E., & Hage, H. (2018). *Understanding Trust, Privacy and Financial Fears in Online Payment.* Paper presented at the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

El Haddad, G., Hage, H., & Aïmeur, E. (2017). *E-payment plan: a conditional multi-payment scheme based on user personalization and plan agreement.* Paper presented at the International Conference on E-Technologies.

El Haddad, G., Shahab, A., & Aïmeur, E. (2018). *Exploring User Behavior and Cybersecurity Knowledge-An experimental study in Online Shopping.* Paper presented at the 2018 16th Annual Conference on Privacy, Security and Trust (PST).

Elahi, M., Ricci, F., & Rubens, N. (2016). A survey of active learning in collaborative filtering recommender systems. *Computer Science Review, 20*, 29-50.

Enterprise, V. (2017). 2017 Data breach investigations report.

Erkan, I., & Evans, C. (2018). Social media or shopping websites? The influence of eWOM on consumers' online purchase intentions. *Journal of Marketing Communications, 24*(6), 617-632.

Faísca, J. G., & Rogado, J. Q. (2016). *Decentralized semantic identity.* Paper presented at the Proceedings of the 12th International Conference on Semantic Systems.

Faqih, K. M. (2016). An empirical analysis of factors predicting the behavioral intention to adopt Internet shopping technology among non-shoppers in a developing country context: Does gender matter? *Journal of Retailing and Consumer Services, 30*, 140-164.

Filieri, R., Alguezaui, S., & McLeay, F. (2015). Why do travelers trust TripAdvisor? Antecedents of trust towards consumer-generated media and its influence on recommendation adoption and word of mouth. *Tourism Management, 51*, 174-185.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, 382-388.

Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study–A case of China. *Computers in Human Behavior, 53*, 249-262.

Gneezy, A., Gneezy, U., Nelson, L. D., & Brown, A. (2010). Shared social responsibility: A field experiment in pay-what-you-want pricing and charitable giving. *Science, 329*(5989), 325-327.

Gómez, J. A., Arévalo, J., Paredes, R., & Nin, J. (2018). End-to-end neural network architecture for fraud scoring in card payments. *Pattern Recognition Letters, 105*, 175-181.

Gommans, L., Vollbrecht, J., Gommans-de Bruijn, B., & de Laat, C. (2015). The Service Provider Group framework: A framework for arranging trust and power to facilitate authorization of network services. *Future Generation Computer Systems, 45*, 176-192.

Gong, Y., & Zhang, Q. (2016). *Hashtag Recommendation Using Attention-Based Convolutional Neural Network.* Paper presented at the IJCAI.

Gray, J. M. (2015). How Apple Pay Coincides with the Consumer Financial Protection Act: Will Apple Become a Regulated Entity. *J. High Tech. L., 16*, 170.

Guo, G., Zhang, J., Sun, Z., & Yorke-Smith, N. (2015). *LibRec: A Java Library for Recommender Systems.* Paper presented at the UMAP Workshops.

Guo, G., Zhang, J., Thalmann, D., & Yorke-Smith, N. (2014). Leveraging prior ratings for recommender systems in e-commerce. *Electronic Commerce Research and Applications, 13*(6), 440-455.

Guo, H., Tang, R., Ye, Y., Li, Z., & He, X. (2017). DeepFM: a factorization-machine based neural network for CTR prediction. *arXiv preprint arXiv:1703.04247*.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications, 28*(12), 3629-3654.

Hadash, G., Shalom, O. S., & Osadchy, R. (2018). *Rank and rate: multi-task learning for recommender systems.* Paper presented at the Proceedings of the 12th ACM Conference on Recommender Systems.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

Hagemann, N., O'Mahony, M. P., & Smyth, B. (2018). *Module advisor: a hybrid recommender system for elective module exploration.* Paper presented at the Proceedings of the 12th ACM Conference on Recommender Systems.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5): Prentice hall Upper Saddle River, NJ.

Hajli, N. (2015). Social commerce constructs and consumer's intention to buy. *International Journal of Information Management, 35*(2), 183-191.

Han, J., Yu, J., Lu, J., Peng, H., & Wu, J. (2017). *An Anonymization Method to Improve Data Utility for Classification.* Paper presented at the International Symposium on Cyberspace Safety and Security.

Hannak, A., Soeller, G., Lazer, D., Mislove, A., & Wilson, C. (2014). *Measuring price discrimination and steering on e-commerce web sites.* Paper presented at the Proceedings of the 2014 conference on internet measurement conference.

Hara, K., Adams, A., Milland, K., Savage, S., Callison-Burch, C., & Bigham, J. (2017). A Data-Driven Analysis of Workers' Earnings on Amazon Mechanical Turk. *arXiv preprint arXiv:1712.05796*.

Harper, F. M., & Konstan, J. A. (2016). The movielens datasets: History and context. *Acm transactions on interactive intelligent systems (tiis), 5*(4), 19.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102-113.

