République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia

جامعة بجاية
Tasdawit n'Bgayet
Université de Béjaïa

Faculté des Sciences Exactes
Département d'Informatique

En vue de l'obtention du diplôme de Master Recherche en Informatique

Option **: Réseaux & Systèmes Distribués**

Mémoire de Fin de Cycle

Thème

APPROCHE HYBRIDE POUR LA CONFIANCE DANS LE COMMERCE ÉLECTRONIQUE

Réalisé par

*M^lle^* DJERROUD Souâd
*M^r^* TITOUAH Abdeslem

Soutenu devant le jury

Président	:	*M^lle^ KHOULALENE Nadjet*	Université de Béjaia
Examinateur	:	*M^r^ KHANOUCHE M^ed^ Essaid*	Université de Béjaia
Rapporteur	:	*M^r^ MIR Foudil*	Université de Béjaia

Septembre 2011

Dédicaces

À la mémoire de mon cousin TARIK et de mon oncle SADDEK,
À mes parents,
À mes frères et sœurs,
À mes nièces : Kahina,Inass, Malak,
À toute ma famille,
À ma binôme Souâd et sa famille,
À mes ami(e)s et camarades : par peur d'oublie,aucun ne sera cité,
Et à toutes les personnes que j'ai connue et qui m'ont aidé.

Mr Abdeslem TITOUAH

À la mémoire de ma regretté grand-mère,
À mon père, qui m'a tant encouragé, poussé en avant et orienté,
À ma mère, qui n'a cessé de me soutenir et d'avoir confiance en moi,
À mes frères et sœurs qui ont toujours été là pour me supporter,
À mes belles sœurs et beaux frères,
À mes chèrs petits Poussins, qui illuminent quotidiennement notre vie :
fifi, doudou, sisouh, badi, yani, mili, midou, mimou, badis, mimine, zira
À tous les membres de ma famille,
À mon binôme Afnani et sa famille,
À mes ami(e)s qui m'ont toujours répondu présents : Amel, yacine, Bary,
la miss, farid, lily, Fayçal,...
Et à tous ceux que je connais et j'estime.

Souâd DJERROUD

Remerciements

Ce travail n'aurait pas pu aboutir à des résultats satisfaisants sans l'aide et les encouragements de plusieurs personnes que nous remercions.

Nos vifs remerciements accompagnés de toute notre gratitude vont à notre promoteur **M^{r} Foudil MIR**, enseignant à l'université de Béjaia, pour nous avoir proposé ce sujet intéressant, pour nous avoir fait autant confiance, pour ses critiques, conseils et orientations, sans compter le temps qu'il nous a consacré pour corriger et guider notre travail et pour sa disponibilité dans les moments de faille et d'incertitude.

Nous remercions également les membres du Jury à savoir, **M^{lle} KHOULALENE Nadjet** pour avoir accepté de présider le Jury, ainsi que **M^{r} KHANOUCHE M^{ed} Essaid** pour avoir accepté de juger notre travail.

nos vifs remerciements vont aussi à nos ami(e)s qui nous on aidé :Hamza, Hmimi, Fares, Brahim, Yacine et Meriem.

Nous ne pourrons oublier d'adresser notre reconnaissance, nos remerciements et notre plus profonde gratitude à nos familles (DJERROUD & TITOUAH) en particulier nos parents, qui, sans eux, nous ne serons pas arrivés là où nous sommes aujourd'hui.

Enfin, pour éviter le risque d'oublier quelqu'un, nous remercions toutes les personnes que nous avons côtoyées et qui nous ont aidés, de près ou de loin.

Souâd & Abdeslem

Résumé

Le e-Commerce désigne l'échange de biens et de services entre deux entités sur les réseaux informatiques, notamment Internet. Par la pluralité de choix des produits, le gain de temps, la comparaison des prix, le e-Commerce est favorisé. Cependant, payer en ligne n'est pas une solution sollicitée. La variété des modes de paiement ne rassure pas les clients soucieux de préserver leurs données privées.

Par l'utilisation néfaste et maligne, plusieurs attaques peuvent être exécutées au détriment d'un site e-Commerce, ces attaques sont destinées à compromettre la disponibilité, l'intégrité, et la confidentialité des informations. Pour remédier à ces attaques différentes techniques de sécurité ont été mises en place. Malgré les efforts de sécurisation les clients restent méfiants.

Le manque de confiance exprimé par les utilisateurs, constitue l'obstacle majeur qui freine la constante croissance du e-Commerce. Puisque la confiance est considérée comme un élément fondateur de tout échange, un facteur essentiel pour la stabilité et la continuité dans le temps, des relations entre les parties. Alors, comment susciter cette confiance ?

Par hybridation des travaux de Meziane et Kasiran avec la norme universelle Web-Trust, nous avons proposé un modéle qui permet de répondre aux soucis des clients. Ceci par le fait qu'il offre les informations jugées importantes par les clients concernant un site donné en plus de la recommandation et la verification de la tierce partie.
Mots clés : Confiance, E-Commerce, E-paiement, Sécurite.

Abstract

E-Commerce refers to the exchange of goods and services between two entities on computer networks, including Internet. By the plurality of choice of the products, time savings, the price comparison, e-Commerce is enhanced. However, paying online is not a sought solution. The variety of payment methods does not reassure customers anxious about preserving their privacy.

By the harmful and malignant use, several attacks can be executed on the expense of a site e-Commerce ; these attacks are intended to compromise the availability, the integrity, and the confidentiality of information. To address these attacks different security techniques have been developed. Despite efforts to secure, customers remain wary.

The lack of trust expressed by users is the major obstacle hindering the constant growth of e-Commerce. Since trust is considered a fundamental element of any exchange, a key factor for stability and continuity over time, of different relationship. Then, how to arouse this trust ?

By hybridization of works of Meziane and Kasiran with the universal standard Web-Trust, we have proposed a model that meets the concerns of customers. This by the fact that it offers the information considered to be significant by the customers concerning a given site. it increases the level of customers' trust by recommendation of the third party.
Keywords : Trust, E-commerce, E-payment, Security.

Table des matières

Table des figures

Liste des algorithmes

Acronymes

AICPA	:	American Institute of Certified Public Accountants
AJAX	:	Asynchronous Javascript and XML
B2B	:	Business to Business
B to C /B2C	:	Business to consumer
C2C	:	Consumer to Comsumer
CA	:	Certification authority
CB	:	Carte bancaire
CICA	:	Centre International de Communication Avancée
CPA	:	Certified Public Accountant
EDI	:	Échange de données informatisées
FAI	:	Fournisseur d'accé Internet
FEVAD	:	La féderation du e-Commerce et de la vente à distance
FTP	:	File transport protocole
G2B	:	Governement to Business
G2C	:	Government to Citizen
GSM	:	Global System for Mobile
HSM	:	Hardware Specific Module
HTTP	:	HyperText Transfer Protocol
ICP	:	Infrastructure à clés publique
IGC	:	Infrastructure de gestion de clés
IMAP	:	Internet Message Access Protocol
MD5	:	Message Digest 5

MCI	:	Master Card Internationale
PHP	:	Hypertext Preprocessor
PKI	:	Public key infrastructure
PME	:	Petite et moyenne entreprise
POP	:	Post Office Protocol
SET	:	Secure Electronic Transaction
SMS	:	Short message service
SMTP	:	Simple Mail Transfer Protocol
SQL	:	Structured Query Language
SSL	:	Secure Sockets Layers
TCP-IP	:	Transmission Control Protocol-Internet Protocol
Telnet	:	Telecommunication Network
TLS	:	Transport Layer Security
URL	:	Uniform Resource Locator
VPC	:	vente par correspondance
WIFI	:	Wireless Fidelity
XML	:	Extensible Markup Language
XUL	:	XML-based User interface Language

Introduction Générale

La révolution de l'Internet bouscule nos modes de pensée, traditions juridiques et administratives et modifie les règles de la compétition. Elle crée une situation d'incertitude, aux évolutions largement imprévisibles, mettant en cause le cadre intellectuel. Au cœur de ces transformations, le commerce électronique peut être sommairement défini comme l'ensemble des échanges numérisés, liés à des activités commerciales, l'irruption de l'Internet modifie considérablement la perspective, puisque son coût réduit et sa relative simplicité d'utilisation en favorisent une diffusion très rapide, notamment vers les petites entreprises et vers les consommateurs. Le développement de la vente électronique des produits et services constitue aujourd'hui le phénomène le plus médiatisé. La croissance de e-commerce est sans pareil, et les chiffres d'affaires connaissent une explosion [**1**].

Au 1er trimestre 2011, le chiffre d'affaire de l'ensemble des sites de ventes en ligne a progressé de 20% par rapport au même trimestre de l'année 2010 pour atteindre 8,8 milliards d'euros [**2**], où le secteur pesait 7,2 milliards d'euros, estime la FEVAD (Fédération du e-Commerce et de la vente à distance)[**3**].

Grâce au commerce électronique, une place du marché s'est ouverte avec des milliers d'entreprises. Par leur nom ou leur façon de traiter les affaires, tous les prestataires ne sont pas reconnus comme étant digne de confiance. Beaucoup de disciples ont argué du fait que la confiance est un préalable au commerce réussi, parce que les consommateurs sont hésitants à faire des achats à moins qu'ils fassent confiance au vendeur. La confiance du consommateur peut être bien plus importante dans les transactions électroniques, que dans les transactions traditionnelles, Selon Schlenker et al (1973), faire confiance c'est compter sur une information reçue d'une autre personne à propos d'états incertains de l'environnement et de leurs conséquences dans une situation de risque. Lors des opérations

de vente traditionnelles, se déroulant physiquement dans un local de vente, la possibilité de créer la confiance est offerte par une impression optique directe liée au local, lors de l'entretien avec les personnes concernées et par le produit directement palpable. En revanche, dans le commerce électronique, beaucoup de faits peuvent être simulés, car les protagonistes ne sont pas toujours connus et les locaux ne peuvent pas être examinés.

Cette nouvelle dynamique du marché est caractérisée par la dématérialisation des transactions et leur indépendance par rapport à la géographie et aux frontières. Cependant, le e-commerce n'a pas encore atteint son plein épanouissement, à cause du manque de confiance, invoqué lorsque les clients sont invités a introduire des données personnelles.

La nouvelle littérature sur la confiance considère généralement que, lorsque les agents économiques se font mutuellement confiance, il y a plus de transactions, plus de contrats conclus et plus de gains qui en résultent. En conséquence, la croissance économique augmenterait lorsque la confiance mutuelle s'améliore.

Ce manque de confiance nourri par la prolifération des fraudes, explique que beaucoup sont encore réfractaires ou du moins demeurent réticents à l'égard du commerce électronique. Quels sont les facteurs expliquant la confiance du consommateur lors d'un achat sur un site marchand ? Quelles sont les variables qu'impose la spécificité du contexte du commerce électronique ? Comment augmenter la confiance exprimée par les clients ? Comment garantir la véracité des informations fournies par un site ? Comment transmettre ces informations aux clients ? Telles sont les questions auxquelles nous allons essayer de répondre.

Notre mémoire va s'articuler en plusieurs étapes. Dans le premier chapitre , nous mettrons plus de lumière sur le commerce électronique, ensuite dans le deuxième chapitre nous parlerons des différents moyens de paiement, et les techniques de sécurisation, puis dans le troisième chapitre nous nous attarderons sur les concepts de la confiance et ses déterminants, en faisant un état de l'art de quelques travaux. Pour ensuite dans le quatrième chapitre proposer notre solution. Enfin nous terminons par une conclusion générale et des perspectives.

1

Commerce électronique

Introduction

Aujourd'hui, la plupart des entreprises du commerce en détails s'adaptent progressivement au commerce électronique via l'Internet. Pour les grandes entreprises de la vente à distance, le réseau informatique complète le courrier et le mobile. Il leur permet une relation plus interactive avec le client. Personnaliser cette relation est aussi une motivation pour les entreprises traditionnelles du commerce en magasin, qui misent sur l'image favorable du web auprès des consommateurs. Le commerce en ligne est également le fait de petites entreprises créées spécifiquement pour exercer cette activité. Les détaillants attendent du commerce électronique une augmentation de la clientèle et du chiffre d'affaire mais craignent une augmentation de la concurrence .

Nous allons voir dans ce chapitre un historique et des généralités sur le e-Commerce ; nous y concentrons notre étude sur le modèle « B to C(Business to consumer) »car c'est le modèle sur lequel se base notre travail. Nous allons donc voir les possibles stratégies

adoptées du « B to C », et recenser différents avantages et inconvénients pour les deux parties du modèle « B to C ».

1.1 Historique

L'évolution du e-Commerce est liée à celui de l'Internet. Depuis quelques années, le secteur de l'Internet enregistre des chiffres d'une croissance impressionnante.

Au tout début, il y'avait un manque d'autorité capables de définir des règles et des sanctions, ce qui a laissé apparaître une certaine forme d'anarchie au niveau de l'Internet et a largement freiné le développement d'activités commerciales sur ce réseau. Il y'avait également d'autres facteurs expliquant le retard de l'arrivée du e-Commerce, prenant comme exemple, la langue principale dans les débuts de l'Internet, était l'anglais, l'ergonomie et le graphisme n'étaient pas très poussés mais aussi, l'esprit des principaux acteurs d'Internet, dans les années 80 et 90 étaient orientés vers le painterentreprisesrtage gratuit et libre de l'information, là encore, peu compatible avec des activités commerciales [**4**].

L'ouverture du réseau au grand public et la généralisation des accès à Internet ont complètement contrecarré ces facteurs de ralentissement. Même si l'esprit de gratuité de l'information est toujours présent, ce changement devait se faire. Le réseau ne pouvait continuer à accueillir un nombre d'utilisateurs toujours plus nombreux sans mettre en place un modèle économique viable. les seuls abonnements versés aux fournisseurs d'accès à Internet ne suffisent plus pour financer le coût des équipements et les infrastructures de télécommunication [**4**].

