MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDELHAMID IBN BADIS MOSTAGANEM

Département d'Informatique

MEMOIRE DE FIN D'ETUDES
Pour l'Obtention du Diplôme de Master en Informatique
Option : Ingénierie des Systèmes d'Information

Thème

Développement d'une application de e-commerce sécurisée Etude de cas : Système Groupe Metidji

Nom et prénom d'étudiante:

- **Missoum Rabia**

Nom et prénom de l'encadreur :

- **CHEHIDA Salim**

Deuxième Année Master Ingénierie des Systèmes d'Information

Année Universitaire 2012/ 2013

Résumé

La vie économique est aujourd'hui liée à Internet, où l'organisation économique qui se met en place sur la toile (le "*World Wide Web*"), loin de constituer une anomalie, préfigure au contraire l'économie de demain, qui sera de plus en plus une économie des biens informationnels. **[1]**

L'internet commercial est un business en pleine croissante qui peut devenir un levier majeur de la vie économique, tel que nombreux des entreprises actives en ligne se rendent fort bien compte qu'il leur reste encore une grande marge de manœuvre afin de devenir plus professionnelles, plus interactives et d'être plus à l'écoute des besoins de leurs clients pour sorte d'atteindre des potentiels croissante.

Afin de prolonger un tel service d'aide à l'achat par une comparaison plus qualitative des conditions de l'offre et de constituer de bases de données de client fidèles et régulières par la diffusion des sites proposés sur l'internet.

Ce travail présente une étude de cas du système de **E-commerce sécurisé** (un site web sécurisé pour la société de ***Groupe Metidji***) qui facilite le contact avec les clients et la vente sécurisée de ces produits en évitant les attaques et les personnes malveillantes comme (*Deni of Service*, *Verus, Vers*,…). En effet, cette étude contient toutes les phases de développement en utilisant des méthodologies de *UML, AuthUML, UMLSec*, et des technologies telle que : JSP/Servlet *java (NetBeans), et MySQL* pour la base de donnée.

Sommaire

Chapitre 2 : La conception du système E-commerce METIDJI

Chapitre 3 : Implémentation système E-commerce de METIDJI

Liste de figures

Liste des Tableaux

Introduction générale

Internet est un moyen très important de la communication surtout dans le domaine du E-commerce qui permet aux entreprises de faire la publication de leurs produits ainsi que la vente de ces derniers.

Les moteurs de recherche permettent en effet un accès facile et rapide aux sites web et aux sources d'information. De nombreuses activités, comme la communication, la consultation des médias, les ventes ou les achats des biens et services, peuvent être effectuées en ligne. On pourra dire qu'il n'y a plus de frontières entre les pays dans le domaine du E-commerce **[2]**.

E-commerce est une nouvelle pratique de l'utilisation d'un média électronique pour la réalisation de transactions commerciales et l'établissement de relations virtuelles entre les acheteurs et les vendeurs. Dans la plupart du temps il s'agit de la vente de produits. Il englobe aussi les mécanismes d'achat à travers le réseau internet à partir des différents types de terminaux (ordinateurs, tablettes, Smartphones, consoles, TV connectées) **[3]**.

L'ouverture des systèmes d'information vers l'extérieur engendre des gains de productivité et de compétitivité mais elle expose aussi de plus en plus les systèmes aux actes de malveillance. Les solutions à posteriori de la sécurité comme (firewall, antivirus,…) peuvent donner des résultats mais elles restent toujours insuffisantes pour répondre à l'évolution exponentielle des attaques et risques.

La nouvelle approche à priori de la sécurité consiste à intégrer la sécurité au niveau du cycle de développement en tenant compte des différentes exigences de sécurité (disponibilité, authentification, intégrité, confidentialité, non-Répudiation,...) au niveau de la spécification, de la conception et de l'implémentation. Parmi les méthodes proposées dans ce contexte, il y a l'approche *AuthUML* (*K. Alghathbar, D. Wijesekera*) qui permet d'analyser les besoins de contrôle d'accès dans la phase de spécification des exigences du cycle de vie afin d'éviter les conflits et protéger la cohérence d'autorisation entre les accès aux SI. Cette approche est basée sur le langage UML pour la modélisation formelle et le développement des exigences de la sécurité, et une version personnelle de ***FAF*** (Framework d'Autorisation Flexible) **[4]** pour spécifier ces exigences, et aussi le principe de séparation des taches *SoD* **(***Separation of Duty)* pour valider la conformité des exigences des autorisations **[5]**.

Après la phase de conception vient la phase de développement. Le coté sécurité sera traité au niveau de cette dernière phase, c'est la partie la plus importante de notre application. La technologie *JSF (Java Server Face)* a été choisie comme technologie de développement car elle propose un Framework puissant en termes de sécurité et de performance. Nous utiliserons le NetBeans comme support de développement du langage *JAVA*, le *SGBD* **MySQL** pour la gestion de notre base de données et *Glass Fish* comme serveur d'application web.

Notre travail consiste à réaliser un système E-commerce pour l'entreprise de production du Groupe Metidji. Cette entreprise importe de la matière première, la transforme et la vends sous forme de produits finis.

Notre mémoire est organisé autour de trois chapitres.

Dans le premier chapitre nous présentons une introduction au commerce électronique et la sécurité du système d'information.

Dans le deuxième chapitre nous avons développé la conception du système E-commerce pour l'entreprise Metidji.

Dans le troisième chapitre nous aborderons la partie implémentation du système qui représente la phase d'intégration, de codage et de test de notre démarche de développement.

Enfin, nous avons finalisé cette étude par une conclusion générale qui récapitule notre travail, suivie d'une perspective qui propose la continuité de notre projet.

1. Introduction

E-Commerce est la capacité d'une entreprise d'avoir une présence dynamique sur l'Internet qui lui permet de mener ses affaires par voie électronique. On peut dire que l'entreprise possède une boutique électronique. Les produits peuvent être annoncés, vendus et payés pour tous par voie électronique sans la présence de l'acheteur ou du vendeur.

2. Définition de E-Commerce

Le commerce électronique (e-commerce) est un aspect de la communauté des affaires qui utilise les technologies EFT[1] et EDI[2]. C'est officiellement l'utilisation de transactions numériques entre et au sein des entreprises et des particuliers. C'est l'ensemble d'opérations commerciales effectuées par des personnes et des organisations, sans document papier, à l'aide d'ordinateurs et de réseaux de télécommunications privés ou publics ; leur objectif est de faciliter le financement et les aspects de paiement des transactions commerciales. **[6]**

3. Avantages et Limites du E-commerce

E-commerce offre de nombreuses nouvelles façons pour les entreprises et les consommateurs pour communiquer et faire des affaires. Il y a un certain nombre d'avantages et limites de la conduite des affaires de cette façon.

a) Avantages

Un site e-commerce offre de nombreux avantages à la plupart des entreprises de tous types et tailles. Les principaux avantages sont: **[7]**

❖ ***Pour le Vendeur***

- Augmentation des opportunités de ventes en identifiant de nouveaux fournisseurs et partenaires commerciaux.
- Les entreprises peuvent obtenir de meilleurs prix pour les biens et services en acceptant des offres concurrentielles.

[1] *Transfert électronique de fonds s (EFT) :* sont la transmission électronique des informations sur le compte de réseaux de communications privées.