Haws, K. L., Bearden, W. O., & Nenkov, G. Y. (2012). Consumer spending self-control effectiveness and outcome elaboration prompts. *Journal of the Academy of Marketing Science, 40*(5), 695-710.

He, R., & McAuley, J. (2016). *Ups and downs: Modeling the visual evolution of fashion trends with one-class collaborative filtering.* Paper presented at the proceedings of the 25th international conference on world wide web.

He, X., & Chua, T.-S. (2017). *Neural factorization machines for sparse predictive analytics.* Paper presented at the Proceedings of the 40th International ACM SIGIR conference on Research and Development in Information Retrieval.

He, X., Liao, L., Zhang, H., Nie, L., Hu, X., & Chua, T.-S. (2017). *Neural collaborative filtering.* Paper presented at the Proceedings of the 26th International Conference on World Wide Web.

He, X., Zhang, H., Kan, M.-Y., & Chua, T.-S. (2016). *Fast matrix factorization for online recommendation with implicit feedback.* Paper presented at the Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval.

Heath, S. (2017). Systems and methods for mobile and online payment systems for purchases related to mobile and online promotions or offers provided using impressions tracking and analysis, location information, 2D and 3D mapping, mobile mapping, social media, and user behavior and: Google Patents.

Herlocker, J. L., Konstan, J. A., & Riedl, J. (2000). *Explaining collaborative filtering recommendations.* Paper presented at the Proceedings of the 2000 ACM conference on Computer supported cooperative work.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer Fear of Online Identity Theft: Scale Development and Validation. *Journal of Interactive Marketing, 30*, 1-19.

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236-245.

Hinton, G., Deng, L., Yu, D., Dahl, G., Mohamed, A.-r., Jaitly, N.*, et al.* (2012). Deep neural networks for acoustic modeling in speech recognition. *IEEE Signal processing magazine, 29*.

Ho, K. K., & See-To, E. W. (2018). The impact of the uses and gratifications of tourist attraction fan page. *Internet Research, 28*(3), 587-603.

Ho, K. K., See-To, E. W., & Chiu, G. T. (2013). How does a social network site fan page influence purchase intention of online shoppers: A qualitative analysis. *International Journal of Social and Organizational Dynamics in IT (IJSODIT), 3*(4), 19-42.

Honari, S., Molchanov, P., Tyree, S., Vincent, P., Pal, C., & Kautz, J. (2018). *Improving landmark localization with semi-supervised learning.* Paper presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.

Hoyle, R. H. (1995). *Structural equation modeling: Concepts, issues, and applications*: Sage.

Huang, Z., Zeng, D., & Chen, H. (2007). A comparison of collaborative-filtering recommendation algorithms for e-commerce. *IEEE Intelligent Systems, 22*(5).

Hwang, R.-J., Shiau, S.-H., & Jan, D.-F. (2007). A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications, 6*(2), 184-191.

Isinkaye, F., Folajimi, Y., & Ojokoh, B. (2015). Recommendation systems: Principles, methods and evaluation. *Egyptian Informatics Journal, 16*(3), 261-273.

Jafarkarimi, H., Sim, A. T. H., & Saadatdoost, R. (2012). A naive recommendation model for large databases. *International Journal of Information and Education Technology, 2*(3), 216.

Jiang, S., Fang, S.-C., An, Q., & Lavery, J. E. (2019). A sub-one quasi-norm-based similarity measure for collaborative filtering in recommender systems. *Information Sciences, 487*, 142-155.

Johnson, M. P., Zhao, L., & Chakraborty, S. (2018). Achieving Pareto-Optimal MI-Based Privacy-Utility Tradeoffs Under Full Data. *IEEE Journal of Selected Topics in Signal Processing, 12*(5), 1093-1105.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Jung, M. H., Nelson, L. D., Gneezy, A., & Gneezy, U. (2014). Paying more when paying for others. *Journal of personality and social psychology, 107*(3), 414.

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*(1), 121-159.

Katarya, R., & Verma, O. P. (2017). An effective collaborative movie recommender system with cuckoo search. *Egyptian Informatics Journal, 18*(2), 105-112.

Keller, J. M., Gray, M. R., & Givens, J. A. (1985). A fuzzy k-nearest neighbor algorithm. *IEEE transactions on systems, man, and cybernetics*(4), 580-585.

Ketkar, N. (2017). Introduction to pytorch *Deep learning with python* (pp. 195-208): Springer.

Khosrow-Pour, M. (2008). *Encyclopedia of information science and technology* (Vol. 1): IGI Global.

Kim, C., Tao, W., Shin, N., & Kim, K.-S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications, 9*(1), 84-95.

Kim, D., Park, C., Oh, J., & Yu, H. (2017). Deep hybrid recommender systems via exploiting document context and statistics of items. *Information Sciences, 417*, 72-87.