Le lancement des activités commerciales sur Internet est apparu vers le milieu des années 90. 1400 milliards de dollars : c'est le montant d'argent qui se brassera au niveau mondial dans le commerce électronique en 2015. En 2011, le chiffre d'affaire du e-commerce est évaluée à 681 milliards de $ dans le monde, 80% des internautes ont déjà fait au moins un achat en ligne.

La naissance et le développement du e-Commerce sont liés à des évolutions technologiques du réseau Internet.

1.2 Généralités sur le e-Commerce

Nous allons voir quelques définitions et généralités sur le e-Commerce :

1.2.1 E-business

Le e-business recouvre les différentes applications possibles de l'informatique faisant appel aux technologies de l'information et de la communication (TIC) pour traiter de façon performante les relations de communication d'information d'une entreprise telle qu'une PME avec des organisations externes ou des particuliers. Les technologies utilisées sont principalement celles de l'Internet et du Web[**5**].

1.2.2 Définition du e-Commerce ?

Selon la définition de l'encyclopédie, On appelle « Commerce électronique (ou e-Commerce ou le e-Business) »l'utilisation d'un média électronique pour la réalisation de transactions commerciales et l'échange de biens et de services entre deux entités sur les réseaux informatiques. La plupart du temps, il s'agit de la vente de produits à travers le réseau internet, mais le terme de e-Commerce englobe aussi le commerce interentreprises où l'on utilise des réseaux de type EDI (Échange de données informatisées).

Il y'a aussi des transactions électroniques sur les réseaux téléphoniques qu'on appelle le « M-commerce »(mobile commerce) [**6**]. L'arrivée de l'Iphone a permis à de nombreux sites marchands de développer leur propre application mobile et s'offrir un nouveau canal de vente, telle que Amazon et Rue du Commerce .

1.2.3 Pourquoi e-Commerce ?

Grâce à sa flexibilité, sa large diffusion et au fait qu'une boutique en ligne est ouverte 24h/24 tous les jours de l'année, le commerce électronique devient chaque jour un outil de vente plus important aux yeux des entreprises modernes. Même les entreprises les plus traditionnelles exploitent désormais Internet afin de stimuler leurs ventes et se lancent dans l'aventure du commerce électronique.

Avec l'évolution téchnologique, les sites de ventes en ligne possèdent des systèmes de paiements de plus en plus sécurisés. Les sites e-Commerces étant de plus en plus contraints

à une plus grande transparence quant à la non-diffusion des informations personnelles de leurs clients. Les lignes hauts débit se sont démocratisées, et il est maintenant possible de recevoir un certain trafic à moindre coût. Grâce aux médias présents sur internet, les internautes sont mieux informés du risque qui peut ne pas exister lorsqu'ils effectuent des commandes de produits en ligne. Le prix est plus attractif sur Internet car les frais de fonctionnement sont moindres, (pas d'employé pour votre showroom,...). La comparaison des prix de chacun, les délais de livraison proposés sont très courts (48 heures au max). Les produits peuvent désormais être réservés avant leur date de commercialisation officielle, etc [**7**].

1.2.4 Déroulement et Processus impliqués dans le e-Commerce

Le e-Commerce, et dans une plus large mesure le e-business, implique un grand nombre de processus : navigation à la commande, gestion de la commande à l'envoi du produit, du service après-vente au traitement des avis des clients, toutes ces étapes sont cruciales pour une société de e-Commerce.

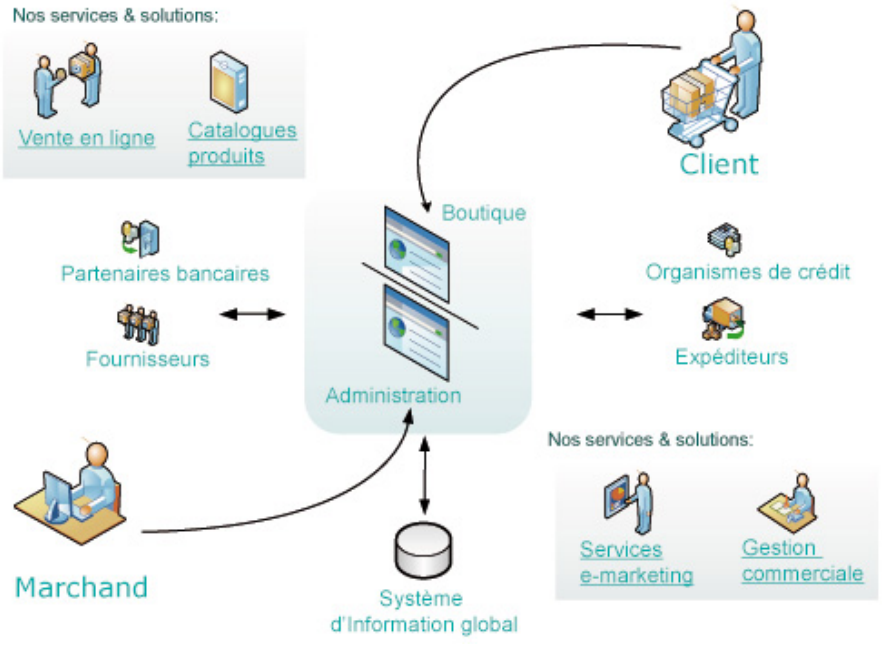

FIGURE 1.1 – *Les différents composants du e-Commerce* [**8**].

Pour qu'un client accède à un site de vente en ligne il faut d'abord qu'il le trouve : le référencement est si important qu'il est même devenu le nouveau nerf de la guerre sur internet. Une fois sur le site, le client devra à la fois trouver le site agréable et fonction-

nel : s'il ne trouve pas ce qu'il cherche en quelques cliques, le client ira ailleurs. Avec les nouvelles technologies, le client sait en permanence où en est sa commande : l'étape de la logistique est l'une des plus déterminantes de l'opinion du client... Toutes ces étapes résument parfaitement la philosophie d'une solution e-Commerce : prendre en compte tous les processus d'une commande pour pouvoir booster un chiffre d'affaires. Donc les transactions de commerce électronique se déroulent généralement comme suit : un acheteur consulte un catalogue en ligne, commande un article ou un service et fournit ses informations de carte de crédit, ainsi qu'une adresse de livraison. Le vendeur vérifie ensuite les informations du moyen de paiement, traite la commande et s'occupe de la livraison [**9**].

1.2.5 Fonctions du e-Commerce

Les principales fonctions du e-Commerce sont :

- Inscription et validation des clients et utilisateurs.
- Obtention d'un devis.
- Conseil et catalogue électronique.
- Gestion du panier, commandes et achat en ligne.
- Gestion des stocks en temps réel.
- Paiement en ligne.
- Suivi de la livraison.
- Service après vente en ligne.

1.3 Type d'échanges

Il existe différentes catégorisations du commerce électronique :

1.3.1 Le commerce B2C (Business to Consumer)

« Il s'agit de la vente au grand public par une entreprise depuis un site Internet. La variété des sites B2C est immense et de nombreux modèles d'affaires existent au sein de cette catégorie. »[**10**].

le commerce électronique B2C est sans doute l'aspect le plus viable du commerce électronique car il permet au consommateur d'acheter directement sur Internet des biens et des services pour son usage personnel. Dans ce type de commerce, l'entreprise peut utiliser

un questionnaire en ligne qui lui permettra de mieux connaitre ses clients, d'individualiser les contrats, les offres et d'accompagner les prospects de la commande jusqu'à la livraison.

1.3.2 Le commerce B2B (Business to Business)

« Il s'agit de commerce entre entreprises. Cette forme de commerce est plus ancienne que la précédente. Historiquement, elle s'appuie sur des solutions d'interconnexion de réseaux utilisant l'EDI (Echange de Données Informatisées). Les places de marché sont une variante de cette forme de commerce électronique »[**10**].

L'utilisation de l'informatique comme outil de commerce entre entreprises ne date pas de l'ère Internet. Bien avant, l'EDI avait permis de simplifier considérablement les transactions commerciales entre entreprises. L'apport d'Internet dans ce domaine concerne surtout la baisse des coûts et par conséquent la« démocratisation » du commerce électronique. En effet, la mise en place de liaisons EDI correspondait à des investissements lourds que seuls les grands groupes pouvaient se permettre. Dès lors, la baisse des prix de l'informatique et le passage par Internet, rend cette technologie accessible à l'ensemble des PME(Petite et moyenne entreprise).

1.3.3 Le commerce G2C (Government to Citizen)

« Il s'agit de toutes les solutions que développent un Etat, une administration ou une collectivité territoriale afin de faciliter les démarches administratives des usagers d'un service public. On parle également d'administration électronique ou de e-administration »[**10**].

1.3.4 Le commerce G2B (Governement to Business)

« Il s'agit des solutions électroniques mises en place par les structures publiques pour gérer les relations avec ces institutions. Ce sont des sites qui centralisent les appels d'offre publique des administrations ».

1.3.5 Le commerce C2C (Consumer to Comsumer)

Ce type de commerce existait deja avant l'ère Internet. Internet lui donna une nouvelle dimension en démultipliant les possibilités d'échange et en facilitant la recherche de bien

.

Dans notre étude nous allons nous focaliser essentiellement sur le B2C ,et de manière encore plus fine.

1.4 Avantages et inconvénients du e-Commerce

1.4.1 Avantages

Le commerce électronique offre aux vendeurs sur Internet de nombreux avantages : Les avantages sont classés selon deux parties : avantages pour la société et avantages pour les clients [**11**].

Pour l'entreprise

- Il ouvre un nouveau canal de distribution, un circuit complémentaire pour certains produits et services de l'entreprise.
- Il permet de couvrir des niches de marché dont l'atteinte serait jugée trop onéreuse par les moyens classiques de commercialisation.
- Il apporte une plus forte convivialité par rapport à la VPC (vente par correspondance) et à la commande à distance traditionnelle grâce aux multimédias qui regroupent le son, l'image, la couleur, le texte et l'animation.
- Il favorise l'interactivité en développant une relation personnelle avec le consommateur ou le client, facilitant la vente « one to one »(personnalisée).
- Il permet d'envisager des politiques de fidélisation du client à travers une offre de services .
- Il facilite les transactions en évitant à l'acheteur de se déplacer.
- Il donne la possibilité de réduire les prix publics des produits en éliminant la marge laissée habituellement aux intermédiaires.
- L'enregistrement des données via Internet est quasiment automatique et demande peu d'effort.
- Il recueil une masse précieuse d'informations sur les habitudes, les besoins de l'internaute. Ainsi, plus l'utilisateur visite le site, plus on apprend à le connaître afin d'en retirer le maximum de profits [**12**].

Pour les clients

Et pour les clients les avantages sont les suivants :

- Le e-Commerce est un excellent outil de présélection.
- La recherche du meilleur prix.
- Pas de pression de la part des vendeurs.
- Un marché de proximité à l'échelle mondiale.
- Il offre un gain de temps considérable.
- Une offre actualisée (mise à jour régulière).

1.4.2 Inconvénients

Comme chaque outil commercial il présente aussi des inconvénients **[13]** :

Pour les entreprises

- Les entreprises qui ont adopté ce mode rencontrent une résistance psychologique chez certains clients.
- L'incertitude et le manque de confiance autour de la sécurisation des moyens de paiement, malgré le fait qu'actuellement les méthodes de cryptage de données assurent une confidentialité quasi parfaite lors de la transaction.
- La résistance des intermédiaires (grossistes, distributeurs) qui craignent une destruction d'emplois assortie d'une perte de chiffre d'affaire.

Pour les clients

- Il permet le pistage informatique à partir des cookies, c'est-à-dire ces petits fichiers qui identifient l'ordinateur appelant de façon unique afin de pouvoir retracer toutes les habitudes d'appel et de consommation.
- L'insécurité des paiements et la peur de tomber sur un cybermarchand malhonnête qui ne livre pas.
- Le manque de relations humaines et le sentiment d'isolement devant sa machine(cas des internautes peu expérimentés).
- Le manque de contact avec le produit.
- Les coûts de téléphone.

- Les détails et tarifs de livraison.
- Les difficultés de recours en cas d'ennuis.

1.5 Les chiffres clés du commerce électronique

Les chiffres les plus récents du commerce électronique sont éloquents.

FIGURE 1.2 – *Chiffre d'affaire du commerce électronique* [**14**].

Une très importante hausse du chiffre d'affaire du e-Commerce, ceci appuie sa croissance prononcé. "Un chiffre d'affaires multiplié par deux en trois ans", relève le ministre de l'Economie numérique.

Les Français ont dépensé 17,5 milliards d'euros sur internet au 1er semestre 2011, les sites de vente en ligne ont vu leur chiffre d'affaires progresser de 20% par rapport au premier semestre 2010 pour atteindre 8,8 milliards d'euros, selon le communiqué de presse du 8 septembre 2011 publié par la FEVAD, pour atteindre 37,8 Milliard Euro, d'ici la fin de l'année en court, conformément aux prévisions de la fevad 2011[**15**].

Progression du nombre de sites marchands actifs

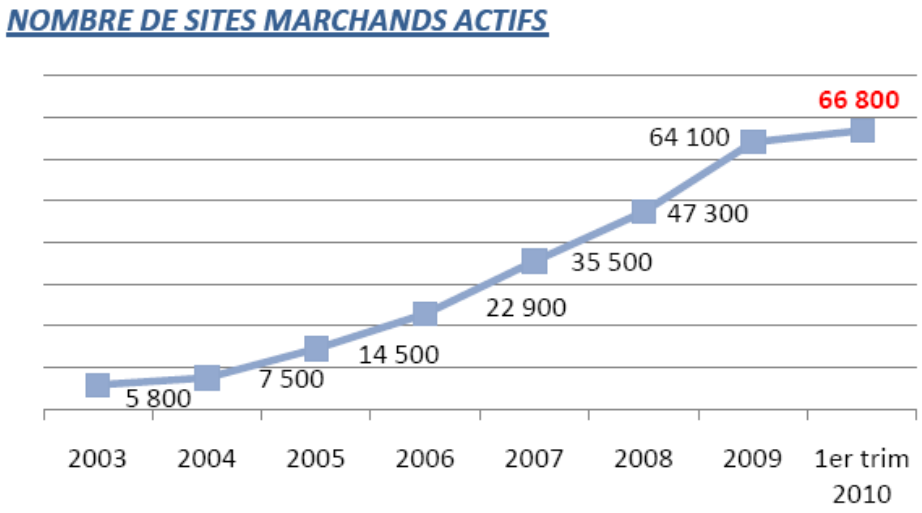

FIGURE 1.3 – *Progression du nombre de sites marchands actifs*

L'offre de site marchand continue de croitre, on compte 66 800 sites au 1er trimestre 2010, soit + 4% par rapport à la fin de l'année 2009 [**16**].