[2] *Échange de données informatisé (EDI) :* se produit quand une entreprise transmet les données lisibles par ordinateur dans un format standard à une autre entreprise.

- Réduit les coûts en réalisant des processus d'affaires en ligne comme les enquêtes sur les ventes, les prix, la prise de commande et le suivi de l'inventaire.

❖ **Pour l'Acheteur**

- Augmente les possibilités d'achat en offrant un large éventail de choix que celui offert par le commerce traditionnel car les acheteurs peuvent envisager de nombreux produits et services différents de nombreux vendeurs différents.
- Différents niveaux d'information sur les produits et les services sont disponibles à tout moment.
- Les produits numériques comme les logiciels, la vidéo, la musique ou les images peuvent être téléchargées immédiatement par Internet réduisant ainsi les coûts et le temps passé à attendre ces produits achetés.
- Faciliter le paiement des factures ainsi que leur suivi.
- Fournir des produits et services disponibles dans les régions éloignées.

b) Limites

Malgré les avantages du E-Commerce, Il y a certaines limites dans le choix de la norme de sécurité, à savoir : **[8]**

❖ ***Pour le vendeur***

- Les entreprises qui ont adopté ce mode de commerce 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 l'acheteur***

- 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 règles d'appel et de consommation.
- L'insécurité des paiements et la peur de tomber sur un cybermarchand malhonnête qui ne livre pas la marchandise commandée et payée.
- Le manque de contact avec le produit.
- Les difficultés de recours en cas d'ennuis.

4. Moyens de Paiement en Ligne

Internet offre un large choix de moyens de paiement ayant tous des caractéristiques différentes concernant la sécurité des transactions, la popularité et le coût de revient.

4.1. Paiement Par Carte Bancaire

L'acheteur utilise sa carte bancaire classique pour payer. Il faut bien sûr vérifier que le site d'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. **[9]**

4.2. Paiement par e-numéro de carte

C'est un moyen de paiement rattaché à la carte bancaire qui permet de payer sans donner un numéro de carte bancaire. Des e-numéros sont attribués des numéros de carte bancaire temporaires. On peut citer les cartes bancaires virtuelles à titre d'exemple ; Cette méthode de paiement se définit davantage comme un service qui peut s'adjoindre à votre portefeuille électronique, à votre carte ou à votre compte bancaire. Ce service repose sur le principe de base suivant : il permet d'avoir un numéro de carte bancaire internationale (Visa ou Mastercard) différent pour chaque achat que vous effectuez. **[9]**

4.3. Paiement sans carte bancaire

C'est un moyen très utilisé qui permet d'éviter les problèmes de violation. C'est un moyen simplifié qui n'utilise pas la carte bancaire. Parmi les méthodes de paiement sans carte, on peut en citer les suivantes : **[10]**

- **Virement bancaire:** C'est un moyen de paiement idéal vu qu'il passe par une banque. Le système bancaire est un système très sécurisé, mais ce mode de paiement présente un coût de revient élevé.
- **Chèque:** Le chèque est le moyen de paiement le moins utilisé en e-commerce car il nécessite une activité physique complètement indépendante du site internet. Même si le coût est moindre, voir négligeable, il reste très peu utilisé**.**

5. Sécurité d'E-Commerce

La sécurité des systèmes d'information *(SSI)* est un ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système informatique**.** La sécurité du commerce électronique consiste en la sécurité de logiciels, en l'achat de Certificat de *SSL (Secure Socket Layer)* et en une certaine configuration du serveur.

5.1. Service de Sécurité

La sécurité informatique consiste à garantir les ressources matérielles ou logicielles par plusieurs types d'enjeux en prenant en compte différents critères **[11] :**

- ***L'intégrité*** : est le moyen de s'assurer que le message que l'on reçoit est bien celui qui a été envoyé et qu'il n'a donc pas été altéré de façon fortuite ou volontaire.
- ***La confidentialité***: Seule les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché. Il faut qu'aucun intrus ne vienne violer l'intégrité des informations transmises.
- ***La disponibilité*** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
- ***La non-répudiation et l'imputation*** : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur, pour garantir que le contrat de départ n'a pas été modifié et accepté par chacune des parties.
- ***L'authentification*** : L'authentification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

5.2. Politique de la sécurité

La politique de sécurité d'un système d'information consiste à mettre en place un ensemble de procédures et d'opérations suivies par l'entreprise pour déterminer les mesures de sécurité à appliquer et à gérer. Ceci consiste à : **[12]**

- Connaitre tous les besoins de l'entreprise en matière de sécurité et évaluer les risques.
- Proposer à tous les départements des outils, des processus et des règles en ligne avec les risques considérés primordiaux pour l'entreprise.

- détecter les vulnérabilités de réseaux et combler les éventuelles failles sur les applications ou sur le système d'exploitation et le matériel utilisés**.**
- élaborer une série de procédures et d'actions à mener en cas de dangers (vulnérabilité ou menaces d'attaques informatiques par exemple)

La procédure qui spécifie la politique de la sécurité est la suivante :

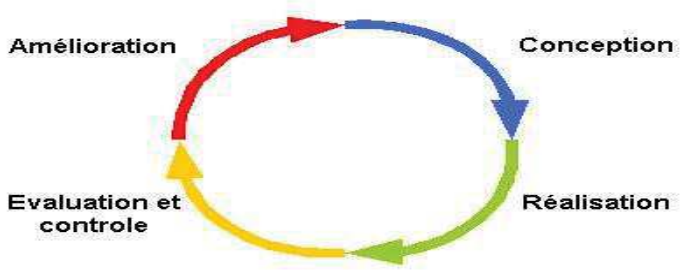

Fig1. Procédure spécifique de la politique de sécurité **[12]**

- *Conception* **:** Cette première étape permet d'identifier et d'évaluer les risques afin de développer un plan de gestion et de définir le périmètre et le contexte du futur système.
- *Réalisation :* consiste à appliquer la politique de la sécurité créée à l'étape de conception. Les organisations et les techniques sont appliquées par les personnes.
- *Evaluation et Contrôle :* s'assurer que les procédures mises en place fonctionnent comme prévu.
- *Amélioration :* améliorer les outils de protection comme l'achat d'un outil ***anti virus.***

5.3. Bases de sécurité des applications web

Une application Web se contente de présenter des interfaces utilisateurs simples, en format HTML, générées entièrement côté serveur et d'utiliser des outils tels que des bases de données, JavaScript et PHP (ou ASP.Net) pour offrir des expériences au-delà de la page Web standard ou formulaire web **[13].**

Les attaques s'appuient généralement sur l'injection *SQL* de fautes pour exploiter les vulnérabilités de la syntaxe et de la sémantique d'une application Web ou pirater un exploit particulier en modifiant automatiquement un lien *URI* (Uniform Resource Indicator). Les vulnérabilités de sécurité au sein des applications Web sont liées à des erreurs de programmation avec un langage de programmation d'applications Web (par

exemple Java, .NET, PHP, Python, Perl et Ruby), à une bibliothèque de codes, à un trait de conception ou à l'architecture **[14].**

5.4. Vulnérabilités des applications web

Les applications Web peuvent comporter chacune des vulnérabilités. Les six catégories publiées par le consortium WASC (Web Application Security Consortium) sont : **[14]**

- *Authentification* : c'est le vol des identités de compte utilisateur comme : faiblesse de la validation de restauration du mot de passe (piratage ou modification du mot de passe), attaque par authentification insuffisante (piratage pour accéder au contenu)
- *Autorisation :* accès illégal à des applications comme : la prédiction de certificat/session, attaque par autorisation insuffisante, ou par expiration de session insuffisante.
- *Attaques côté client :* exécution illégale de code étranger comme : usurpation de contenu (Spoofing), script intensité (Cross-site Scripting - XSS)
- *Exécution de commandes :* prise de contrôle d'une application Web comme : attaques par débordement de la mémoire tampon (Buffer Overflow), prise de contrôle à distance du système d'exploitation, Injection (Code *SQL, SSI (*Server-Side Include), *XPath)*
- *Divulgation d'informations :* affichage des données sensibles pour les pirates.