Kim, H. M., Ghiasi, B., Spear, M., Laskowski, M., & Li, J. (2017). Online serendipity: The case for curated recommender systems. *Business Horizons, 60*(5), 613-620.

Kim, J. B. (2012). An empirical study on consumer first purchase intention in online shopping: integrating initial trust and TAM. *Electronic Commerce Research, 12*(2), 125-150.

Kim, K., & Kim, J. (2011). Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust. *Journal of Interactive Marketing, 25*(3), 145-158.

Kim, S., & Park, H. (2013). Effects of various characteristics of social commerce (s-commerce) on consumers' trust and trust performance. *International Journal of Information Management, 33*(2), 318-332.

Kittur, A., Chi, E. H., & Suh, B. (2008). *Crowdsourcing user studies with Mechanical Turk.* Paper presented at the Proceedings of the SIGCHI conference on human factors in computing systems.

Kline, R. B. (2015). *Principles and practice of structural equation modeling*: Guilford publications.

Kohnfelder, L. M. (1978). *Towards a practical public-key cryptosystem.* Massachusetts Institute of Technology.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Koren, Y. (2008). *Factorization meets the neighborhood: a multifaceted collaborative filtering model.* Paper presented at the Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining.

Koren, Y. (2009). The bellkor solution to the netflix grand prize. *Netflix prize documentation, 81*(2009), 1-10.

Koren, Y., & Bell, R. (2015). Advances in collaborative filtering *Recommender systems handbook* (pp. 77-118): Springer.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1-10.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038.

Kuan, H.-H., Bock, G.-W., & Vathanophas, V. (2008). Comparing the effects of website quality on customer initial purchase and continued purchase at e-commerce websites. *Behaviour & Information Technology, 27*(1), 3-16.

Ładyżyński, P., & Grzegorzewski, P. (2015). Vague preferences in recommender systems. *Expert Systems With Applications, 42*(24), 9402-9411.

Lee, Y.-H., Hu, P. J.-H., Cheng, T.-H., & Hsieh, Y.-F. (2012). A cost-sensitive technique for positive-example learning supporting content-based product recommendations in B-to-C e-commerce. *Decision Support Systems, 53*(1), 245-256.

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids–A comprehensive survey. *Computer Standards & Interfaces, 56*, 62-73.

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly, 33*(2), 250-257.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. *Crime, Law and Social Change, 67*(1), 3-20.

Lewis, J. A. (2005). Aux armes, citoyens: Cyber security and regulation in the United States. *Telecommunications Policy, 29*(11), 821-830.

Li, H., Jiang, J., & Wu, M. (2014). The effects of trust assurances on consumers' initial online trust: A two-stage decision-making process perspective. *International Journal of Information Management, 34*(3), 395-405.
Li, N., Li, T., & Venkatasubramanian, S. (2007). *t-closeness: Privacy beyond k-anonymity and l-diversity.* Paper presented at the Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on.
Li, P., Wang, Z., Ren, Z., Bing, L., & Lam, W. (2017). *Neural rating regression with abstractive tips generation for recommendation.* Paper presented at the Proceedings of the 40th International ACM SIGIR conference on Research and Development in Information Retrieval.
Li, T., & Li, N. (2009). *On the tradeoff between privacy and utility in data publishing.* Paper presented at the Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining.
Li, Y. (2014). A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications, 13*(1), 32-44.
Li, Y., Liu, T., Jiang, J., & Zhang, L. (2016). *Hashtag recommendation with topical attention-based LSTM*.
Li, Z., & Liao, Q. (2017). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*.
Liang, W.-Y., Huang, C.-C., Tseng, T.-L. B., Lin, Y.-C., & Tseng, J. (2012). The evaluation of intelligent agent performance—An example of B2C e-commerce negotiation. *Computer Standards & Interfaces, 34*(5), 439-446.
Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications, 10*(6), 702-715.
Liao, T.-H. (2017). Online shopping post-payment dissonance: Dissonance reduction strategy using online consumer social experiences. *International Journal of Information Management, 37*(6), 520-538.
Liao, Z., & Cheung, M. T. (2001). Internet-based e-shopping and consumer attitudes: an empirical study. *Information & Management, 38*(5), 299-306.
Lim, A. S. (2008). Inter-consortia battles in mobile payments standardisation. *Electronic Commerce Research and Applications, 7*(2), 202-213.
Limbu, Y. B., Wolf, M., & Lunsford, D. (2012). Perceived ethics of online retailers and consumer behavioral intentions: The mediating roles of trust and attitude. *Journal of Research in Interactive Marketing, 6*(2), 133-154.
Liu, C.-W., Hsieh, A.-Y., Lo, S.-K., & Hwang, Y. (2017). What consumers see when time is running out: Consumers' browsing behaviors on online shopping websites when under time pressure. *Computers in Human Behavior, 70*, 391-397.
Liu, Z., Qu, W., Li, H., & Xie, C. (2010). A hybrid collaborative filtering recommendation mechanism for P2P networks. *Future generation computer systems, 26*(8), 1409-1417.
LLC, S. S. E. T. (2002). SET Secure Electronic Transaction Specification. *Book 1: Business Description. Version, 1*.
López-Nores, M., Pazos-Arias, J. J., García-Duque, J., Blanco-Fernández, Y., Martín-Vicente, M. I., Fernández-Vilas, A.*, et al.* (2010). MiSPOT: dynamic product