1.6 Conclusion

L'arrivée du commerce électronique constitue un vrai moteur de relance pour l'économie. Son introduction devient de plus en plus nécessaire vu le développement des nouvelles technologies dans le monde et son implantation va permettre aux utilisateures de s'engager dans le marché international.

Cependant, sa croissance dépend de la confiance manifestée par les vendeurs/acheteurs. Toute fois, ils seront moins mefiants si un moyen de paiement plus sécurisé est mis en place. ceci est le sujet de notre prochain chapitre.

2

Sécurité & E-paiement

2.1 Introduction

Lorsque l'on veut vendre sur Internet, se pose le problème du paiement électronique sécurisé. Quelle que soit l'activité ou la taille de la société, qu'il s'agisse de biens physiques à livrer, de services ou de produits numériques à délivrer en ligne... le moment du paiement en ligne est crucial. Une étude indiquait d'ailleurs, il y a quelques temps, que 67 % des internautes qui réalisaient des emplette en ligne s'arrêtaient avant la fin de ce dernier, ceci pouvant être lié au manque de choix ou de confiance, mais aussi par la peur du paiement en ligne.

C'est pourquoi les solutions de paiement se sont largement diversifiées : en Plus des solutions dites « classiques », on voit se développer de plus en plus de solutions « modernes »dans le sens où elles se servent des nouvelles technologies comme les GSM (Global System for Mobile)ou le Wifi(Wireless Fidelity) ; ou alors elles s'adaptent à une demande

bien particulière comme les problématiques de micro-paiement qui ont fait leur apparition avec les offres « premium »de nombreux sites, ce qui a poussé les prestataires bancaires et techniques à trouver de nouvelles solutions.

Renouveler son nom de domaine, acheter des fournitures de bureau, payer ses liens sponsorisés, acheter des billets de train ou d'avion pour ses voyages d'affaires... Un chef d'entreprise a mille et une bonnes raisons de recourir au paiement en ligne. Comment choisir la bonne solution de paiement ? Connaître les dangers des transactions financières en ligne et les méthodes pour payer en toute sécurité : des informations indispensables pour optimiser ses achats.

2.2 Définitions

Définition du paiement électronique (E-paiement)

Le paiement électronique est un moyen permettant d'effectuer des transactions commerciales pour l'échange de biens ou de services sur Internet. Actuellement, il est très bien implanté et utilisé par la majorité des personnes et entreprises ayant un commerce sur internet [**17**].

2.3 E-Commerce et E-paiement

Le paiement électronique constitue l'un des principaux freins au développement du commerce en ligne. Aujourd'hui encore, le grand public perçoit généralement Internet comme un espace non sécurisé où les numéros de carte bancaire peuvent être facilement volés.

Cette peur, facilement compréhensible, est pourtant en partie exagérée dans le sens où donner son numéro de carte sur le web n'est pas plus dangereux que de le donner par téléphone ou que de confier sa carte à un serveur au restaurant. Le risque est peut être plus présent après la transaction, si les numéros de cartes sont imprudemment stockés sur un serveur.

Cependant, selon une étude France Télécom datée de Mai 2010, la carte bancaire qui effraye tant de e-consommateurs est paradoxalement le moyen de paiement le plus utilisé sur Internet, avec plus d'un achat sur deux réalisé (83%) grâce aux moyens bancaires classiques (CB, chèques, mandats...). Suivent ensuite les paiements via Kiosque (35%), puis 7% par service audiotel, et enfin 4% par re-facturation de son FAI (Fournisseur d'accé Internet [**15**].

2.4 Adaptation du paiement au contexte électronique

Le paiement possède plusieurs modalités qui méritent une attention particulière au regard du commerce électronique. Le moment du paiement, son lieu, les frais qui y sont relatifs, ainsi que la quittance, sont autant d'éléments susceptibles d'y être modifiés. De la même façon, l'utilisation des moyens de paiement traditionnels tel que la carte de crédit, le chèque et l'argent comptant est différente lorsque les parties à la transaction ne sont pas en contact direct. Enfin, les moyens de preuve sur support électronique sont différents de ceux disponibles dans le cadre du commerce traditionnel.

2.4.1 Moment du paiement

Le choix du moment où le paiement sera dû est laissé à la discrétion des parties. Celles-ci fixent le moment du paiement avant ou après l'exécution de l'obligation principale, en fonction de ce qui convient le mieux à leur situation particulière. Dans la pratique du commerce électronique, le commerçant exige presque toujours le paiement au moment de l'envoi de la commande. Il s'agit d'une forme de paiement anticipé puisque celui-ci a lieu avant l'exécution de l'obligation.

2.4.2 Lieu du paiement

L'endroit où le paiement doit être effectué relève de la volonté des parties. Lorsqu'une transaction est conclue par le biais d'un site Web, les parties semblent convenir implicitement que le lieu du paiement se situe sur la plate-forme de paiement fournie à l'adresse du commerçant.

2.4.3 Quittance

La quittance est une attestation écrite par laquelle le commerçant libère le consommateur de son obligation envers lui. Une fois le paiement exécuté, le consommateur a droit à celle-ci. Dans le contexte des environnements dématérialisés, la quittance devrait prendre la forme d'un courrier électronique. Le simple affichage d'une page sur le site Web du commerçant ne semble pas suffisant puisque celle-ci peut s'avérer difficile à conserver pour le consommateur. Le courrier électronique devrait être envoyé automatiquement au moment du paiement afin de confirmer le bon déroulement de la transaction.

2.5 Moyens de paiement en ligne

2.5.1 Payer par carte bancaire

L'acheteur utilise sa carte bancaire classique pour payer. Il faut bien sûr vérifier que le site du e-Commerce sur lequel on fait nos achats est équipé d'un système de paiement sécurisé. C'est un mode de cryptage des données personnelles (nom, adresse, coordonnées bancaires) qui les rend invisibles et donc qui ne peuvent pas être récupérées par les hackers.Une fois certain de la sécurisation du site,le payeur communique ses coordonnées.

2.5.2 Payer par e-numéro de carte

C'est un moyen de paiement rattaché à la carte bancaire qui permet de payer sans donner son numéro de carte bancaire. Des e-numéros sont attribués, des numéros de carte bancaire temporaires.

2.5.3 Payer sans carte bancaire

Ce sont des services très appréciés par les internautes : ils permettent de régler ses achats sans communiquer son numéro de carte bancaire. Ils offrent aussi des tas de services connexes très intéressants pour un chef d'entreprise.
Le fameux service Paypal et son concurrent Google Checkout. Ces solutions de paiement en ligne nécessitent une adresse e-mail et un numéro de carte bancaire (vous le communiquez uniquement à Paypal lors de l'inscription). Avec un compte Paypal, vous pouvez également recevoir de l'argent : vendre un objet, demander un transfert d'argent...

2.6 Les menaces particulières aux sites marchands

Cette section compile les principales attaques techniques pouvant être exécutées au détriment d'un site de commerce électronique. Rappelons qu'une attaque est destinée à compromettre la disponibilité, l'intégrité ou la confidentialité des informations d'un tel site et que nous prendrons en compte ces trois aspects pour chaque type d'attaque.
Nous donnerons ici une vision trés synthetique de ces attaques.

Pour mieux appréhender le contexte technique de ces attaques, nous allons les classifier en trois catégories : attaques sur les protocoles de communication, attaques sur les systèmes et les applications standard et attaques sur l'information[**18**].

2.6.1 Les attaques sur les protocoles de communication

Il s'agit généralement d'exploiter les faiblesses ou anomalies des protocoles de base d'Internet (la suite TCP/IP(Transmission Control Protocol-Internet Protocol)) ou des principaux protocoles utilises dans le commerce électronique en s'appuyant sur lui (HTTP(HyperText Transfer Protocol), FTP(File transport protocole), Telnet(Telecommunication Network), SMTP(Simple Mail Transfer Protocol)). Dans cette catégorie d'attaques nous pouvons trouver :

- Les attaques visant à rendre indisponible le serveur ou un des services.
- L'écoute passive des communications et le rejeu.
- La substitution et la manipulation des données
- L'utilisation des protocoles non prévus ou le détournement des protocoles [**18**].

2.6.2 Les attaques sur le système et les applications standards

En matière de système d'information, l'émergence d'un monde ouvert et standardisé ainsi que le fondement d'Internet en tant que support universel du commerce électronique, sont des évolutions majeures. Le nombre réduit de systèmes d'exploitation (Unix, NT et assimilés) et des applications de communication basées sur des protocoles ouverts et standard (messagerie sur SMTP, accès interactif par HTTP, consultation des basses de donnés par SQL(Structured Query Language), etc.) ont permis aux éditeurs de produire à un prix raisonnable des outils de construction de sites de e-Commerce.

Mais cette standardisation facilite aussi l'élaboration de scenarios et d'outils qui per-

mettent d'exploiter les faiblesses propres soit à ces applications standard, soit à la mise en œuvre de cette application sur un type de système, par un constructeur ou par un éditeur. Cependant, les menaces les plus fréquentes ne correspondent pas à cette exploitation des faiblesses mais à la recherche et à l'exploitation de mauvaises configurations de ces services sur un site donné. Ces mauvaises configurations ont généralement pour cause des erreurs ou la méconnaissance des subtilités de l'installation des systèmes employés et des applications standard, lorsque l'on se place dans un contexte d'exposition vers Internet en général et dans le cadre du commerce électronique en particulier. Nous trouvons dans cette catégorie :

1. Des attaques sur des services réseaux non utilisés et non ou faiblement protégés ;
2. Des attaques sur la disponibilité du service par utilisation des bugs des applications ;
3. Des attaques visant à accéder au système d'information de l'entreprise [**18**].

2.6.3 Les attaques sur les informations.

C'est l'objectif principal des attaques. Sauf dans le cas des attaques visant à rendre indisponible le site, le principal objectif des attaques des catégories précédentes est d'atteindre les informations relatives au commerce électronique pour obtenir un profit, soit par la divulgation, soit par la modification de ces informations. Mais des motivations plus complexes, telles que la modification des informations pour atteindre l'image de marque de la societe, ne doivent pas être sous-estimées. Nous trouverons dans cette catégorie :

1. Les attaques à la disponibilite du site par saturation ou par manipulation des informations ;
2. Les attaques visant à une appropriation illégale des informations présentes sur le site et ne devant pas être divulguées ;
3. Les modifications malveillantes des informations affichées sur un site afin de désinformer les clients ou de compromettre la responsabilite civile des propriétaires ou exploitants ;
4. Les modifications de contenu des transactions visant un bénéfice direct [**18**].

2.7 Typologie des attaques sur le e-Commerce

La classification théorique des menaces que nous venons de faire se decline en pratique selon diverses attaques techniques contre les site de commerce électronique.

2.7.1 Ecoute passive et rejeu

L'écoute passive suivie d'un rejeu est une technique permettant de s'authentifier sur un serveur en réutilisant les paramètres d'authentification d'un tiers. Cette attaque consiste à écouter les communications réseau par un moyen passif, c'est à dire n'agissant pas sur les communications. Le but est généralement d'en extraire les identifiants et authentifiants utilisés. Il peut s'agir de mots de passe transmis en clair, mais aussi d'autres techniques d'authentification plus élaborées. En renvoyant immédiatement le couple (identifiant, authentifiant) écouté, le pirate peut se connecter au serveur, déjouant ainsi les techniques d'authentification [**18**].

2.7.2 Substitution ou manipulation de données

La substitution ou la manipulation des données est une technique de piratage consistant à envoyer au serveur de fausses informations ayant l'apparence de vraies. Le but recherché peut-être de réaliser une attaque en déni de service , par dépassement de tampon par exemple, mais aussi de générer une transaction dans l'intérêt de l'acheteur.

Par exemple, si la boutique en ligne utilise des requêtes HTTP POST afin de faire parvenir au serveur un bon de commande, et que cette requête contient le prix des articles commandes, il est facile de générer artificiellement une requête POST dans laquelle les prix ont été modifiés. Le pirate est alors en mesure de faire son prix [**18**].

2.7.3 Virus

Un virus informatique est un programme qui possède la faculté de créer des répliques de lui-même (on parle de programme auto-reproducteur) au sein d'autres programmes ou sur des zones système.

L'attaque virale d'un serveur web est relativement rare. Elle est toutefois possible, que ce soit par l'intermédiaire du webmaster (préalablement contaminé) ou par attaque pirate. Les conséquences de ce type d'attaque sont doubles :

1. Si le virus est placé dans du code s'exécutant sur le serveur, celui-ci est susceptible de subir les même dommages qu'une machine ordinaire (perte des fichiers, propagation du virus, etc.) ;
2. Si le serveur propage le virus chez des visiteurs, la responsabilité civile du commerçant peut alors être engagée [**18**].

2.7.4 Chevaux de Troie

Un cheval de Troie est un programme informatique contenant une fonction cachée, inconnue de l'utilisateur. Cette fonction est notamment utilisée afin de s'introduire dans l'ordinateur et consulter, modifier ou détruire des informations. Ces programmes sont ainsi utilisés pour récupérer des mots de passe, voir pour prendre le contrôle intégral à distance de la machine.
Il existe aujourd'hui de nombreux programmes de piratage fonctionnant selon le principe du cheval de Troie. Ces programmes pourront permettre au pirate de prendre le contrôle complet de la machine à distance, ou encore d'utiliser la machine comme relais pour une attaque élaborée vers une cible secondaire.
Les attaques en déni de service réparties fonctionnent à l'aide d'un programme apparente aux chevaux de Troie. C'est alors la machine piratée qui semblera attaquer la cible finale. La responsabilité de l'entreprise peut dans ce cas être recherchée. Il est donc fondamental de se protéger afin de ne pas servir de relais [**18**].