5.5. Techniques de Sécurité de Paiement

La sécurité informatique consiste à la protection contre plusieurs attaques qui proviennent d'une exploitation frauduleuse de l'environnement internet (les applications Web). Parmi ces techniques il existe :

5.5.1. Chiffrement (Cryptage)

On utilise la Cryptographie pour le *chiffrement et le déchiffrement.* Cette technique a été utilise dans notre application pour assurer les exigences de sécurité : Confidentialité et intégrité des informations critiques comme le mot de passe qui apparait en crypté dans la base de données.

5.5.1.1. Types de Chiffrement

On distingue trois types : **[15]**

➢ **Chiffrement Symétrique**

C'est une Cryptographie de « Clé Secrète ». Cette clé ne doit être connue que des personnes censées avoir le droit de chiffrer / déchiffrer le message. Le chiffrement secret est un procédé de chiffrement "symétrique" si les clés de chiffrement et de déchiffrement sont similaires. Il utilise plusieurs algorithmes (*DES*, *IDEA, TDES…)*.

Fig2. Principe de Cryptographie Symétrique

➢ **Chiffrement Asymétrique**

C'est une Cryptographie de « Clé Publique» qui utilise l'algorithme de *RSA (Rivest Shanir Adlemen)*, si une personne souhaite que ses correspondants lui envoient des messages chiffrés, il doit utiliser deux clés différentes qui sont : la clé de chiffrement et de déchiffrement qui devra alors générer 2 clés :

- *Une première clé (Clé Publique)* 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 (Clé Secrète),* servant quant à elle au déchiffrement, et qui devra rester privée, afin que seule la personne émettrice des clés puisse déchiffrer les messages.

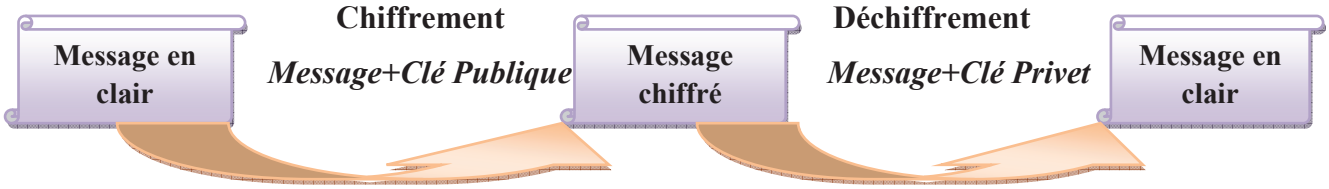

Fig3. Principe de Cryptographie Asymétrique

- **Chiffrement Hybride**

Le Chiffrement hybride est une méthode de chiffrement qui combine deux ou plusieurs systèmes de chiffrement et inclut habituellement une combinaison de chiffrement symétrique et asymétrique (clé publique) pour tirer parti des points forts de chaque type de cryptage.

Les données sont cryptées au moyen du cryptage symétrique. Cependant, une clé de session unique est générée pour chaque transfert de données ou de fichiers, respectivement, et est transmise aux partenaires de la communication par cryptage asymétrique ou jointe au message approprié. Ces touches ne constituent qu'un très faible volume de données.

5.5.2. Signature Numérique

La signature numérique est une Clé Publique qui fournit un mécanisme permettant d'authentifier les messages, cette technique utilise à clé secrète pour chiffrement, où l'expéditeur d'un message remplit un calcul (opération effectuée par la fonction de Hachage) impliquant la structure réelle du fichier à transmettre et utilise clé secrète, et le résultat de ce (signature numérique de lui même) est ajouter à la fin de transmission, Le récepteur peut alors effectuer un calcul de message reçut et utilise la clé publique de l'expéditeur pour déchiffrement, et si tout est valide, l'identité de l'expéditeur aura été vérifiée. **[16]**

Les avantages de la signature numérique sont :

- Vérification de l'identification de l'expéditeur ainsi que du contenu original de la transmission.
- Permet d'authentifier l'auteur d'un document.
- Permet de donner une valeur juridique (sous certaines conditions) au document.

5.5.3. Infrastructure à clés publiques (PKI)

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, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (systèmes et applications) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques. **[17]**

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

- Enregistrement des utilisateurs (ou équipement informatique).
- 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).

5.5.4. 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 notée **CA**

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). Il existe trois catégories de certificats d'authentification : **[18]**

- **Certificat Client :** il est stocké sur le poste de travail de l'utilisateur. Il permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur.
- **Certificat Serveur :** Installé sur un serveur web, il permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir l'URL et en particulier le domaine de la page. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole SSL
- **Certificat VPN**

VPN (*Virtual Private Network*) consiste en la fabrication d'un tunnel[3] logique qui sera contracté par les communications de l'entreprise. Installé dans les équipements

[3] Tunnel : est un moyen de transférer des données entre deux réseaux similaires sur un réseau intermédiaire.

réseaux, il permet de chiffrer les flux de communication de bout en bout entre deux points, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat IP Sec ou PPTP *(Point-to-Point Tunneling Protocol*).

5.5.5. Protocole de Sécurité

5.5.5.1. SSL

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clé 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 ou IMAP et S/HTTP. Un serveur web sécurisé par SSL possède une URL commençant par https://, où le "s" signifie bien évidemment sécurisé. Il a été renommé en 2001 Transport Layer Security (*TLS*). Tel qu'on parle de SSL pour désigner indifféremment SSL ou TLS, Il chiffre les données afin d'empêcher leur lecture par des tiers **[19]**.

5.5.5.2. IP Sec

IP Sec (*Internet Protocol Security*) est une collection de protocoles cryptographiques de sécurisation des réseaux IP, indépendamment des applications et du transport fiable TCP ou du transport UDP. Il se compose de deux protocoles : le premier, AH (*Authentication Header)* offre les services d'authentification et d'intégrité de la totalité du paquet IP et le second ESP (*Encapsulating Security Payload*) offre les services d'authentification, d'intégrité et de confidentialité des données utiles associées au paquet IP et les données du paquet sont signées ou chiffrées selon la politique en vigueur **[20].**

5.5.5.3. HTTP/ HTTPs

S/HTTP "Secure HyperText Transfer Protocol" opère au niveau applicatif et permet d'échanger des messages, des documents ou des pages web de manière sécurisée entre un utilisateur relié à Internet et un serveur web connecté sous le protocole SSL. Il est utilisé

pour toutes les transactions de paiement effectuées par Internet (e-banking, e-commerce, etc.) **[21].**