placement for digital TV through MPEG-4 processing and semantic reasoning. *Knowledge and Information Systems, 22*(1), 101-128.
Lops, P., De Gemmis, M., & Semeraro, G. (2011). Content-based recommender systems: State of the art and trends *Recommender systems handbook* (pp. 73-105): Springer.
Lu, S., & Smolka, S. A. (1999). *Model checking the secure electronic transaction (SET) protocol.* Paper presented at the Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1999. Proceedings. 7th International Symposium on.
Lu, Y., Yang, S., Chau, P. Y., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. *Information & Management, 48*(8), 393-403.
Lucas, J. P., Luz, N., Moreno, M. N., Anacleto, R., Figueiredo, A. A., & Martins, C. (2013). A hybrid recommendation approach for a tourism system. *Expert Systems with Applications, 40*(9), 3532-3550.
Luo, J. N., Yang, M. H., & Huang, S.-Y. (2016). An Unlinkable Anonymous Payment Scheme based on near field communication. *Computers & Electrical Engineering, 49*, 198-206.
Machanavajjhala, A., Gehrke, J., & Kifer, D. (2006). *ℓ-density: Privacy beyond k-anonymity.* Paper presented at the Proc. of the International Conference on Data Engineering (ICDE'06), Atlanta, Georgia.
Mahadevan, L., & Kaleta, J. P. (2017). Consumer Perceptions about E-Commerce-The Influence of Public Internet Trust.
Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266.
Martín-Vicente, M. I., Gil-Solla, A., Ramos-Cabrer, M., Pazos-Arias, J. J., Blanco-Fernández, Y., & López-Nores, M. (2014). A semantic approach to improve neighborhood formation in collaborative recommender systems. *Expert Systems with Applications, 41*(17), 7776-7788.
Martin, J., Mortimer, G., & Andrews, L. (2015). Re-examining online customer experience to include purchase frequency and perceived risk. *Journal of retailing and consumer services, 25*, 81-95.
Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research, 82*, 103-116.
Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36-58.
Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, 45*(2), 135-155.
Martínez, V., Berzal, F., & Cubero, J.-C. (2017). A survey of link prediction in complex networks. *ACM Computing Surveys (CSUR), 49*(4), 69.
Mazumdar, A., & Giri, D. (2012). On-line electronic payment system using signcryption. *Procedia Technology, 6*, 930-938.
McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions, 5*, 1.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., *et al.* (2013). *A fistful of bitcoins: characterizing payments among men with no names.* Paper presented at the Proceedings of the 2013 conference on Internet measurement conference.

Meuter, M. L., Ostrom, A. L., Roundtree, R. I., & Bitner, M. J. (2000). Self-service technologies: understanding customer satisfaction with technology-based service encounters. *Journal of marketing, 64*(3), 50-64.

Micu, A.-E. (2016). Modeling a fuzzy system for assisting the customer targeting decisions in retail companies. *Analele Universitatii" Ovidius" Constanta-Seria Matematica, 24*(3), 259-273.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). *Zerocoin: Anonymous distributed e-cash from bitcoin.* Paper presented at the Security and Privacy (SP), 2013 IEEE Symposium on.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449-473.

Mitchison, N., Wilikens, M., Breitenbach, L., Urry, R., & Portesi, S. (2004). *Identity theft: a discussion paper*: European Commission, Directorate-General, Joint Research Centre.

Mohseni, S., Jayashree, S., Rezaei, S., Kasim, A., & Okumus, F. (2018). Attracting tourists to travel companies' websites: the structural relationship between website brand, personal value, shopping experience, perceived risk and purchase intention. *Current Issues in Tourism, 21*(6), 616-645.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3-4), 103-117.

Moreno, A., & Redondo, T. (2016). Text analytics: the convergence of big data and artificial intelligence. *IJIMAI, 3*(6), 57-64.

Morosan, C. (2014). Toward an integrated model of adoption of mobile phones for purchasing ancillary services in air travel. *International journal of contemporary hospitality management, 26*(2), 246-271.

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management, 47*, 120-130.

Morse, E. A. (2018). From Rai stones to Blockchains: The transformation of payments. *Computer Law & Security Review, 34*(4), 946-953.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2011). Disclosure antecedents in an online service context: the role of sensitivity of information. *Journal of Service Research*, 1094670511424924.

Mou, J., Shin, D.-H., & Cohen, J. (2017). Understanding trust and perceived usefulness in the consumer acceptance of an e-service: A longitudinal investigation. *Behaviour & Information Technology, 36*(2), 125-139.