2.7.5 Répudiation

La répudiation consiste à nier avoir participé à une transaction. Par exemple, si le client peut nier avoir fait un achat, et refuser le paiement. Selon les systèmes de paiement utilisés, le commerçant peut alors ne pas être payé, alors que la marchandise aura été livrée.
Même si la répudiation est parfois légitime pour le client (dans le cas où il n'aurait réellement pas passe la commande), le vendeur subit dans tous les cas une perte sèche, à moins que le système de paiement ne garantisse le recouvrement.
La signature électronique ayant désormais valeur légale, il est de l'intérêt du commerçant de se prémunir contre les risques de répudiation [**18**].

2.7.6 Déni de service

Le déni de service est un type d'attaque informatique. Il consiste à rendre un service informatique (par exemple, un serveur Internet) indisponible.
Une méthode d'attaque en déni de service couramment utilisée actuellement est l'attaque repartie, elle consiste à générer des flux d'information adressés à la machine cible depuis un grand nombre de machines relais situées un peu partout sur le réseau Internet.
Une autre méthode couramment employée lors des attaques en déni de service est le dépassement de tampon. Elle consiste à envoyer au serveur un message plus grand que la capacité de réception du serveur. Ce message peut être fabriqué à l'aide des techniques de substitution et de manipulation de données [**18**].

2.7.7 Spamming

Le spamming consiste en l'envoi massif de courriers électroniques non sollicités, généralement à tendance commerciale ou pseudo-commerciale.
Pour le commerçant, « spammer »ses clients serait plutôt une mauvaise idée : cela risque de les faire fuir, et cela portera dans tous les cas préjudice à l'image de l'entreprise. Toutefois, l'attaque dont nous parlons ici est le spamming réalisé par un tiers à l'insu du commerçant.
Cette attaque est possible si le « spammeur »parvient à récupérer la liste des clients en piratant le serveur web, ou si le commerçant gère une liste de diffusion permettant à un tiers d'envoyer un message. De nombreux commerçants électroniques mettent en place une liste de diffusion, qui leur sert par exemple à avertir leurs clients de nouveautés ou de promotions. Il est fondamental que le logiciel de gestion de liste soit paramétré de sorte que seul le propriétaire de la liste, c'est-à-dire le commerçant, ait la possibilité d'envoyer un message sur la liste.
De la même manière, le commerçant devra prendre soin que ses passerelles de messagerie soient configurées de manière à interdire le mail-relay (possibilité pour un tiers de faire partir du courrier depuis le serveur de messagerie de l'entreprise). En effet, les serveurs ouverts au mail-relay sont utilisés prioritairement par les « spammeurs »pour se camoufler.

2.8 Techniques de Sécurité de l'e-paiement

2.8.1 Chiffrement

Le chiffrement(ou cryptage) est l'action de transformation d'un texte **lisible** en un texte **illisible**, via une clé de chiffrement. Seule une personne disposant de la clé de déchiffrement (qui peut être la même que celle de chiffrement) sera en mesure de déchiffrer le texte [**19**].
On distingue deux types de chiffrement :

Chiffrement symétrique

Un procédé de chiffrement est dit **symétrique** si les clés de chiffrement et de déchiffrement sont les mêmes. Le chiffrement symétrique est aussi appelé **chiffrement à clé secrète**, puisque cette clé ne doit être connue que par des personnes censées avoir le droit de chiffrer/déchiffrer le message [**19**].

Chiffrement asymétrique

Le chiffrement asymétrique est aussi appelé **chiffrement à clé publique**.En effet, si une personne souhaite que ses correspondants lui envoient des messages chiffrés, elle devra alors générer 2 clés : Une première clé servant à chiffrer les messages, qui devra être communiquée à ses correspondants, pour que ceux-ci l'utilisent afin de chiffrer leurs messages. Une seconde clé, servant quant à elle au déchiffrement, et qui devra rester privée, afin que seule la personne émettrice des clés puisse déchiffrer les messages [**19**].

2.8.2 Signature numérique

La signature numérique d'un document électronique à pour vocation de répondre aux mêmes exigences que la signature manuscrite d'un document papier [**19**] :

- Permettre d'authentifier l'auteur d'un document.
- Garantir qu'une fois signé, le document ne sera plus modifié (falsifié).
- Donner une valeur juridique (sous certaines conditions) au document.

En pratique, une signature numérique est nettement plus fiable qu'une signature manuscrite, puisque cette technologie utilise la technique du chiffrement asymétrique : vous

signez numériquement un document à l'aide de votre clé privée, et la lecture du document se fait par l'intermédiaire de la clé publique correspondante, en général transmise avec le document puisque contrairement au chiffrement classique, le but n'est pas de rendre secret le contenu du message.

Ces clés font partie de ce qu'on appelle **un certificat d'authentification**(voir section 2.8.4) la valeur juridique du document n'est reconnue que si le certificat d'authentification a été fourni par un organisme certifié et agréé. Il existe des logiciels gratuits pour permettre de signer numériquement les documents (le plus connu étant PGP), mais ces documents n'auront donc pas de valeur légale.

2.8.3 Infrastructure à clés publiques

Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques ou HSM(Hardware Specific Module), des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques [**20**].

Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs :

- Enregistrement des utilisateurs (ou équipements informatiques).
- Génération de certificats.
- Renouvellement de certificats.
- Révocation de certificats.
- Publication de certificats.
- Publication des listes de révocation (comprenant la liste des certificats révoqués).
- Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'IGC).
- Archivage, séquestre et recouvrement des certificats (option).

2.8.4 Certificat d'authentification

Un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé **autorité de certification** (souvent notée CA pour Certification Authority).
L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité, ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

2.9 Protocole de sécurité dans le paiement en ligne

Nous allons voir les trois (03) protocoles les plus utilisés dans la sécurité du paiement en ligne :

2.9.1 Protocole SSL

Définition

SSL(Secure Sockets Layers,ou couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet. Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet. Son principe consiste à établir un canal de communication sécurisé (chiffré)entre deux machines (un client et un serveur) après une étape d'authentification.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP(Post Office Protocol) ou IMAP(Internet Message Access Protocol). En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).

De cette manière, SSL est transparent pour l'utilisateur. Par exemple, un utilisateur qui se connecte à un site du commerce électronique sécurisé par SSL enverra des données chiffrées sans aucune manipulation nécessaire de sa part.

Un serveur web sécurisé par SSL possède une URL(Uniform Resource Locator) commençant par https ://, où le « s »signifie bien évidemment secured (sécurisé). Il a été renommé en 2001 Transport Layer Security (TLS).Il y a très peu de différences entre SSL version 3 et TLS version 1, TLS diffère de SSL pour la génération des clés symétriques. Cette génération est plus sécurisée dans SSLv3 dans la mesure où aucune étape de l'algorithme ne repose uniquement sur MD5(Message Digest 5), pour lequel sont apparues des faiblesses en cryptanalyse. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.

Fonctionnement de SSL

La sécurisation des transactions par SSL est basée sur un échange de clés entre client et serveur. La transaction sécurisée par SSL se fait selon le modèle suivant :

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- Le serveur à la réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du crypto système le plus haut dans la liste avec lequel il est compatible.
- Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire, chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

Mise en œuvre d'un service HTTPS

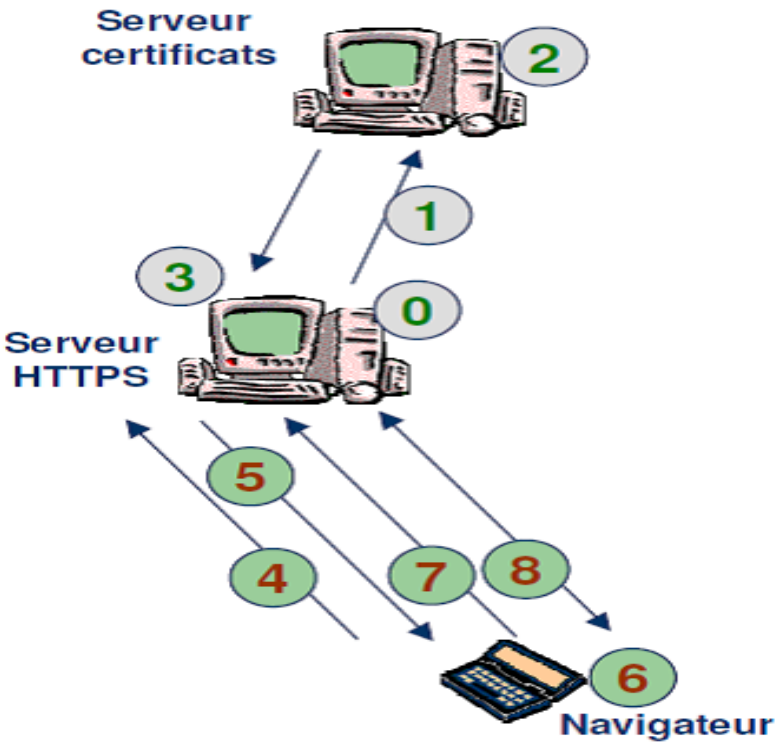

FIGURE 2.1 – *Etapes de la mise en œuvre d'un service HTTPS*

Phase Mise en production

– 0 : Génération clé publique / clé privé.

– 1 : Demande auprès d'une autorité (publique) d'un certificat serveur.

– 2 : Génération du certificat serveur.

– 3 : Installation du certificat serveur sur le Serveur Web.

Phase Navigation internaute

– 4 : Ouverture connexion SSL : « clic sur URL https ://www.x.dz ».

– 5 : Envoi certificat du serveur vers le client.

– 6 : Génération clé de session symétrique.

– 7 : Envoi clé symétrique (chiffrée avec clé publique du serveur).

– 8 : Echanges protégés (confidentialité, intégrité).

2.9.2 Protocole SET

Le SET (Secure Electronic Transaction) est un protocole destiné spécialement à sécuriser les transactions Internet de paiement par carte bancaire. Il a été développé à l'origine

par Visa International et MasterCard, en 1996, avec l'aide des grandes compagnies informatiques de la planète.

Son champ d'application se réduit au chiffrement des seules données bancaires, contrairement à SSL qui peut chiffrer les images et le texte. Le protocole SET implique trois parties : le client, le vendeur et la banque du vendeur. Ce système SET requiert des certificats auprès des trois parties. Les certificats du client et du vendeur sont fournis par leurs banques respectives après quoi la transaction commerciale peut avoir lieu. Avec le SET, le numéro de carte bancaire peut ne pas être connu du vendeur, donc ne sera pas stocké dans ses fichiers et être récupéré par une personne mal intentionnée. Le SET assure en principe une transaction de non répudiation, mais cette clause peut varier d'un pays à l'autre suivant la législation en vigueur.

2.9.3 Protocole 3-D Secure

Définition

3-D Secure est un protocole de paiement sécurisé sur Internet. Il a été développé par Visa pour augmenter le niveau de sécurité des transactions, et il a été adopté par Mastercard. Il permet une meilleure authentification du détenteur de la carte de paiement lors d'achats effectués sur des sites web. 3-D Secure ne doit être confondu ni avec le code secret de la carte bancaire, ni avec le cryptogramme visuel (3 derniers chiffres imprimés au dos de la carte).

Fonctionnement

Le concept de base de ce protocole (basé sur XML(Extensible Markup Language)) est de lier le processus d'autorisation financière avec une authentification en ligne. Cette authentification est basée sur un modèle comportant 3 domaines (d'où le nom 3D) qui sont :

- Le commerçant (Acquirer Domain en anglais)
- La banque (Issuer Domain en anglais)
- Le système de carte bancaire (Interoperability Domain en anglais)

Le protocole utilise des messages XML envoyés via des connexions SSL (qui garantit l'authentification du serveur et du client par des certificats numériques).

Mode d'authentification

Selon la banque émettrice de la carte, les modalités d'authentification varient, Nous avons pris exemple sur quelques banques françaises

- Crédit Mutuel : Le client doit s'authentifier avec son identifiant de banque en ligne, puis indiquer un des codes inscrit sur sa « carte de clés personnelles »(une grille de 64 codes à 4 chiffres dans laquelle il faut piocher le bon code en fonction de la ligne et de la colonne demandée par le site web).
- BNP Paribas : Le client doit indiquer sa date de naissance ; depuis juillet 2009 un code est envoyé par SMS(Short message service).
- Société Générale : Le client doit indiquer sa date de naissance, depuis septembre 2009 un code est envoyé par SMS.
- Groupama Banque : Le client doit indiquer son nom, le code postal de sa résidence et sa date de naissance.

2.10 Conclusion

Malgré les efforts de sécurisation, toute information échangée sur Internet ne peut être complètement à l'abri de l'intrusion maligne dans les systèmes informatiques.
Les caractéristiques spécifiques d'un site de commerce électronique consistent à prévoir et anticiper la montée en charge de ce site. La démarche de sécurité doit être structurée. De plus, l'architecture informatique doit intégrer la souplesse et le renouvellement permanent inhérent au métier du commerce.
En effet, le commerce, qu'il soit traditionnel ou électronique, est toujours basé sur la confiance. Cette confiance, qui doit s'établir entre un acheteur et un vendeur, ne s'obtient pas sans sécurité. Cette confiance fera l'objet de notre prochain chapitre.

3

La confiance dans le commerce électronique

3.1 Introduction

Le développement des systèmes informatiques distribués donne lieu à l'existence de plusieurs entités de différentes natures qui coopèrent et collaborent entre elles afin de réaliser des tâches particulières. La collaboration est le résultat de l'interaction, l'échange et même le partage d'un ensemble d'informations entre les différentes entités. Cet échange nécessite un certain degré de confiance qui varie selon l'importance des données échangées.