5.5.6. Firewall/Pare-feu

C'est un dispositif matériel ou logiciel établi en fonction des besoins personnels liés au raccordement des réseaux d'entreprises à Internet pour protection. Il constitue un filtre d'accès entre un réseau local et un réseau non sûr tel que l'internet ou un autre réseau local. Il permet de sécuriser, de détecter, de parer ou d'éviter de nombreuses attaques. Il permet de même de bloquer les connexions et les contenus non désirés. Il existe trois types différents de firewall selon leur fonction : *firewalls routeur, applicatif* et *circuit* **[22].**

5.5.7. Anti Virus

C'est un programme qui présente une solution simple à mettre en place et très efficace pour lutter contre les centaines de milliers de virus. Il surveille si le comportement d'un ordinateur est modifié par la présence d'un virus (analyse la mémoire et les fichiers exécutables) et détecte les nouvelles intrusions. **[23]**

6. Approches à Priori de la Sécurité

L'ouverture des systèmes d'information à l'extérieur expose de plus en plus les systèmes d'information aux actes de malveillance. Les solutions à posteriori de la sécurité des SI (Firewall, Antivirus, etc.) peuvent donner des résultats mais elles ne constituent pas une véritable politique de sécurité. La nouvelle approche à priori de la sécurité consiste à la prise en compte des exigences de sécurité (intégrité, confidentialité, non-répudiation, disponibilité, etc.) au niveau des différentes phases de processus de développement **[24].**

En effet, La sécurité des SI se pratique à tous les niveaux du cycle de vie de ce dernier. On utilise les modèles de contrôle d'accès (*MAC, RBAC, DAC..)* et pour la modélisation formelle nous avons utilisé *UMLSec et AuthUML* (qui sont détaillés au chapitre2). L'objectif est de mettre en place des mécanismes de sécurité appropriés pour détecter, prévenir et lutter contre une attaque de sécurité comme : chiffrement, signature informatique, barrage de trafic.

7. Conclusion

L'E-commerce s'appuie sur la sécurité des applications ou des logiciels ; C'est un thème difficile car il est nécessaire d'ancrer une sécurité des applications protégées. Les solutions de la sécurité des systèmes d'information (Farewell, Anti Virus,….) et les protocoles de sécurité (*SSL, IPSec,….*) utilisés par la cryptographie pour la garantie des services de sécurité (confidentialité, Intégrité,…) contre les attaques sont insuffisantes car ces attaques sont très modulables et bien que la détection fasse d'énormes progrès, elles restent toujours très compliquées à mettre en place de manière efficace. Il ne suffit pas de multiplier les outils de prévention, Il faut aussi voir l'aspect financier de ces attaques et adapter le budget de protection aux risques, car la course contre les pirates ne s'arrêtera jamais.

1. Introduction

Après étude des différentes notions liées au domaine du e-commerce, nous allons développés dans ce chapitre la conception du système e-commerce de la société *« **Groupe Metidji »*** de la wilaya de Mostaganem**.** Cette société est spécialisée dans la production de produits alimentaires comme les snacks (Chili, Fromage,..), les céréales du petit déjeuner (Boules au Chocolat, Pétales au Chocolat,…), les pattes (Langue d'oiseau, Cheveux d'ange,..) et du couscous (Gros, demi Gros, Moyen) et d'autres produits comme les blés de mouture (Farine et Semoule).

Cette étude repose au départ sur les différents modèles de conception des systèmes d'information. Nous avons utilisé la *démarche de conception sécurisée **DCS*** qui est basée sur la méthode *Rational Unified Process (RUP)* issue de la méthode *UP*[1] **[25]**. Cette dernière regroupe les activités à mener pour transformer les besoins d'un utilisateur en système de logiciel basé sur des extensions d'UML afin de modéliser des objets, spécifier tous les aspects, analyser et faire la conception d'un système.

2. Démarche et Outils

2.1. DCS

La démarche ***DCS*** présente quatre phases: **[26]**

- *Expression et spécification des besoins* : étudier les fonctionnalités du système selon les besoins des différents utilisateurs, ainsi que la spécification des exigences de sécurité induites par l'utilisation du système.
- *Analyse et conception :* déterminer les objets et les classes du système à construire, ainsi que leur structure et leurs relations .Chaque objet doit être décrit selon deux axes : axe statique (Structure de l'objet) et axe dynamique (diagramme de séquence)

[1] UP est un processus fournit les lignes directrices pour un développement efficace d'un logiciel de qualité et Réduit les risques et améliore les prévisions, et permet comment implémenter en utilisant les outils standards de développement logiciel « itératif et incrémental, centré sur l'architecture, conduit par les cas d'utilisation et piloté par les risques »

- *Modélisation de la navigation :* utilisée pour modéliser avec précision la navigation dans l'application web, et les conventions propres à la navigation dans le site web.
- *Conception technique :* Cette étape définie une architecture basée sur les techniques…. et une configuration matérielle du système par l'utilisation des diagrammes de composant et de déploiement.

3. Microsoft Office Visio

Microsoft Office Visio est une interface qui permet de modéliser des Systèmes d'information ou tout autre système en UML. Il met à disposition beaucoup d'outils qui permettent de se servir de manière optimale du langage de modélisation UML.

Microsoft Office Visio est un outil complet pour les concepteurs de logiciel. Il permet alors de modéliser les diagrammes de flux, les cas d'utilisation, etc. Il inclut des modèles prédéfinis qui permettent la modélisation, la réalisation et l'utilisation de l'interface utilisateur de Windows (XP, 7,…) pour faciliter la représentation et tracer les diagrammes UML. **[27]**

4. Expression et spécification des besoins

4.1. Recueil initial des besoins

Cette étape constitue la modélisation des aspects du système**.** On effectuera un repérage des besoins fonctionnels et de sécurité en utilisant le texte pour définir le cahier des charges (fonctionnel et de sécurité), et des diagrammes de collaboration pour visualiser le contexte du système.

4.1.1. Cahier de charge

4.1.1.1. Objectifs du Groupe Metidji

Le Groupe Industriel **METIDJI** a été fondé par Monsieur Hocine Mansour METIDJI qui s'est lancé dans les années 1990 dans la région de *Mostaganem* dans le domaine de l'agro-alimentaire du secteur céréalier.

Par la suite, le Groupe METIDJI se renforce encore plus et investit dans le domaine de la technologie de transformation des céréales, en édifiant en 2001, les quatre sociétés suivantes : **[28]**

- Les *Grands Moulins du Dahra* : Minoterie semoulerie, spécialisée dans la production de différentes catégories de farines et semoules à partir de blés hautement sélectionnés.
- *Les Moulins de SIG:* Minoterie semoulerie aux capacités de stockage très importantes.
- Le *Comptoir du Maghreb* : Société d'importation de produits agro-alimentaires.
- L'*Amidonnerie de Maghnia* : Entreprise de transformation du maïs en ses dérivés essentiels, notamment l'amidon, le sirop de glucose, les dextrines et le gluten.

Parmi les objectifs principaux du système du *Groupe Metidji :*

- Développer les produits et saisir les coordonnées des gammes d'articles.
- Assurer la communication et les coordonnées entre l'administrateur et les clients.
- Assurer la promotion des produits et la disponibilité accrue des clients.