Mu, N., Rui, L., Guo, S., & Qiu, X. (2014). *Generalized Lagrange based Resource Negotiation Mechanism in MANETs.* Paper presented at the 10th International Conference on Network and Service Management (CNSM) and Workshop.

Mukherjee, B., Neupane, R. L., & Calyam, P. (2017). *End-to-End IoT Security Middleware for Cloud-Fog Communication.* Paper presented at the Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference on.

Mulligan, D., & Bamberger, K. (2007). Security breach notification laws: Views from chief security officers. Samuelson Law, Technology & Public Policy Clinic. *Univ. of California, Berkeley School of Law. http://www. law. berkeley. edu/clinics/samuelson/cso study. pdf (last access: 7 Dec 2007)*.

Nadeem, W., Andreini, D., Salo, J., & Laukkanen, T. (2015). Engaging consumers online through websites and social media: A gender study of Italian Generation Y clothing consumers. *International Journal of Information Management, 35*(4), 432-442.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted, 1*(2012), 28.

Narayanan, A., & Shmatikov, V. (2008). *Robust de-anonymization of large sparse datasets.* Paper presented at the Security and Privacy, 2008. SP 2008. IEEE Symposium on.

Nepomuceno, M. V., Laroche, M., & Richard, M.-O. (2014). How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. *Journal of Retailing and Consumer Services, 21*(4), 619-629. doi: http://dx.doi.org/10.1016/j.jretconser.2013.11.006

Netzer, L., Gutentag, T., Kim, M. Y., Solak, N., & Tamir, M. (2018). Evaluations of emotions: Distinguishing between affective, behavioral and cognitive components. *Personality and Individual Differences, 135*, 13-24.

Núñez-Valdez, E. R., Quintana, D., Crespo, R. G., Isasi, P., & Herrera-Viedma, E. (2018). A recommender system based on implicit feedback for selective dissemination of ebooks. *Information Sciences, 467*, 87-98.

Omariba, Z. B., Masese, N. B., & Wanyembi, G. (2012). Security and privacy of electronic banking. *International Journal of Computer Science Issues, 9*(4), 432-446.

Oppliger, R., Hauser, R., & Basin, D. (2008). SSL/TLS session-aware user authentication revisited. *Computers & Security, 27*(3-4), 64-70.

Othman, A. M., Omachonu, V., & Abualsauod, E. H. (2017). The Effect of Online Service Retailers' Quality Gaps on Customer Satisfaction. *International Journal of Systems and Service-Oriented Engineering (IJSSOE), 7*(1), 21-44.

Papagelis, M., Plexousakis, D., & Kutsuras, T. (2005). Alleviating the sparsity problem of collaborative filtering using trust inferences *Trust management* (pp. 224-239): Springer.

Pappas, I. O., Kourouthanassis, P. E., Giannakos, M. N., & Lekakos, G. (2017). The interplay of online shopping motivations and experiential factors on personalized e-commerce: A complexity theory approach. *Telematics and Informatics, 34*(5), 730-742.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1988). Servqual: A multiple-item scale for measuring consumer perc. *Journal of retailing, 64*(1), 12.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security, 42*, 165-176.

Parvinen, P., Oinas-Kukkonen, H., & Kaptein, M. (2015). E-selling: A new avenue of research for service design and online engagement. *Electronic Commerce Research and Applications, 14*(4), 214-221.

Pascual-Miguel, F. J., Agudo-Peregrina, Á. F., & Chaparro-Peláez, J. (2015). Influences of gender and product type on online purchasing. *Journal of Business Research, 68*(7), 1550-1556.

Pavlou, P. (2001). Integrating trust in electronic commerce with the technology acceptance model: model development and validation. *Amcis 2001 proceedings*, 159.

Pazzani, M. J., & Billsus, D. (2007). Content-based recommendation systems *The adaptive web* (pp. 325-341): Springer.

Pee, L. G., Woon, I. M., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information & Management, 45*(2), 120-130.

Pereira, J. A., Matuszyk, P., Krieter, S., Spiliopoulou, M., & Saake, G. (2018). Personalized recommender systems for product-line configuration processes. *Computer Languages, Systems & Structures*.

Phelan, O., McCarthy, K., & Smyth, B. (2009). *Using twitter to recommend real-time topical news.* Paper presented at the Proceedings of the third ACM conference on Recommender systems.

Plouffe, C. R., Vandenbosch, M., & Hulland, J. (2001). Intermediating technologies and multi-group adoption: a comparison of consumer and merchant adoption intentions toward a new electronic payment system. *Journal of Product Innovation Management: AN INTERNATIONAL PUBLICATION OF THE PRODUCT DEVELOPMENT & MANAGEMENT ASSOCIATION, 18*(2), 65-81.

Ponnapureddy, S., Priskin, J., Ohnmacht, T., Vinzenz, F., & Wirth, W. (2017). The influence of trust perceptions on German tourists' intention to book a sustainable hotel: A new approach to analysing marketing information. *Journal of Sustainable Tourism, 25*(7), 970-988.