L'hétérogénéité des définitions et l'absence d'une définition simple et commune de la confiance ne doit pas surprendre puisqu'il s'agit d'un phénomène traité par différentes disciplines. Ainsi, les points de vue recensés sont à definir dans un contexte bien spécifique selon les objectifs finaux de chacun.

Dans une étude menée durant l'été 2000, le cabinet de conseil en marketing Dia-Mart et

la société To Team constataient, que le paiement en ligne était en France le premier frein au développement du commerce sur Internet. Mais, interrogés sur les éléments susceptibles de les rassurer dans leurs achats en ligne, les internautes exprimaient des attentes qui n'ont parfois qu'un lien très indirect avec la sécurisation des paiements. La notoriété de l'enseigne, la présence de magasins physiques, le contrôle sur le processus de commande, venaient avant les processus de sécurisation des paiements en ligne. Conclusion du cabinet : « les internautes ne veulent pas de la sécurité, mais de la confiance ».

3.2 La notion de la confiance

La question de la confiance est fréquemment posée dans différents domaines de la vie et c'est sans doute parce qu'elle est en crise qu'elle fait aujourd'hui l'objet d'une attention spécifique en particulier dans le domaine économique où elle est largement évoquée et analysée. A l'heure actuelle, il n'existe pas un consensus sur la définition de la confiance ; ceci est dû essentiellement à sa nature ambiguë. Par conséquent, la notion de la confiance demeure confuse et l'établissement d'une définition cohérente reste encore à établir [**21**].

Certains chercheurs préfèrent ne pas définir la confiance, tandis que d'autres lui associent diverses définitions.

3.2.1 Définitions et avantages de la confiance

Dès les travaux fondateurs de Deutsch[**22**], la confiance est définie par les intentions et les attentes croisées des personnes impliquées dans une situation d'échange.

Suite à cette définition, une pléthore de la notion de la confiance ont été présenté dans la littérature.

Ces définitions sont liées aux domaines d'applications c'est-à-dire la mise en valeur de ses caractéristiques essentielles varie selon les disciplines, les auteurs et les domaines [**23**]. Des définitions simples peuvent être trouvées, comme en théorie des organisations où le concept de confiance s'associe aux concepts de coordination, de coopération et d'engagement, ou bien en marketing où la confiance est considérée comme un facteur important de la stabilité des relations d'échange fournisseurs-clients et inter-firmes [**21**]. D'autre part, pour le professionnel du marketing Georges Fischer qui considère simplement que la

confiance est un actif immatériel [**24**].

De son côté, le scientifique des technologies de sécurité Michel Riguidel définit la confiance comme « une relation non réflexive, non symétrique et non transitive ». « Non réflexive »signifie qu'on ne se fait pas nécessairement confiance à soi-même. « Non transitive »signifie que la confiance ne se transfère pas. « Non symétrique »signifie que la confiance n'est pas nécessairement réciproque [**24**].

De leur côté, Mc Knight et Chervany[23], ont considéré que la confiance est supportée par un ensemble de métriques. Ils l'ont définie comme la croyance en la bonne foi, la loyauté, la sincérité, la fidélité d'autrui (ou en ses capacités), la compétence et la qualification professionnelle.
D'un point de vue sociologique, Putnam [**25**], a jugé que la confiance crée des capitaux sociaux, où le capital social est défini par Coleman [**26**] comme : « the ability of people to work together for common purposes in groups and organizations ».
D'un point de vue économique, la confiance représente un moyen pour diminuer les coûts associés aux critères de choix d'un produit/service et permettant de décider de la réalisation d'une transaction.

Une définition assez captivante est celle de Rotter [**27**] « Trust is a generalized expectancy held by an individual or group that the word, promise, verbal or written statement of another individual or group can be relieved on ». De toutes ces définitions découle le fait que la confiance est un élément fondateur de tout échange et c'est un facteur essentiel pour la stabilité et la continuité, dans le temps, des relations entre les parties. En plus des avantages économiques, les chercheurs soulignent aussi que la confiance dispose d'un impact important sur l'utilité des sites, et sur la fixation des intentions des visiteurs [**28**].

3.2.2 Les origines de la confiance

C'est en connaissant l'origine de la confiance qu'on estime, pouvoir parvenir à la stimuler. Plusieurs auteurs ont mis en relief ces sources en tentant de dresser la liste des types de confiance. L'inventaire des sources identifiées révèle que deux types de sources peuvent être distinguées et qu'il est utile de les présenter ainsi dans un souci de clarté. D'une part, il y a les sources directes de la confiance. Ce sont les circonstances ou les faits

qui agissent sans intermédiaire sur le degré de confiance du client. D'autre part, il y a les sources indirectes de la confiance ce sont les autres confiance des acheteurs/vendeurs, la réputation du marchand [**29**]. Selon certains auteurs, ces expressions pourront prendre un sens plus ou moins restrictif. Ce sont les circonstances ou les faits qui ont pour effet d'encourager ou de contraindre le destinataire de la confiance à honorer son engagement, ce qui provoque par ricochet la confiance de l'autre entité. Selon Williams, ce genre d'incitatif serait même indispensable pour établir la confiance ; il faudrait impérativement qu'il y ait des structures, des assurances, des garanties pour générer la coopération [**29**].

3.2.3 Le rôle de la confiance

On ramène souvent la confiance à l'idée générale, en apparence très simple, qu'elle serait un lubrifiant des rapports sociaux, un facilitateur dans la mise en place de relations entre les acteurs économiques. Des auteurs comme Alain Peyrefitte et Francis Fukuyama [**30**], ont décrit la confiance comme un facteur crucial de développement. Niklas Luhmann [**31**], a présenté la confiance comme un mécanisme permettant de réduire la complexité de l'existence. Anthony Pagden [**32**], s'est attaché à illustrer comment la prospérité peut être affectée lorsque la confiance est prise d'assaut. Il n'est dès lors pas surprenant que des économistes l'aient décrite comme un catalyseur de transactions, un facteur de prospérité et un stimulant à l'investissement. L'accent sera mis sur ces facettes, même si plusieurs autres rôles, qui ne sont pas nécessairement de nature économique, ont été avancés. La vigilance des parties à une transaction permet d'appréhender les comportements opportunistes et de réduire les coûts liés à ces comportements. Cependant, la vigilance a aussi son coût. En ce qu'elle permet d'abaisser le niveau requis de vigilance, la confiance aurait pour effet de faciliter les transactions et d'en réduire le coût [**29**].

3.2.4 Quelques spécificités de la confiance électronique

Un contexte risqué et une vulnérabilité plus accrue

Si certains sites proposent le paiement à la livraison, pour la majorité le règlement s'opère à la commande. Le consommateur est alors un peu perdu, lui, qui a l'habitude d'acquérir le produit tout de suite après le paiement. Il devient dépendant du marchand et il n'a aucune emprise sur ses actions, le consommateur se place dans une situation de

vulnérabilité. Intimement liées, les notions de vulnérabilité et de risque vont de pair. Sur Internet, si le consommateur est autant vulnérable c'est parce qu'il est confronté à un contexte risqué.

Absence physique d'un vendeur

Une des particularités de l'achat sur Internet est l'absence physique d'un vendeur. Ainsi, à une relation interpersonnelle se substitue une interaction homme-machine.

3.3 Quelques determinants de la confiance en ligne

3.3.1 Qualité perçue du site :

Dans les recherches, la qualité d'un site apparaît comme un facteur important de la confiance. C'est une variable charnière qui pourrait influencer le jugement du consommateur sur le marchand. En effet, le site est un médiateur entre le consommateur et l'entreprise vendant ses produits sur Internet. Pour les marchands peu connus, le site est la première impression que le consommateur aura sur l'entreprise. Dans la mesure où une certaine image est véhiculée par le site (Crobitt et al., 2003), il est important que ce dernier traduise le sérieux et le professionnalisme du marchand. Ainsi, à l'instar d'un vendeur qui doit avoir une apparence physique soignée, un site web doit aussi avoir une qualité de présentation qui inspire confiance [**33**].

3.3.2 Sécurisation et vie privée :

La sécurisation est une question fondamentale et pour le moins cruciale dans le contexte des transactions électroniques. Son impact sur la confiance a été mis en évidence par plusieurs chercheurs (e.g., Yoon, 2002, Suh et Han, 2003, Corbitt et al., 2003). Sur Internet, toute information échangée peut être interceptée par des tierce non autorisés. L'utilisation frauduleuse des numéros de cartes de crédit demeure la crainte majeure des consommateurs. Pour réduire le risque de violation de la confidentialité des données et se prémunir contre le phénomène du hacking, les marchands ont recours à des technologies avancées (e.g., les protocoles SSL , SET ,...). Le cryptage 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 décoder.
La sécurisation est une condition nécessaire mais non suffisante pour construire la confiance. En effet, comme le soulignent Shankar et al. (2003).
aujourd'hui « la confiance est beaucoup plus large que la sécurisation et la vie privée ». Plus clairement, un site non sécurisé suscitera d'emblée la méfiance des consommateurs, en revanche, le fait qu'un site soit sécurisé n'aura qu'un impact marginal sur la confiance. A partir de là, on voit bien l'asymétrie de l'effet de cette variable. Sa présence n'affecte que marginalement la confiance alors que son absence peut être rédhibitoire pour l'achat [**33**].

3.3.3 Réputation perçue du marchand :

Au même titre que les travaux traditionnels sur la confiance, la réputation est un déterminant important de la confiance en ligne (Jarvenpaa et Tractinsky, 1999 ; Fung et Lee, 1999 ; Mcknight et al., Yoon, 2002). Une bonne réputation constitue un gage permettant de rassurer le consommateur. En effet, les marchands renoncent à agir d'une façon opportuniste pour préserver leur capital « réputationnel ». La réputation renvoie à l'historique, au passé de l'entreprise. C'est dans ce sens qu'elle garantit une certaine prévisibilité du comportement futur. Mcknight et al. (2002) soulignent que la réputation est particulièrement prépondérante dans la phase initiale du développement de la confiance. En effet, faute d'avoir une expérience personnelle avec le marchand électronique, le consommateur base son jugement sur les évaluations des parties tierces. Ainsi par exemple, si un ami ou un proche a déjà eu une expérience positive avec le marchand, la confiance 'initiale' du consommateur s'en trouve d'emblée affectée. De même, l'image véhiculée par les médias (émissions télévisées, magazines spécialisés,...) contribue inéluctablement à affaiblir, renfoncer ou à construire la confiance vis-à-vis des vendeurs Internet [**33**].

3.3.4 Satisfaction par rapport aux expériences passées

A l'instar des travaux sur la confiance traditionnelle (e.g., Ganesan, 1994), la satisfaction suite à des interactions passées avec le marchand est un facteur explicatif de la confiance (Pavlou, 2003). Comme la réputation, elle renvoie à un passé, à un historique. En revanche, elle suppose une évaluation d'une expérience personnelle faite par le consommateur (et non par des tierce) sur une transaction donnée ou à un ensemble de

transactions. Déterminant important de la confiance, la satisfaction doit être considérée avec prudence. En effet, un consommateur satisfait a de grandes chances de renouveler sa confiance vis-à-vis du site. Toutefois, la moindre insatisfaction peut être fatale pour le marchand [**33**].

3.3.5 Propension à faire confiance

La propension à faire confiance ou la disposition à faire confiance a été étudiée notamment en psychologie (Rotter,1967). Assez curieusement, peu nombreuses sont les recherches en marketing l'ayant intégrée dans leurs modèles. Toutefois, des travaux en commerce électronique attestent du regain d'intérêt pour cette variable (e.g., Gefen, 2000, Lee et Turban, 2001, Mcknight, Choudhury et Kacmar, 2002 ; Stewart, 2003). Elle est considérée comme un trait de personnalité stable qui se manifeste à travers différentes situations. Elle permet de distinguer les individus généralement « confiants »et(ou de) ceux généralement « méfiants ». Les individus manifestant une tendance stable à être « confiants »présument d'emblée que les « autres »sont dignes de confiance jusqu'à preuve du contraire [**33**].

3.3.6 Familiarité avec le site/avec Internet

La familiarité fait référence au nombre d'expériences antérieures accumulées par le consommateur (Alba et Hutchinson, 1987). Elle suppose la compréhension d'un état présent permettant d'asseoir des attentes quant à un état futur (Gefen, 2000). Certains auteurs vont même jusqu'à dire que la familiarité est une condition préalable à la confiance (Luhmann, 1979). Fondée sur tout un historique, la familiarité permet de garantir une certaine prévisibilité du comportement. Dès lors, que la prévisibilité est de mise, la confiance pourrait trouver un terrain propice pour se développer. La familiarité favorise donc la formation de la confiance. L'impact positif significatif de la familiarité (avec le site et/ou avec Internet) sur la confiance a été d'ailleurs démontré par plusieurs auteurs (e.g., Gefen, 2000 ; Bhattacherjee, 2002 ; Gefen et Straub, 2004, Corbitt et al., 2003)) [**33**].

3.3.7 Le risque perçu

La notion du risque renvoie à l'incertitude quant aux potentielles conséquences négatives relatives à une décision d'achat (Bauer, 1960). Dans le contexte d'un achat sur Internet, trois dimensions du risque perçu deviennent particulièrement prépondérantes : le risque financier (inhérent au paiement via Internet), le risque privé et le risque de performance. Le risque financier renvoie à l'éventuelle utilisation frauduleuse des données bancaires. Le risque privé fait référence au fait que des informations personnelles données sur un site commercial peuvent être utilisées à d'autres fins (Cases, 2002). Le risque de performance fait référence à la qualité réelle du produit. En effet, dans un contexte virtuel, le produit, objet de l'échange, devient insaisissable, non palpable. Pour prendre sa décision, le consommateur devra se contenter de quelques représentations imagées du produit et faire confiance au descriptif présenté sur le site [**33**].