4.1.1.2. Besoins fonctionnels

A. Acteurs du Système

Les différents acteurs identifiés sont :

a) ***Client :*** se connecter sur le site, passer les commandes et choisir le mode de paiement (Chèque ou virement bancaire).

b) ***Banque :*** qui valide (ou rejette) les opérations des paiements par confirmation du versement en contrôlant le N° de compte de client.

c) ***Magasinier :*** il gère les commandes (complètes ou partielles), effectue les réapprovisionnements du stock, et achemine les articles commandés au client. Il édite les bons de livraison et les factures et lance le transport avec toutes les coordonnées des chauffeurs.

d) ***Administrateur :*** consulte sans cesse les tableaux récapitulatifs des clients pour saisir le N° compte des clients afin de permettre le payement des commandes valides, fait la mise à jour des articles et définit les promotions.

B. Fonctionnalité :

a) Espace administrateur

Un espace est réservé pour l'administrateur du site. L'administrateur pourra gérer les comptes des clients. Il aura accès à des tableaux récapitulatifs de tous les clients, toutes les commandes et de tous les produits. La gestion comprendra :

- La gestion des comptes client (suppression ou modification de compte). Pour chaque compte client, il sera indiqué toutes les coordonnées du client et les achats qu'il a effectués.
- La gestion d'article (ajout, suppression ou modification des prix) ; chaque article sera détaillé à l'aide de ses coordonnés. Il peut aussi définir des promotions.

b) Espace Client

Le client pourra se connecter sur le site par Pseudo/Mot de passe s'il existe pour commander des produits, sinon il entrera ses coordonnés personnelles pour valider son inscription ; il pourra par la suite consulter le catalogue d'articles et le tableau récapitulatif des commandes validées par le magasinier et payer ses factures.

c) Espace Magasinier

Il pourra gérer le magasin et les commandes de chargements pour les clients ; il aura accès à tous les produits. La gestion comprendra :

- gestion de commande (état de la commande et facturation). Pour chaque commande, il sera indiqué le nom du client, le nom de l'article, le prix total, le numéro de commande, le mode de paiement et l'état (statut) de la commande.

d) Espace Panier

Rappelons que le panier de l'utilisateur contient des articles. Chaque article pouvant rester trente minutes maximum (la durée par défaut) avant de disparaitre. Le client peut incrémenter ou retirer la quantité des produits choisis sur panier (selon la limite de temps), et valider son mode de paiement.

4.1.1.2. Exigences de la sécurité

a) Menace :

Sur Internet, il y a beaucoup de risques qui menacent les systèmes d'informations (*SI).* Parmi ces risques il y a :

- Usurpation d'identité (*Spoofing*) :c'est une technique visant à envoyer des paquets IP avec une fausse adresse qui permet de faiblisse de création de site web et qui ont l'air d'être publié par des organisations légitimes.
- Vol de session (*Hyacking*) : c'est une technique consistant à intercepter une session TCP initiée.
- Ecoute du réseau (*Sniffing*) : c'est un dispositif permettant d'écouter le réseau et de voir les informations qui circulent.

b) Exigences :

Le système doit répondre à certaines exigences :

- Assurer les clients qu'ils sont sur le site « Metidji » et non pas sur un faux site.
- Assurer aux clients que leurs informations personnelles ne sont pas accessibles à des malfaiteurs, lorsqu'ils procèdent à une transaction sur le site.
- Permettre aux clients de payer facilement et d'une manière sécurisée leurs factures en utilisant leurs chèque ou virement.
- Le Système «Metidji » doit permettre aux clients de suivre et de consulter leurs factures et leur paiement en toute sécurité.

Ces exigences permettent de déterminer les principaux objectifs en terme de sécurité pour le système «Metidji» : **[29]**

- **Authentification :** Le système doit assurer l'authentification des Clients. Les clients doivent être en mesure de s'assurer qu'ils sont devant le site «***Groupe Metidji***» et qu'ils envoient leurs informations privées à une entité réelle et non pas à un *spoof* site qui se fait passer pour une banque ou autre.
- **Confidentialité :** les données sensibles pour la communication, doivent être assurées par le système, telles que les informations personnelles des clients, de l'administrateur ou du magasinier.
- **Intégrité de données :** il faut s'assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des parties non autorisés.

- **Non répudiation :** Il ne devrait pas être possible pour un client ou la banque à prétendre raisonnablement qu'il ou qu'elle n'a pas exécuté un paiement.
- **La disponibilité :** assurer au client convenable et non abusif l'accessibilité et éviter toute forme de déni des services et/ou des ressources du système.

4.1.2. Modélisation du contexte

Cette étape consiste à élaborer le modèle de contexte fonctionnel et de sécurité en se basant sur le cahier des charges. Le diagramme de contexte est représenté par des objets reliés au système par des liens ; Chaque lien supporte des messages en sortie du système pour représenter les différents services fonctionnels et de sécurité assurés par le système.