Ponte, E. B., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management, 47*, 286-302.

Preibusch, S., Peetz, T., Acar, G., & Berendt, B. (2015). *Purchase details leaked to PayPal.* Paper presented at the International Conference on Financial Cryptography and Data Security.

Qu, Y., Cai, H., Ren, K., Zhang, W., Yu, Y., Wen, Y.*, et al.* (2016). *Product-based neural networks for user response prediction.* Paper presented at the 2016 IEEE 16th International Conference on Data Mining (ICDM).

Quadrana, M., Karatzoglou, A., Hidasi, B., & Cremonesi, P. (2017). *Personalizing session-based recommendations with hierarchical recurrent neural networks.* Paper presented at the Proceedings of the Eleventh ACM Conference on Recommender Systems.

Raisaro, J. L., Choi, G., Pradervand, S., Colsenet, R., Jacquemont, N., Rosat, N.*, et al.* (2018). Protecting privacy and security of genomic data in I2B2 with homomorphic

encryption and differential privacy. *IEEE/ACM transactions on computational biology and bioinformatics, 15*(5), 1413-1426.
Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology, 60*(10), 1119-1139.
Ricci, F., Rokach, L., & Shapira, B. (2015). Recommender systems: introduction and challenges *Recommender systems handbook* (pp. 1-34): Springer.
Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273.
Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120-126.
Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. *Procedia Computer Science, 121*, 568-575.
Rose, S., Clark, M., Samouel, P., & Hair, N. (2012). Online customer experience in e-retailing: an empirical model of antecedents and outcomes. *Journal of Retailing, 88*(2), 308-322.
Ross, J. (2017). Cybersecurity: A Real Threat to Patient Safety. *Journal of PeriAnesthesia Nursing, 32*(4), 370-372.
Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. *Electronic Commerce Research and Applications, 19*, 33-43.
Roy, S., & Venkateswaran, P. (2014). *Online payment system using steganography and visual cryptography.* Paper presented at the Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on.
Roy, S. K., Balaji, M., Sadeque, S., Nguyen, B., & Melewar, T. (2017). Constituents and consequences of smart customer experience in retailing. *Technological Forecasting and Social Change, 124*, 257-270.
Ruiz-Mafe, C., Martí-Parreño, J., & Sanz-Blas, S. (2014). Key drivers of consumer loyalty to Facebook fan pages. *Online Information Review, 38*(3), 362-380.
Ruiz-Martínez, A., Reverte, Ó. C., & Gómez-Skarmeta, A. F. (2012). Payment frameworks for the purchase of electronic products and services. *Computer Standards & Interfaces, 34*(1), 80-92.
Runnemark, E., Hedman, J., & Xiao, X. (2015). Do consumers pay more using debit cards than cash? *Electronic Commerce Research and Applications*.
Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S.*, et al.* (2015). Imagenet large scale visual recognition challenge. *International journal of computer vision, 115*(3), 211-252.
Sachdeva, N., Gupta, K., & Pudi, V. (2018). *Attentive neural architecture incorporating song features for music recommendation.* Paper presented at the Proceedings of the 12th ACM Conference on Recommender Systems.

Sahnoune, Z., Aïmeur, E., El Haddad, G., & Sokoudjou, R. (2015). *Watch your mobile payment: An empirical study of privacy disclosure.* Paper presented at the 2015 IEEE Trustcom/BigDataSE/ISPA.

Sakurai, K., & Yamane, Y. (1996). *Blind decoding, blind undeniable signatures, and their applications to privacy protection.* Paper presented at the Information Hiding.

Schafer, J. B., Frankowski, D., Herlocker, J., & Sen, S. (2007). Collaborative filtering recommender systems *The adaptive web* (pp. 291-324): Springer.

Scholz, M., Dorner, V., Schryen, G., & Benlian, A. (2017). A configuration-based recommender system for supporting e-commerce decisions. *European Journal of Operational Research, 259*(1), 205-215.

Seckler, M., Heinz, S., Forde, S., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior, 45*, 39-50.

See-To, E. W., & Ho, K. K. (2016). A study on the impact of design attributes on E-payment service utility. *Information & Management, 53*(5), 668-681.

See-To, E. W., & Ngai, E. W. (2018). An empirical study of payment technologies, the psychology of consumption, and spending behavior in a retailing context. *Information & Management*.

Shafritz, J. M., Ott, J. S., & Jang, Y. S. (2015). *Classics of organization theory*: Cengage Learning.

Shaji, S. (2014). Anti Phishing approach using Visual Cryptography and Iris Recognition. *IJRCCT, 3*(3), 088-092.

Shani, G., & Gunawardana, A. (2011). Evaluating recommendation systems *Recommender systems handbook* (pp. 257-297): Springer.