3.4 Conséquences de la confiance

3.4.1 L'intention d'achat sur le site

Le client est à la quête de signaux montrant que le marchand mérite sa confiance. Faute d'expériences antérieures, la confiance du consommateur est plutôt basée sur le jugement d'autrui (réputation du marchand, recommandation d'un proche...). Il s'agit plutôt d'une confiance " initiale " ou " exploratoire " qui se fonde plutôt sur les évaluations des parties tierces. A ce stade, une digression s'impose. En effet, selon les caractéristiques du marchand, les variables intervenantes (réputation, recommandations, qualité du site) ne semblent pas avoir le même poids.

3.4.2 L'intention de recommander le site

Si les consommateurs se réfèrent au bouche à oreille pour juger la qualité d'un produit, d'un service ou d'un vendeur Internet, ils peuvent aussi en produire (Dianne, Cermak et Prince, 1994). D'une part, les consommateurs ayant reçu une information favorable sur un marchand vont lui accorder plus facilement leur confiance. D'autre part, les consommateurs " confiants " vis-à-vis d'un marchand seront plus enclins à recommander le site à leur entourage (famille, amis...=).

3.4.3 L'intention de retour sur le site

L'intention de retour sur le site traduit l'intention du consommateur de consulter à nouveau le site que ce soit pour s'informer ou pour acheter. Si le marchand arrive à inspirer confiance au consommateur, il est fort probable que ce dernier finisse par adopter le site (i.e., l'utiliser d'une façon récurrente). L'impact de la confiance sur l'intention d'utiliser le site a été démontré par plusieurs chercheurs (Suh et Han, 2003 ; Gefen, 2000).

3.5 Travaux relatifs

3.5.1 Le rôle de l'intimité et de la sécurité

F. Belanger et al [**34**], ont étudié l'importance relative, lors d'achat de biens et de services en ligne, en considérant quatre indices de confiance (cachet d'intimité de tierce, attributs du site, cachet de sécurité de tierce, et dispositifs de sécurité). Les résultats indiquent que les dispositifs de sécurité sont évalués, par les consommateurs, sensiblement plus que les trois autres indices.

Les résultats de leur étude ont également indiqué que la présence de cachet d'une tierce partie, qu'il soit d'intimité ou de sécurité, augmente considérablement leur confiance. Aussi, ils révèlent qu'en prenant la décision de fournir des informations privées, les consommateurs comptent sur leurs perceptions de fiabilité indépendamment de si le négociant est électronique seulement ou terre et électronique. En outre, ils ont remarqué que les dispositifs d'intimité et de sécurité étaient de peu d'importance que ceux de plaisir. Le but primaire de cette étude, faite sur un échantillon, était d'examiner l'importance relative du site web reflétant la sécurité et l'intimité. Les résultats indiquent que les dispositifs de sécurité étaient les plus importants pour le consommateur. Ils expliquent encore qu'il est possible que les utilisateurs ne comprennent pas le concept de la sécurité et celui de l'intimité, la sécurité étant un concept plus concret.

Ils affirment que l'importance des attributs de site Web est au-dessus et au delà des soucis d'intimité et de sécurité. Par ailleurs, L'étude accentue l'importance d'employer la sécurité et l'intimité en tant que deux concepts distincts, quoiqu'elles soient conceptuellement connexes.

3.5.2 En utilisant la logique floue

Les auteurs Meziane et Nefti [**35**], ont mis au point un nouveau modèle pour évaluer la confiance à l'aide d'un raisonnement flou, ils l'ont choisi car il permet l'encodage de l'information disponible sur le site du marchand sous une forme qui peut être utilisée pour refléter la manière d'atteindre la décision des clients pour s'engager dans une transaction électronique.

L'utilisation d'un raisonnement flou est l'approche adéquate pour mesurer les données complexes. Le modèle proposé se compose de cinq modules (existence, affiliation, politique, et réalisation), le cinquième module décision machine sera utilisé pour évaluer le facteur de confiance.

Durant la phase de transformation en un ensemble flou , trois fonctions (faible, élevée, et moyenne) seront utilisées pour toutes les variables qui sont reliées aux modules. Elles seront appliquées pour le module décision machine. Ces fonctions appartiennent à l'intervalle [0,1] avec 0 pas de confiance et 1 confiance totale.

Si une grande quantité d'informations est disponible sur le site d'un fournisseur et si ces informations sont valides alors on peut faire confiance au marchand. Toutefois, l'importance de ces facteurs varie d'un client à l'autre.

3.5.3 Information fournie sur les sites Web des négociants

F Meziane et Kasiran [**36**], appuient le fait de considérer des variables pour essayer de mesurer ou de juste comprendre le rapport de la confiance entre le fournisseur et le consommateur. Ils trouvent que des stratégies doivent être établies pour assurer la fiabilité et des systèmes doivent être développés pour aider les consommateurs à évaluer le niveau de confiance.

Les deux auteurs définissent la confiance comme étant la bonne volonté d'un individu de se comporter de façon à ce qu'il suppose qu'une autre partie se comportera selon des espérances dans une situation risquée.

Ils affirment qu'il n'est pas question de seulement identifier et comprendre les facteurs qui favorisent la confiance en ligne mais également fournir aux utilisateurs inexpérimentés des outils pour les aider à vérifier la disponibilité d'une telle information sur le site Web du négociant et à comprendre cette information.

Dans la recherche suivie dans cet article des variables principales ont été identifiées, puis un système d'extraction de données est alors développé pour extraire et localiser ces variables sur des sites Web. C'est alors qu'un modèle basé sur l'information actuelle sur les sites Web des négociants est développé pour évaluer la confiance du site Web. En conclusion, les deux auteurs ont évalué un échantillon de sites Web du e-Commerce quant à l'ensemble de variables identifiées pour découvrir si elles sont largement répandues dans des sites Web du e-Commerce.

3.5.4 Webtrust

Le concept WebTrust [**37**], a été développé par AICPA(American Institute of Certified Public Accountants) et par CICA (Centre International de Communication Avancée) en collaboration avec VeriSign. Si la page Web d'un prestataire porte le sceau WebTrust, un client peut en déduire que le prestataire concerné remplit les critères élaborés par l'AICPA et par le CICA et que la page Web a été contrôlée sur le respect de ces critères par un représentant des CPA(Certified Public Accountant), la confiance du client dans le commerce électronique peut être renforcée.

WebTrust a été développé à partir de deux points de vue. Premièrement, il devait être difficile de falsifier ce sceau de confiance et, deuxièmement, il devait être facile d'éliminer un prestataire si son application de commerce électronique ne remplissait plus les critères.

En cliquant sur le sceau, les clients peuvent contrôler s'il s'agit d'un prestataire détenteur légitime du sceau de confiance. Une confirmation lui est ainsi indiquée s'il a affaire à un participant au programme WebTrust. Afin de pouvoir transposer les exigences techniques du WebTrust, l'AICPA et le CICA ont collaboré avec VeriSign. L'article fait uniquement référence au sceau de confiance « Business to Consumer »le plus largement développé et le mieux connu, sceau pensé pour l'établissement de la confiance entre les clients et les prestataires.

Pour qu'un participant obtienne l'autorisation de pouvoir arborer sur sa page Web le sceau WebTrust, il doit remplir tous les principes et les exigences fixés au préalable. L'AICPA et le CICA ont déterminé trois principes au moyen desquels les participants du programme WebTrust sont évalués. Pour chaque principe, des critères détaillés ont été fixés.

1. Le participant doit rendre publiques ses pratiques commerciales dans le domaine du commerce électronique.
2. Il s'agit de contrôler si les transactions sont complètes, exécutées correctement et facturées comme convenu
3. Des contrôles sont définis afin d'assurer que les données du client ne sont utilisées que dans le but pour lequel elles sont effectivement prévues.

3.5.5 Confiance dans le commerce électronique de C2C

Pour développer et examiner un modèle de confiance d'e-Commerce du consommateur-à-consommateur (C2C). K Jones [**37**], ont considéré deux secteurs qui peuvent influencer la confiance d'une personne :interne et externe. Les influences internes se composent de la propension normale d'une personne de faire confiance et de la perception d'une personne de la qualité de site Web dans lequel il est près a effectué des transactions d'e-Commerce de C2C. Les influences externes se composent de la confiance de l'acheteur et/ou du vendeur autrement dit la réputation et de leur identification par des établissements de tierce.

Aprés avoir effectué l'étude sur un échantillon d'étudiants composé d'acheteur et de vendeur.Les auteurs affirment que la confiance d'e-Commerce de C2C est différente de celle d'e-Commerce de B2C. Car ils ont constaté que seulement la perception de la qualité de site Web et de l'identification de tierce ont influencé la confiance d'e-Commerce de C2C, contrairement à l'environnement B2C. Par conséquent, de manières à aider les réalisateurs d'e-Commerce à fournir une atmosphère digne de confiance et à identifier les consommateurs dignes de confiance, ils ont suggéré que les consommateurs de C2C devraient se concentrer sur l'établissement des sites Web de qualités et de d'une tierce partie afin d'améliorer la confiance, par conséquant, améliorer potentiellement leur volume de transaction.

3.5.6 Au delà du souci : le modèle intimité-confiance-intention comportementale de commerce électronique

Les soucis d'intimité pour l'e-Commerce de B2C sont devenus une question importante en raison de la participation directe des clients et de la capacité potentielle de l'organisation d'accéder, stocker, et partager cette information personnelle.

C'est pour cela que C Liu [**38**], ont voulu proposer et examiner un modèle théorique qui va essayer d'expliquer comment l'intimité influence la confiance et la confiance influence l'intention comportementale du consommateur pour effectuer des transactions en ligne en tenant compte de la perception d'individu de l'intimité. Le modèle est illustré dans figure suivante :

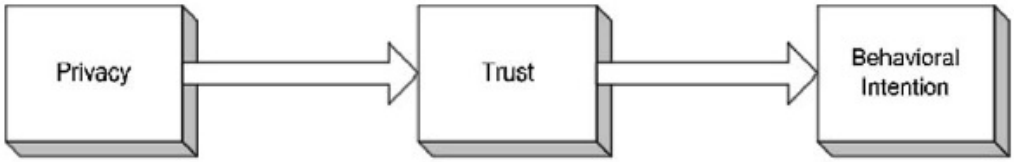

FIGURE 3.1 – *Privacy-trust-behavioral intention model.*

Alternativement, le modèle suggère que la confiance est une variable intermédiaire importante qui influence l'intention comportementale d'un client pour effectuer des transactions en ligne.

Les auteurs ont fait leurs études sur un échantillon d'étudiants, où ils les ont invité a acheté des livre sur Internet, ceci en considérant deux sites, un qui répond aux quatre dimensions (notification, accès, choix, et sécurité), et un autre qui ne l'est pas. Les sujets sont informés que des informations personnelles seront demandées et enregistré. Enfin, un questionnaire leurs a été passé.

Les résultats empiriques ont approuvé les directions hypothétiques. En outre, les résultats d'étude ont indiqué que la perception d'intimité a fortement influencé la confiance, et la confiance, à son tour, a fortement influencé l'intention comportementale.

Il s'avérerait également qu'une compagnie peut augmenter le niveau de la confiance et de l'intention comportementale d'un client en intégrant la notification, l'accès, le choix,

et les dimensions de sécurité dans la conception du site Web d'e-Commerce .

3.6 Conclusion

La construction de la confiance est aujourd'hui un élément important du succès d'une entreprise en ligne. Il est donc primordial que les responsables des sites pensent à inclure des éléments susceptibles d'éveiller un sentiment de confiance envers leur site. Un grand nombre de clients utilisant Internet ont des préoccupations profondes à propos de la confiance, et son gain reste l'obstacle primaire à l'augmentation des transactions et des chiffres d'affaires, et par conséquent, à la croissance continue du e-Commerce.

Sans un minimum de confiance, les transactions ne sont guère possibles. En effet, c'est la confiance qui autorise les échanges. Dans le contexte d'Internet, la confiance est cruciale. Elle 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.

4

Approche par hybridation : Modéle pour la confiance dans le commerce électronique « AHMCCE »

4.1 Introduction

En faisant des achats en ligne, les consommateurs recherchent l'information sur les risques, les avantages et les pèsent les uns contre les autres pour prendre une décision. Les consommateurs ont habituellement un certain nombre de questions sur l'expédition, le service de paiement et les politiques de garanties (retour de produit). Dans ce chapitre nous proposons une solution à ces problèmes.

Notre approche est basée essentiellement sur deux études à savoir les travaux effectués par Meziane et Kasiran en l'occurrence l'étude qu'ils ont effectué sur les informations

fournies sur le site web du marchand et deuxièmement sur la norme universelle WebTrust ,nous reprendrons ces deux études en détails dans ce chapitre pour aboutir à notre proposition.

4.2 WebTrust

Comme déjà défini dans le chapitre précédent(section 3.5.4), WebTrust est une norme universelle qui certifie les sites du commerce électronique en se basant sur plusieurs critères, sans être exhaustifs voici quelques un [**37**] :

- Transparence des pratiques commerciales, l'entreprise indique ses pratiques en matière de commerce électronique et effectue ses opérations conformément à celles-ci.
- Intégrité des opérations.
- L'entreprise a mis en place des contrôles efficaces de nature à procurer une assurance raisonnable que les commandes passées par le client par la voie du commerce électronique sont traitées et facturées comme convenu.
- Protection de l'information, essentiellement les données privées des clients.

WebTrust est un label, un cachet qui se trouve sur les sites certifiées, il existe deux sceaux l'un se trouve sur la page web du site, il s'appelle sceau électronique et l'autre c'est le sceau de cértification.

4.2.1 Le sceau électronique WebTrust

Le sceau WebTrust s'affiche sur les pages du site de l'entreprise certifiée. Il garantit que l'entreprise respecte les règles de sincérité, de sécurité et de confidentialité définies par la norme et contrôlées par un certificateur indépendant.

4.2.2 Le sceau de certification WebTrust

Le sceau est reconnu au plan international et confère ainsi à l'entreprise une notoriété au niveau mondial même si elle n'est pas connue dans le pays de l'internaute.