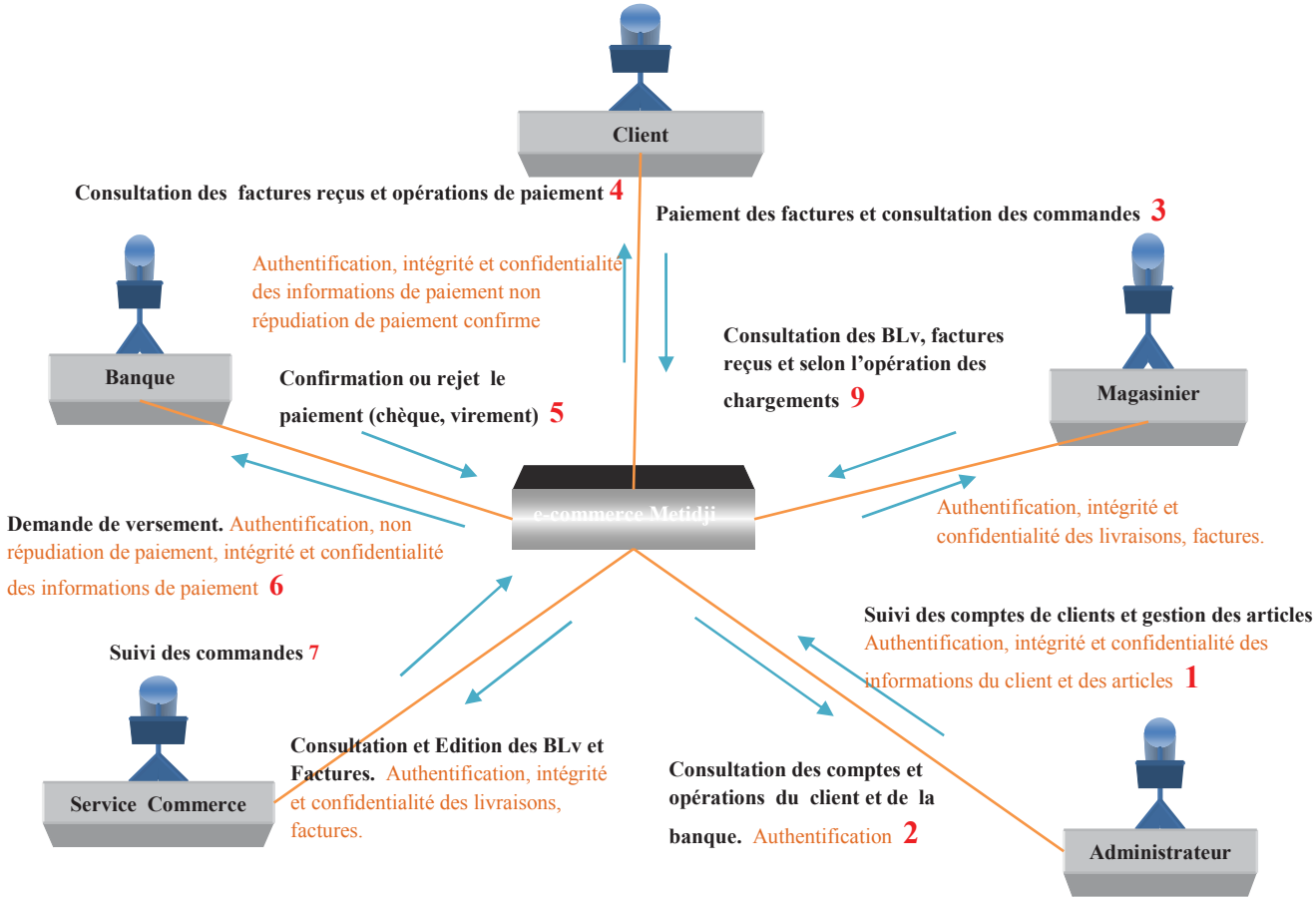

Fig4. Modèle de contexte du système e-commerce Metidji.

4.2. Identification et description des cas d'utilisation et des cas de sécurité

A partir des modèles de contexte établis dans la phase précédente, cette étape consiste à identifier les cas d'utilisation qui représentent un ensemble de séquences d'actions réalisées par le système pour les différents acteurs et aussi les cas de sécurité (*Security case*) représentant un service de sécurité rendu par le système pour un ou plusieurs acteurs ; il permet de spécifier un comportement attendu du système pour répondre à des exigences de sécurité sans imposer le mode de réalisation de ce comportement. **[30]**

4.2.1. Identification

Le tableau suivant présente les cas d'utilisation et leurs acteurs.

Cas d'utilisation	**Acteur**
➢ Créer Compte client ➢ Consulter informations client ➢ Gérer article.	Administrateur
➢ Effectuer paiement ➢ Effectuer commande ➢ Consulter catalogue ➢ Livrer les Commandes	Client
➢ Consulter demande de versement ➢ Confirmer paiement	Banque
➢ Editer BLv et Facture	Service_Commerce

Tableau1. Identification de cas d'utilisation

Le tableau suivant présent les cas de sécurité et leurs acteurs.

Cas de sécurité	**Acteur**
➢Assurer l'authentification	Administrateur, Client, Banque, Magasinier
➢Assurer la disponibilité de système de paiement	Client
➢Assurer la non-répudiation de paiement	Client, Banque
➢Assurer la confidentialité et l'intégrité des informations de paiement.	Client, Banque
➢Assurer la disponibilité de Facture	Client
➢Assurer l'intégrité et la confidentialité de Livraison et Facture	Magasinier

Tableau2. Identification de cas de sécurité

4.2.2. Description des besoins

Dans la description des cas d'utilisation et cas de sécurité, nous avons utilisé plusieurs approches à priori de la sécurité comme *RBAC, UMLSec, AuthUML.*

a) RBAC

RBAC (contrôle d'accès basé sur le rôle) proposé dans **[31]** comporte six concepts de base : utilisateur, rôle, session, autorisation (permission), opération et objet.

❖ **Confirmer Versement :**

Les relations entre ces concepts sont définies comme suit : à la banque on peut activer dans une session un ou plusieurs rôles nécessaires pour exécuter une tâche donnée et peut assigner un ou plusieurs rôles (**confirmer le versement** ou **échec)**. Les autorisations seront assignées aux rôles, et par conséquent la banque peut acquérir une autorisation par le fait de jouer le(les) rôle(s) approprié(s)**.**

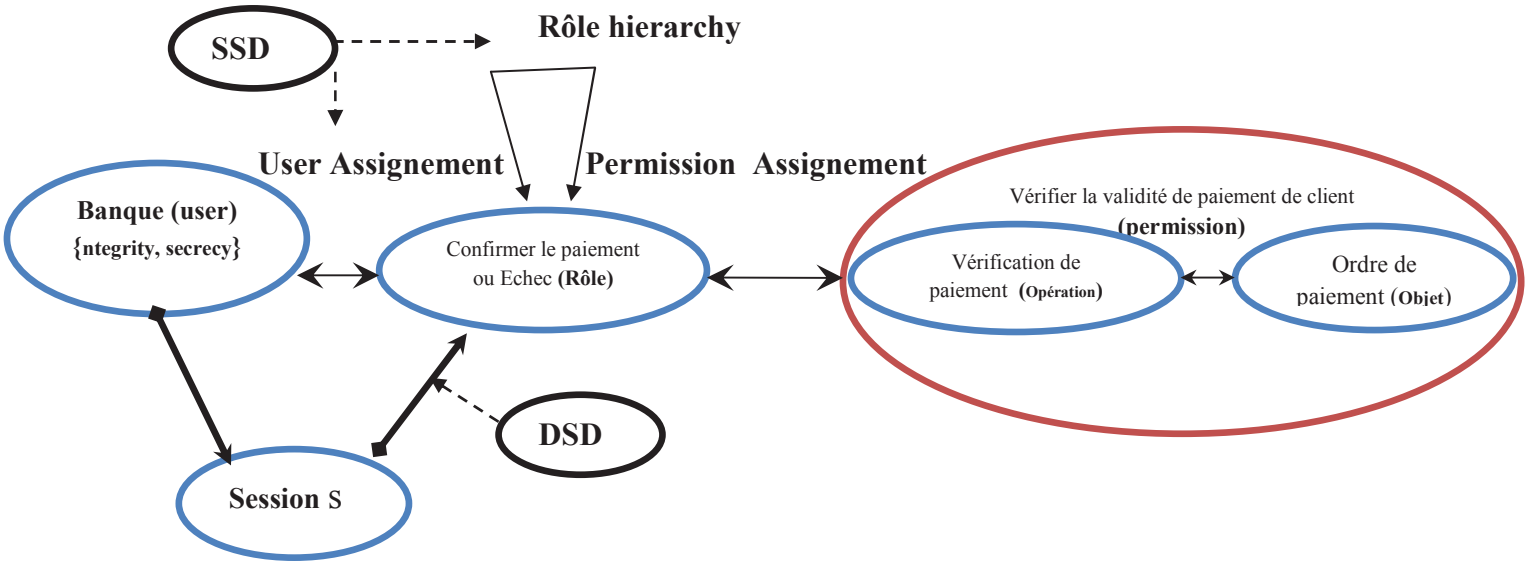

Fig5. Composante de Modèle RBAC

b) UMLSec

Nous avons présenté deux descriptions des scénarios avec deux stéréotypes différents :

❖ **Valider un Compte de Client:**

Le stéréotype « *provable* » permet d'exprimer la non-répudiation dans les transactions d'E-Commerce. Il garantie que si une action est exécutée, elle ne peut pas être niée. Un S/système peut être marqué prouvable avec l'utilisation des étiquettes : le tag *action* {Création d'un Compte Client} et le tag *cert* {Mise à jour des Factures Client}. **[32]**.