Shankar, V., Smith, A. K., & Rangaswamy, A. (2003). Customer satisfaction and loyalty in online and offline environments. *International journal of research in marketing, 20*(2), 153-175.

Shen, C.-C., & Chiou, J.-S. (2010). The impact of perceived ease of use on Internet service adoption: The moderating effects of temporal distance and perceived risk. *Computers in Human Behavior, 26*(1), 42-50.

Shi, L., Carbunar, B., & Sion, R. (2007). Conditional e-cash *Financial Cryptography and Data Security* (pp. 15-28): Springer.

Shi, Y., Larson, M., & Hanjalic, A. (2014). Collaborative filtering beyond the user-item matrix: A survey of the state of the art and future challenges. *ACM Computing Surveys (CSUR), 47*(1), 3.

Shin, J. I., Chung, K. H., Oh, J. S., & Lee, C. W. (2013). The effect of site quality on repurchase intention in Internet shopping through mediating variables: The case of university students in South Korea. *International Journal of Information Management, 33*(3), 453-463.

Shneiderman, B., & Zhao, H. (2016). "In Web We Trust": Establishing Strategic Trust Among Online Customers Irina Ceaparu, Dina Demner, Edward Hung *E-Service: New Directions in Theory and Practice* (pp. 102-119): Routledge.

Shu, W., & Cheng, C. Y. (2012). How to improve consumer attitudes toward using credit cards online: An experimental study. *Electronic Commerce Research and Applications, 11*(4), 335-345.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks, 76*, 146-164.

Sivaramakrishnan, S., Wan, F., & Tang, Z. (2007). Giving an "e-human touch" to e-tailing: The moderating roles of static information quantity and consumption motive in the effectiveness of an anthropomorphic information agent. *Journal of Interactive Marketing, 21*(1), 60-75. doi: https://doi.org/10.1002/dir.20075

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust. *Psychology & Marketing, 32*(8), 860-873.

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2017). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225.

Staykova, K. S., & Damsgaard, J. (2015). The race to dominate the mobile payments platform: Entry and expansion strategies. *Electronic Commerce Research and Applications*.

Stein, A., & Ramaseshan, B. (2016). Towards the identification of customer experience touch point elements. *Journal of Retailing and Consumer Services, 30*, 8-19.

Su, X., & Khoshgoftaar, T. M. (2009). A survey of collaborative filtering techniques. *Advances in artificial intelligence, 2009*.

Sureshkumar, V., Anitha, R., Rajamanickam, N., & Amin, R. (2016). A lightweight two-gateway based payment protocol ensuring accountability and unlinkable anonymity with dynamic identity. *Computers & Electrical Engineering*.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(05), 557-570.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203-223.

Ten, C.-W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems, 23*(4), 1836-1846.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.

Thomas, M., Desai, K. K., & Seenivasan, S. (2011). How credit card payments increase unhealthy food purchases: visceral regulation of vices. *Journal of Consumer Research, 38*(1), 126-139.

Thompson, F. M., Tuzovic, S., & Braun, C. J. B. H. (2019). Trustmarks: Strategies for exploiting their full potential in e-commerce. *62*(2), 237-247.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., Cotten, S. R. J. C., *et al.* (2016). Understanding online safety behaviors: A protection motivation theory perspective. *59*, 138-150.

Turner, S. (2014). Transport Layer Security. *IEEE Internet Computing, 18*(6).

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559.

Vincent, O. R., Makinde, A. S., & Akinwale, A. T. (2017). A cognitive buying decision-making process in B2B e-commerce using Analytic-MLP. *Electronic Commerce Research and Applications, 25*, 59-69.

Vos, A., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). Risk Reduction Strategies in Online Shopping: E-trust Perspective. *Procedia-Social and Behavioral Sciences, 147*, 418-423.

Wang, D., Liang, Y., Xu, D., Feng, X., & Guan, R. (2018). A content-based recommender system for computer science publications. *Knowledge-Based Systems, 157*, 1-9.

Wang, H., Wang, N., & Yeung, D.-Y. (2015). *Collaborative deep learning for recommender systems.* Paper presented at the Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining.

Wang, J.-h., Liu, J.-w., Li, X.-h., & Kou, W.-d. (2009). Fair e-payment protocol based on blind signature. *The Journal of China Universities of Posts and Telecommunications, 16*(5), 114-118. doi: http://dx.doi.org/10.1016/S1005-8885(08)60277-0

Wang, J., & Wang, X. (2019). *Structural equation modeling: Applications using Mplus*: John Wiley & Sons.

Wang, S., Lo, D., Vasilescu, B., & Serebrenik, A. (2018). EnTagRec++: An enhanced tag recommendation system for software information sites. *Empirical Software Engineering, 23*(2), 800-832.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management, 36*(4), 531-542.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review, 20*(1), 35-44.

Williams, M. D. (2018). Social Commerce and the Mobile Platform: Payment and Security Perceptions of Potential Users. *Computers in Human Behavior*.