4.2.3 Le processus de certification

La direction de l'entreprise déclare être en conformité avec la norme WebTrust, elle fait une lettre d'affirmation qui pourrait ressembler à la suivante : dans son site Web consacré au commerce électronique (à l'adresse www.abc.com), la société ABC :
déclare dans son site Web consacré au commerce électronique (à l'adresse www.abc.com) , qu'elle :

- Respect les conditions générales de vente qui s'appliquent à ses opérations de commerce électronique.
- Met en place des contrôles efficaces de nature à procurer une assurance que les commandes passées par le client par la voie du commerce électronique ont été traitées et facturées comme convenu et dans de bonnes conditions de sécurité.
- Met en place des contrôles efficaces de nature à procurer une assurance raisonnable que les renseignements personnels du client obtenus dans le cadre d'une opération du commerce électronique sont protégés contre toute utilisation étrangère aux activités de la société ABC.

4.2.4 Obtention du sceau WebTrust

Pour obtenir le sceau de certification WebTrust, l'entreprise doit respecter tous les principes WebTrust, et pour garantir cette conformité l'entreprise doit :

- Faire appel à un expert-comptable ou à un commissaire aux comptes à qui la Compagnie a formellement délivré une licence autorisant la prestation du service WebTrust ;
- Obtenir un rapport sans réserve de cet expert. Ce dernier certifie la validité des affirmations de l'entreprise et leur conformité par rapport aux critères WebTrust.

La gestion technique du sceau est assurée par un tierce certificateur (actuellement VeriSign, leader mondial de la certification électronique). Il est nécessaire que l'entreprise demande et obtienne de VeriSign un certificat numérique WebTrust.

4.2.5 Conservation du sceau

Une fois le sceau obtenu, l'entreprise doit assurer que l'évolution de son site Web ne remet pas en cause sa conformité à la norme WebTrust. Elle doit donc en informer

l'expert, ce dernier met périodiquement à jour sa certification. L'intervalle entre les mises à jour est en fonction de la fréquence des changements importants apportés au site Web. Dans tous les cas, l'intervalle séparant deux examens ne saurait excéder trois mois.

4.3 Information fournie sur les sites Web

Meziane et Kasiran [**36**] ont développé un modèle de confiance basée sur les informations présentées sur le site web du négociant. Par conséquent, les auteurs ont maintenus les variables qui peuvent être vérifiées par d'autres moyens. Le modèle de confiance qu'il ont proposé est récapitulé dans le schéma ci-dessous et décrit dans les prochaines sous-sections[**36**].

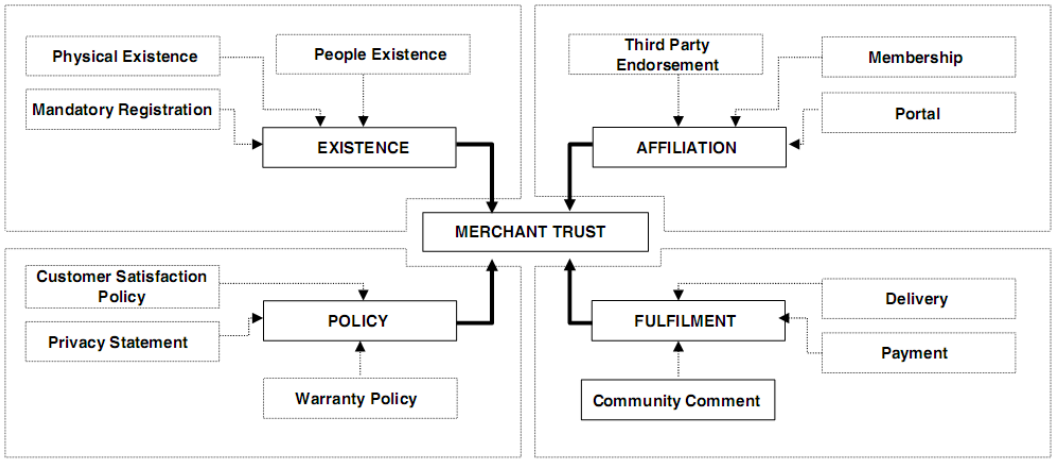

FIGURE 4.1 – *The trust information model.*

4.3.1 La composante d'existence

Dans le commerce électronique le risque est plus grand dû à l'anonymat, la distance et le manque d'interaction physique (Cazier et al [**39**]). Les clients ne peuvent pas dissiper leurs soucis par l'interaction tête à tête avec un marchand ; la présence physique des affaires offre l'assurance qu'elles existent, est accessible et est digne de confiance (Cazier et al [**39**]). Parmi les éléments affectant la crédibilité d'un site Web est l'inclusion de l'adresse physique de l'organisation. Les négociants doivent communiquer qu'officiellement ils existent derrière leurs sites Webs.

Les variables qu'ils ont maintenues pour le modèle d'existence sont : existence physique (E1), existence des personnes (E2) et enregistrement obligatoire (E3). La variable physique

d'existence (E1) est décomposée en adresse (E11), numéro de téléphone (E12) et numéro de fax (E13).

4.3.2 La composante d'affiliation

Du côté du client, un rapport fort de confiance peut être établi avec un marchand par une expérience directe. Cependant, pour les nouveaux clients, la confiance recommandée peut être employée pour établir le rapport initial de confiance (Nöteberg et al [**40**]). Plusieurs méthodes possibles d'affiliation sont employées dans le commerce électronique et les plus populaires sont les : approbation d'une tierce partie, enregistrement d'adhésion. Les influences d'une tierce partie deviendront plus significatives pour les marchands inconnus où le risque perçu est plus haut que les marchands bien connus comme Amazone et eBay. Les variables maintenues pour la composante d'affiliation sont : approbation par une tierce partie (A1), adhésion (A2) .

4.3.3 La composante de politique

La politique en matière de protection de la vie privée en ligne est comprise comme un ensemble de rapports expliquant comment l'intimité des consommateurs est traitée et protégée par le marchand. Les enquêtes indiquent que l'intimité est le souci principal des clients (Cavoukian et al [**41**]).
Les plaintes relatives à la vie privée qui sont déposées à la Commission fédérale des USA incluent des plaintes au sujet d'email non sollicité, de vol d'identité, d'appels téléphoniques harcelants et de la vente des données aux tierce (Mithal [**42**]). Les conditions importantes pour la sécurité du commerce électronique sont la nécessité de protéger les informations sensibles stockées sur des ordinateurs avant et après une transaction. Dans le commerce électronique, les politique telles que l'intimité, la satisfaction du client et la garantie peuvent aider les consommateurs à évaluer la fidélité d'un marchand. Ces politiques peuvent influencer le niveau du risque impliqué dans la transaction. La politique marchande telle que la garantie de remboursement peut aider les clients en les rassurant qu'ils peuvent renvoyer le produit sans perte totale s'ils ne sont pas satisfaits. Les variables maintenues pour les composantes de politique sont : politique de satisfaction du client (P1), rapport d'intimité (Privacy Statement)(P2) et politique de garantie (P3)

4.3.4 Le composant d'accomplissement

Le besoin en ligne des marchands de communiquer leurs capacité d'accomplir leurs fonctions quant aux méthodes de livraison et de paiement. La réputation donne des informations sur le marchands aussi bien sur son comportement dans le passé. Une réputation positive peut créer la base de la confiance et porter une certaine assurance que le marchand exécutera et se comportera de la même manière à l'avenir. Les variables maintenues pour le module d'accomplissement sont : la livraison (F1), paiement (F2) et commentaires de la communauté (F3).

4.4 Proposition

A partir des travaux de Meziane et Kasiran **[36]**, nous avons compris que les marchands devaient mettre à disposition de leurs clients, des informations nécessaires pour augmenter leur confiance.

Par ailleurs, toutes les études concernant la confiance dans le e-Commerce parlent de l'importance de l'approbation d'une tierce partie, ceci nous a amené à nous concentrer sur la façon dont nous pourrions offrir une approbation crédible et objective au client. Nous avons conclu que le concept WebTrust était le mieux placé pour jouer le rôle de cette tierce partie.

Nous avons hybridé le concept WebTrust et le modèle de Meziane et Kasiran pour aboutir à un concept qui utilisera le modèle de Meziane et Kasiran **[36]**, appuié par la vérification de WebTrust. Enfin, mettre tous cela à la disposition du client, ceci augmentera considérablement sa confiance envers un site marchand.

A partir de là, nous avons pensé au module de navigateurs (application ajoutée à un navigateur pour lui apporter de nouvelles fonctionnalités). Ce module fournira les informations nécessaires concernant un site web du commerce électronique.

Ce processus d'hybridation et recapitulé dans le shéma ci-dessous (Figure 4.2).

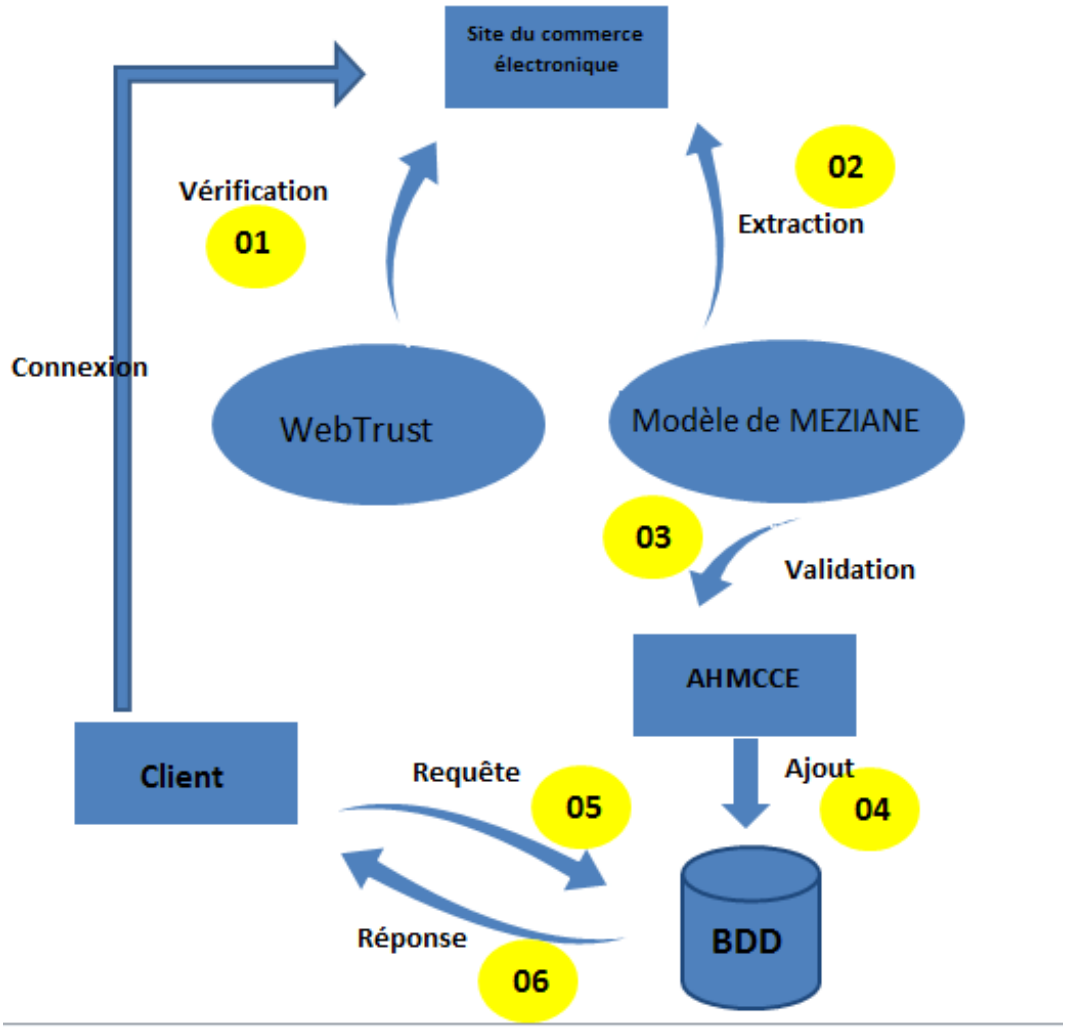

FIGURE 4.2 – *Processus d'hybridation AHMCCE.*

Déscription du processus d'hybridation AHMCCE

(01) Vérification : le site du commerce électronique sera vérifié par rapport à la norme universelle WebTrust.

(02) Extraction : Si les critères WebTrust sont respectés, le site sera approuvé et la procédure d'extraction d'informations sera effectuer, sinon une recommandation sera envoyé à l'entreprise.

(03) AHMCCE : Une fois le site vérifier par rapport à la norme universelle WebTrust et les informations sont extraites du site alors le processus d'hybridation(AHMCCE) est achevé. Et le site sera ajouté à la base de données **(04)**.

(05) Exécution : A la connexion d' un client à un site du commerce électronique, il pourra lancer le module pour une vérification (envoie d'une requête à la BDD).

(06) Renvoi de l'information : à la réception de la requête du client, un ensemble d'informations lui seront renvoyé.

Algorithme AHMCCE

Algorithm 1 Algorithme AHMCCE

// S : site d'une entreprise du commerce électronique
// BDD :Base de donnée
// Info : Information de la base de données
Début :
1. Si (WebTrust(S)= Vrai) alors
2. Hybrid (S) ;
3. Extraction(Info,S) ;
4. Ajout(S, BDD) ;//
5. Sinon
6. Recommander(S) ;//si les critéres WebTrust ne sont pas vérifiés alors //recommander l'adoption de ces critéres au site.

Fin.