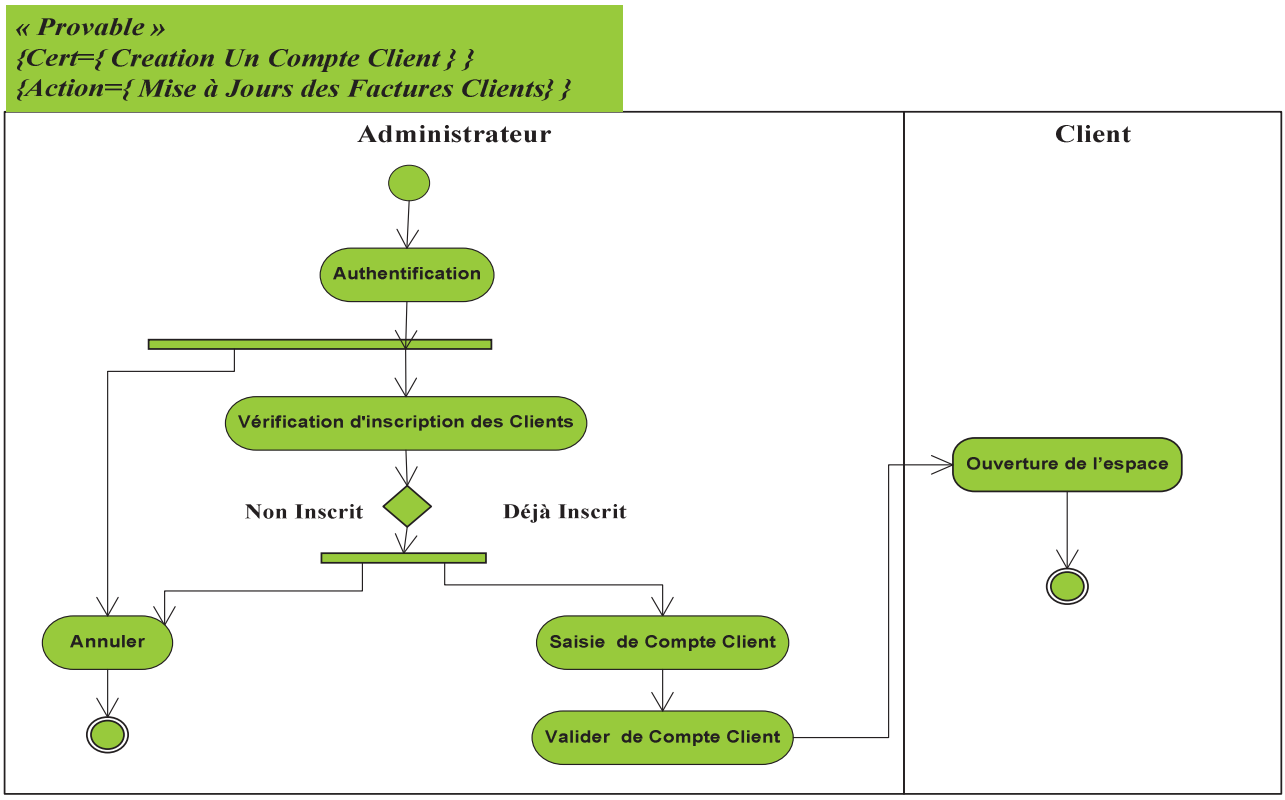

Fig6. Diagramme d'activité pour le cas d'utilisation «*valider un Compte de Client*».

❖ Effectuer Paiement avec Versement

Dans le modèle des scénarios critiques, les contraintes *secrecy*[2] et *integrity*[3] sont utilisés successivement pour assurer la confidentialité et l'intégrité des interactions entre le système et ses acteurs **[33]**.

[2] {Integrity}: pour assurer l'intégrité des interactions

[3] {Secrecy}: pour assurer la confidentialité des interactions

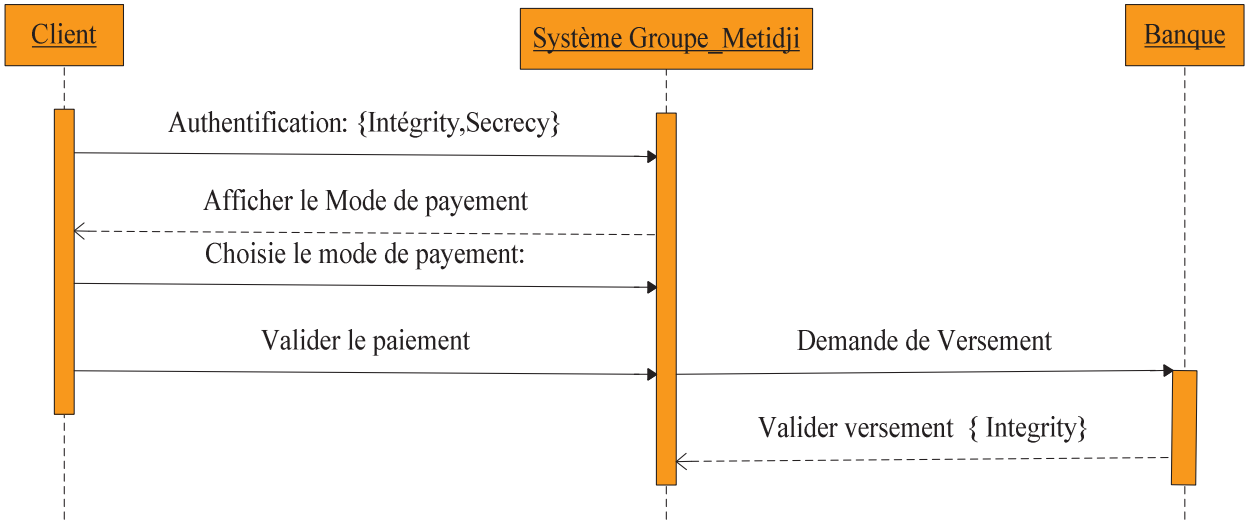

Fig7. Diagramme de séquence du cas utilisation et du cas de Sécurité pour « *effectuer le paiement* »

c) AuthUML

AuthUML [**34],** est un cadre fondé sur la programmation logique qui analyse les besoins de contrôle d'accès dans la phase de spécification d'exigence du cycle de vie pour éviter les conflits entre les accès de l'application et s'assurer qu'elles sont cohérentes et complètes. Il utilise le langage d'UML pour la modélisation formelle et se base sur le cadre FAF (Flexible Authorization Framework) pour spécifier les exigences de sécurité afin d'utiliser les règles de style de programmations logique et les prédicats personnels comme (Can Do, Der Can Do, conflting, ignorer…) pour présenter les autorisations et dérivés. Il est aussi fondé sur le principe de SoD (Separation of Duty) pour séparer les tâches de chaque objet et valider la conformité des exigences des autorisations. AuthUML passe par trois phases qui sont :

1. Traitement des exigences de contrôle d'accès.
2. Veiller à la cohérente, à l'exhaustivité et sans conflit au cas d'utilisation accédé (pour les besoins).
3. Veiller à la cohérente, à l'exhaustivité et sans conflit à accès aux opérations.