Woo, K., & Liu, D. Y.-K. (2019). Integrating third party shopping cart applications with an online payment service: Google Patents.

Wu, L., Chen, B., Zeadally, S., & He, D. (2018). An efficient and secure searchable public key encryption scheme with privacy protection for cloud storage. *Soft Computing*, 1-12.

Xiang, Z., El-Haddad, G., & Aïmeur, E. (2019). *Privacy vs. Utility: An Enhanced K-coRated.* Paper presented at the International Conference on Computational Science and Its Applications.

Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: a theoretical perspective. *Mis Quarterly, 35*(1), 169-196.

Xiao, B., Monath, N., Ananthakrishnan, S., & Ravi, A. (2018). Play Duration based User-Entity Affinity Modeling in Spoken Dialog System. *arXiv preprint arXiv:1806.11479*.

Xing, S., Wang, Q., Zhao, X., & Li, T. (2019). A hierarchical attention model for rating prediction by leveraging user and product reviews. *Neurocomputing, 332*, 417-427.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52.

Xu, N., Bai, S.-z., & Wan, X. (2017). Adding pay-on-delivery to pay-to-order: The value of two payment schemes to online sellers. *Electronic Commerce Research and Applications, 21*, 27-37.

Yang, Q., Pang, C., Liu, L., Yen, D. C., & Tarn, J. M. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *Computers in Human Behavior, 50*, 9-24.

Yao, M., Di, H., Zheng, X., & Xu, X. (2018). Impact of payment technology innovations on the traditional financial industry: A focus on China. *Technological Forecasting and Social Change*.

Ye, Y., Wang, L., Han, J., Qiu, S., & Luo, F. (2017). *An anonymization method combining anatomy and permutation for protecting privacy in microdata with multiple sensitive attributes.* Paper presented at the Machine Learning and Cybernetics (ICMLC), 2017 International Conference on.

Ying, H., Chen, L., Xiong, Y., & Wu, J. (2016). *Collaborative deep ranking: A hybrid pair-wise recommendation algorithm with implicit feedback.* Paper presented at the Pacific-asia conference on knowledge discovery and data mining.

Zhang, F., Lee, V. E., & Jin, R. (2014). *k-CoRating: filling up data to obtain privacy and utility.* Paper presented at the Twenty-Eighth AAAI Conference on Artificial Intelligence.

Zhang, F., Lee, V. E., Jin, R., Garg, S., Choo, K.-K. R., Maasberg, M.*, et al.* (2018). Privacy-aware smart city: A case study in collaborative filtering recommender systems. *Journal of Parallel and Distributed Computing*.

Zhang, F., Lee, V. E., Jin, R., Garg, S., Choo, K.-K. R., Maasberg, M.*, et al.* (2019). Privacy-aware smart city: A case study in collaborative filtering recommender systems. *127*, 145-159.

Zhang, F., Liu, Q., & Zeng, A. (2017). Timeliness in recommender systems. *Expert Systems with Applications, 85*, 270-278.

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy*.

Zhang, K. Z., Zhao, S. J., Cheung, C. M., & Lee, M. K. (2014). Examining the influence of online reviews on consumers' decision-making: A heuristic–systematic model. *Decision Support Systems, 67*, 78-89.

Zhang, Q., Liu, H., Wu, Y., Lin, C., & Lin, G. (2017). *Grey maximum distance to average vector based on quasi identifier attribute.* Paper presented at the Grey Systems and Intelligent Services (GSIS), 2017 International Conference on.

Zhang, S., Yao, L., & Sun, A. (2017). Deep learning based recommender system: A survey and new perspectives. *arXiv preprint arXiv:1707.07435*.

Zhang, X., Zhao, J., & Lui, J. (2017). *Modeling the assimilation-contrast effects in online product rating systems: Debiasing and recommendations.* Paper presented at the Proceedings of the Eleventh ACM Conference on Recommender Systems.

Zhang, Y., Dai, H., Xu, C., Feng, J., Wang, T., Bian, J.*, et al.* (2014). *Sequential Click Prediction for Sponsored Search with Recurrent Neural Networks.* Paper presented at the AAAI.

Zhang, Y., Deng, R. H., Liu, X., & Zheng, D. (2018). Blockchain based Efficient and Robust Fair Payment for Outsourcing Services in Cloud Computing. *Information Sciences*.

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly, 27*(1), 49-56.

Zhao, X., Xia, L., Zhang, L., Ding, Z., Yin, D., & Tang, J. (2018). Deep Reinforcement Learning for Page-wise Recommendations. *arXiv preprint arXiv:1805.02343*.

Zheng, L., Noroozi, V., & Yu, P. S. (2017). *Joint deep modeling of users and items using reviews for recommendation.* Paper presented at the Proceedings of the Tenth ACM International Conference on Web Search and Data Mining.

Zittrain, J. (2008). *The future of the internet--and how to stop it*: Yale University Press.