Algorithm 2 Fonction WebTrust

Fonction WebTrust(S)
// D : Demande
// C : Critére WebTrust
// E : Expert Comptable
// R : Rapport
Debut :
1. Réception(D) ; //Réception de la demande du site qui veut intégrer le processus.
2. Envoi(C) ; //Envoi des critères WebTrust au site.
3. Engage(E) ; //L'entreprise engage un expert pour la vérification du site.
4. Remplir(R) ;//L'expert remplie un rapport detaillé sur le site.
5. EnvoiR() ; //envoi du rapport par l'expert à la commission WebTrust
6. Vérifier(S) ; // Vérification du rapport et validation s'il y as lieu

Fin ;

4.4.1 Fonctionnement du module

Le rôle de notre module est de fournir aux clients les informations concernant un site web donné en se connectant à une base de données pour récupérer les informations le concernant. Cette base de données sera géré en utilisant notre modéle d'hybridation . Lorsqu'un client se connecte à un site du commerce électronique, avec un simple clique sur le bouton qui se trouve en haut de page, il activera par l'occasion une fenêtre pop up qui lui donnera tous les renseignement concernant ce site même. A savoir : Localisation du site, sa date de création, son PDG, son adresse physique, téléphone, fax,

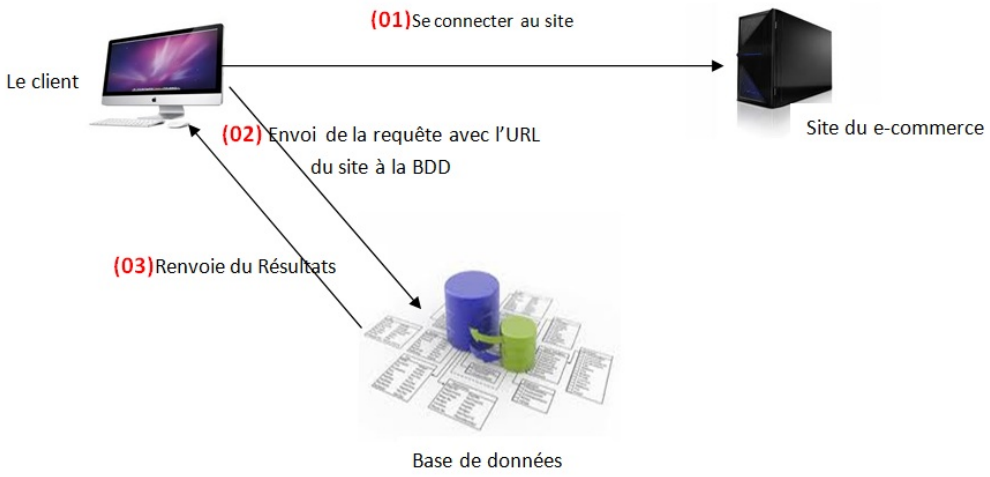

FIGURE 4.3 – *Fonctionnement du module.*

4.5 Implimentation

Pour implimenter notre extention nous avous utilisé trois langages XUL, AJAX et PHP.

4.5.1 XUL :

(XML-based User interface Language) est un langage basé sur XML pour décrire une interface graphique, utilisé dans Firefox et les autres logiciels Mozilla. Il possède ainsi toute une série de balises correspondantes à des boutons, des listes, des menus, des arborescences (treeviews), zones d'éditions etc. Tout pour faire une véritable interface utilisateur.

4.5.2 Php :

(Hypertext Preprocessor) est un langage de scripts libre[principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale.

4.5.3 Ajax :

(Asynchronous Javascript and XML) est une manière de construire des applications Web et des sites web dynamiques basés sur diverses technologies Web. Ils permet notamment de realiser certain contrôle de javascript et de passer des variables via l'URL avec les deux methodes post et get et aussi grâce à la classe xmlhttprequest que nous avons essentiellement utilisée .

Quelques prise d'ecran

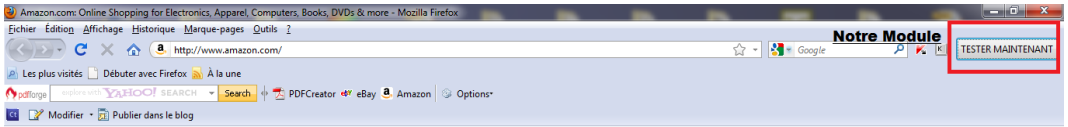

FIGURE 4.4 – *Emplacement du module dans le navigateur.*

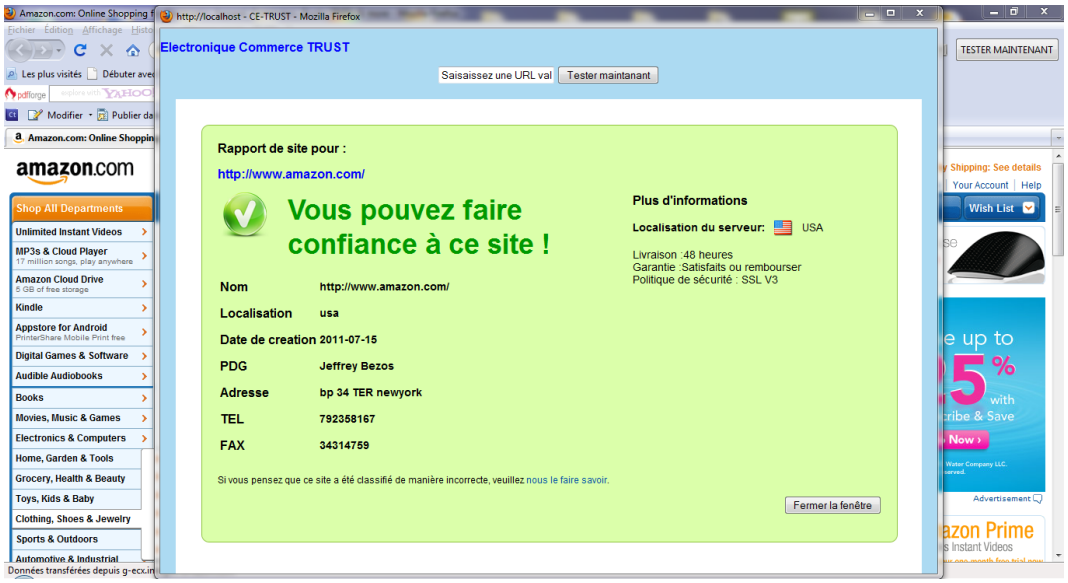

FIGURE 4.5 – *Exemple d'un site approuvé.*

FIGURE 4.6 – *Exemple d'un site non certifié.*

4.6 Conclusion

Par la fusion des travaux de Meziane et de la norme universelle WebTrust, nous avons pu proposer un modèle, qui répond aux soucis de confiance des clients. Ces problèmes atténués par les informations qui parviennent à l'utilisateur accompagnées de l'approbation et de la recommandation d'une tierce partie. De ce fait, les clients plus confiants pourront effectuer plus de transaction et ainsi permettrons au commerce électronique de continuer sur le même élan. En outre, le module que nous avons développé offre une multitude d'avantages, citons : la rapidité, la simplicité, et le gain de temps pour le client.

Conclusion Générale & Perspectives

Nous avons abordé dans notre travail le concept de la confiance dans le commerce électronique, ce dernier qui connaît une hausse phénoménale et qui prend une place, de plus en plus importante dans le quotidien des utilisateurs et dans l'environnement mobile. Malgré l'importance de la sécurité dans le e-Commerce, la notion de confiance demeure un facteur déterminant dans les choix des clients.

Par ailleurs, seule ! la sécurité n'est pas un argument de vente. L'essentiel des efforts sera de réussir à se faire connaître, à susciter la confiance des consommateurs et à faire en sorte que cela se sache auprès des autres consommateurs potentiels.

L'état de l'art de quelques travaux existants que nous avons effectué nous a permis de mieux cerner le sujet et d'aboutir à une proposition basée essentiellement sur deux travaux. Par une approche par hybridation nous avons essayé de fusionner ces deux travaux et implémenté un module dans le but de mettre des informations à la disposition des clients.

Cependant le modéle que nous avons proposé demeure un chantier ouvert à d'éventuels perfectionnements, à savoir :

1. Implémentation des algorithmes proposés.
2. La mise en œuvre et évaluation des essaies pratique.
3. Comparaison avec d'autres modéles.
4. Développer un module de collecte d'informations...

et nous envisageant d'écrire un article dans l'espérance qu'il sera accepté et publié.

Bibliographie

[1] Francis LORENTZ. Commerce électronique : une nouvelle donne pour les consommateurs,les entreprise,les citoyens et les pouvoirs publics. *direction régionale de l'Insee, Midi-Pyrénées.* http://www.insee.fr/fr/themes/document.asp?ref_id=ip771.

[2] http://www.fevad.com/espace-presse/bilan-e-commerce-au-1er-trimestre-2011. Mars 2011.

[3] http://mtv56-service-conseil-formation.agence-presse.net/2010/05/12/fevad-e-commerce-au-1er-trimestre-2010/. Mars 2011.

[4] http://www.e-commerces.eu/e-commerce-les-debuts.html Mars 2011.

[5] www.awt.be. Fiche de l'awt qu'est-ce que l'e-business ? Avril 2000.

[6] Web interface management encyclopedie en ligne. http://esens.unige.ch/lexique.php Mars 2011.

[7] http://www.buzzinessman.com/pourquoivendre-en-ligne/2007/02/21/ Mars 2011.

[8] http://www.ads-com.fr/Rub_330/Solutions-internet/e-commerce.html Mars 2011.

[9] http://www.x2i.fr/magentoecommerce/petite-histoire-du-ecommerce Mars 2011.

[10] Isaac H. *E commerce : De la stratégie à la mise en oeuvre opérationnelle 1ere édition, Pearson Education, Paris.* 2008.

[11] http://www.oeconomia.net/private/cours/economieentreprise/themes/ecommerce.pdf Avril 2011.

[12] Institut national de la statistique et des etudes economies. `http://www.insee.fr/fr/themes/document.asp?ref_id=ip771` Avril 2011.

[13] `http://www.oeconomia.net/private/cours/economieentreprise/themes/ecommerce.pdf` Avril 2011.

[14] Alexandre Guimond. La notion de confiance et le droit du commerce électronique. *Lex Electronica,*, 2008.

[15] FEVAD fédération e-commerce et vente à distance. *Chiffres clés vente à distance e-commerce*. Mai 2010.

[16] Infoéconomie Observatoireéconomique. *Le e-commerce en France*. Juillet 2010.

[17] Antonin CHAZALET. Solution de paiement électronique. `http://membresliglab.mag.fr/donsez/ujf/easrr0405/epayment/epayment.pdf` Avril 2011.

[18] Club de la sécurité des systémes d'information Français. Les dossiers techniques "gérer la sécurité d'un site de commerce électronique". *Commission Réseaux et Systèmes Ouverts*.

[19] `http://securite.developpez.com/faq/?page=dispo` Avril 2011.

[20] Ahmed Mehaoua. Support de cours sur la cryptographie et service de sécurité. `http://www.math-info.univparis5.fr/~mea/cours/Mi/crypto_synthese.pdf` Mai 2011.

[21] Jamil HEBALI. la création de la confiance sur internet : une proposition de cadre conceptual. *HEC Genéve*, juin 2004.

[22] Deutsch MORTON. The effect pf motivational orientation upon trust and suspicion. *journal of Conflict Resolution,*, juin.

[23] Norman L D. Harrison McKnight and Chervany Carlson. Conceptualizing trust :a typology and e-commerce customer relationships model. *Proceedings of the 34th Hawaii International Conference on System Sciences*, 2001.

[24] Arnaud Belleil and Daniel Kaplan. Confiance et sécurité sur les réseaux. *Document de synthèse 12*, octobre 2004.

[25] Robert D. Putnam. Tuning in, tuning out : The strange disappearance of social capital in america. *Political Science and Politics,Harvard University*, Decembre.

[26] J. S. Coleman. Social capital in the creation of human capital. *American Journal of Sociology*, Decembre.

[27] J.B Rotter. Generalized expectancies for interpersonal trust. *American psychologist*, Decembre.

[28] Hyunchul Ahn HyoungYong Lee and Ingoo Han. analysis of trust in the e-commerce adoption. *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

[29] Pierre-Hugues Vallée and Ejan Mackaay. La confiance sa nature et son rôle dans le commerce électronique. *Lex Electronica vol. 11 n° 2*, 2006.

[30] Fukuyama Francis. Trust. the social virtues and the creation of prosperity. *Free Press Paperbacks*, 1996.

[31] Luhmann Niklas. Trust and power. *Toronto, John Wiley and Sons*, 1979.

[32] Pagden Anthony. The destruction of trust and its economic consequences in the case of eighteenth-century naples. *New York, Basil Blackwell*, 1988.

[33] Inès CHOUK and Jean PERRIEN. Déterminants de la confiance du consommateur vis-à-vis d'un marchand internet non familier :une approche par le rôle des tiers. *Cahier n°357*, Avril 2006.

[34] Janine S. Hiller France Belanger and Wanda J. Smith. Trustworthiness in electronic commerce : the role of privacy, security, and site attributes. *Journal of Strategic Information Systems 245-270*, Novembre 2002.

[35] Farid Meziane and Samia Nefti. Evaluating e-commerce trust using fuzzy logic. *International Journal of Intelligent Information Technologie 25-39*, December 2007.

[36] F Meziane and MK Kasiran. Evaluating trust in electronic commerce : study based on the information provided on merchants'websites. *Journal of the Operational Research Society*, December 2007.

[37] ICCA AICPA. Programme webtrust sm/md pour les autorités de certification aicpa-icca. Aout 2001.

[38] June Lub Chang Liua, Jack T. Marchewkaa and Chun-Sheng Yub. Beyond concern : a privacy-trust-behavioral intention model of electronic commerce. *Science Direct Information and Management 127-142*, March 2004.

[39] Shao BBM Cazier JA and Louis RD St. E-business differentiation through value-based trust. *journal of Information and Management*.

[40] Christiaanse E Nöteberg A and Wallage P. The role of trust and assurance service in electronic channels : an exploratory study. in : De p and degross ji (eds). proceedings of the information industry outlook conference, north carolina. *North Carolina. Association of Information Systems : Atlanta, GA, USA*.

[41] Cavoukian A and Crompton M. Web seals : a review of online privacy programs. `http://www.ipc.on.ca/english/pubpres/papers/seals.pdf`.

[42] Mithal M. Illustrating b2c complaints in the online environment. the joint conference of the oecd, hcopil, icc : Building trust in the online environment. `http://www1.oecd.org/dsti/sti/it/secur/act/onlinetrust/presentations.htm`.