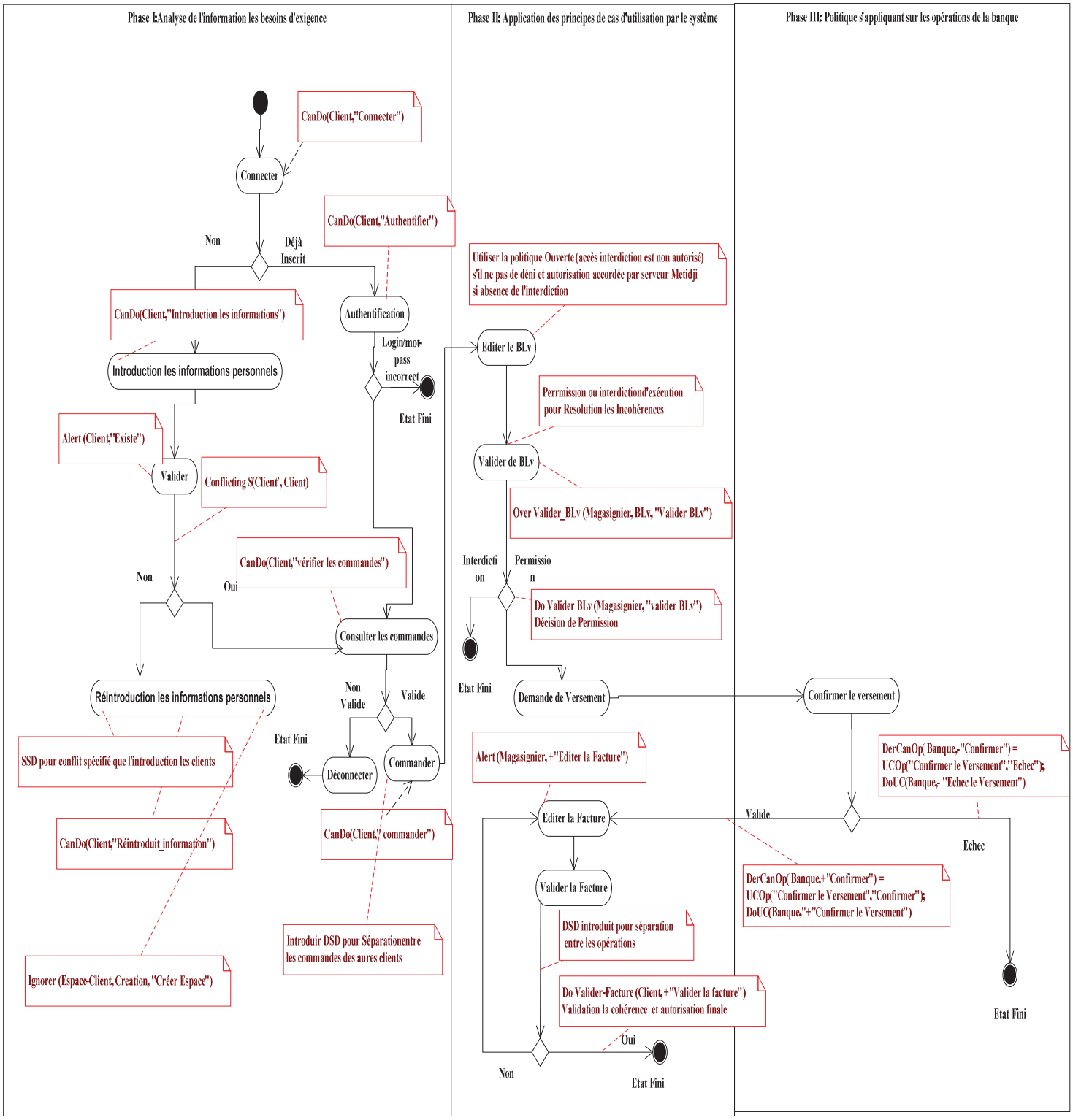

Fig8. Diagramme d'activité pour système d'E-Groupe Metidji par AuthUML.

4.2.3. Représentation des cas d'utilisation

Fig9. Diagramme de Cas d'Utilisation et Cas de Sécurité du système Global pour « *Groupe Metidji* »

5. Analyse et conception

Dans cette phase on déterminera les objets et les classes du système à construire, ainsi que leur structure et leurs relations .Chaque objet doit être décrit selon deux axes : axe statique (Structure de l'objet) et axe dynamique (Etats et messages de l'objet). **[35]**

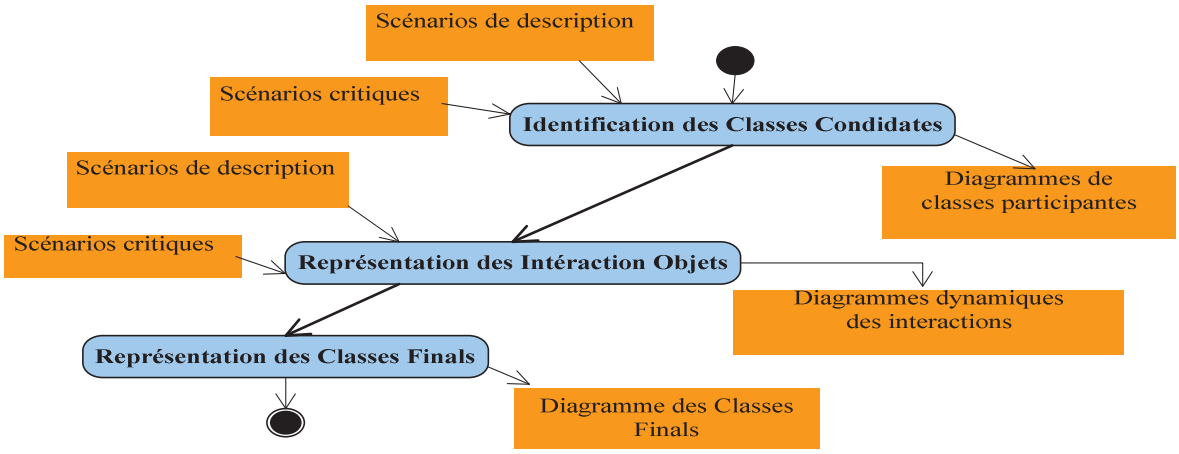

Fig10. Les activités de la phase d'analyse et de conception.

5.1. Identification des classes candidates

Dans cette étape, il s'agit de formaliser sous forme de classes et d'associations le diagramme statique pour chaque cas d'utilisation. Ce diagramme statique est appelé « Le diagramme de classes participantes ».

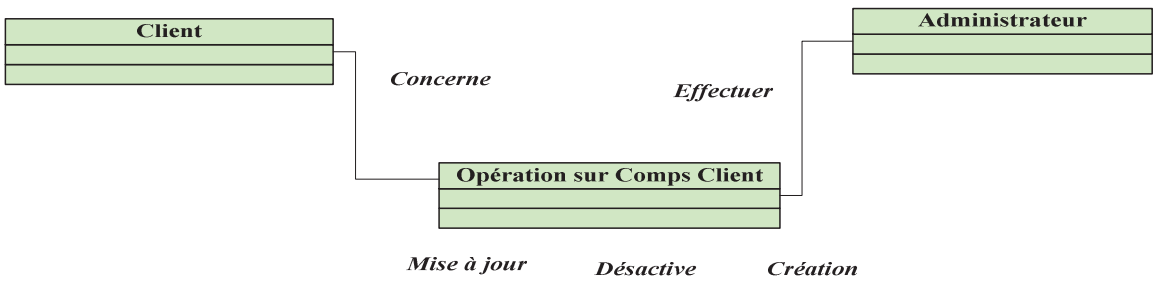

Fig11. Diagramme de Classe Participante pour « *gestion de Compte Client* ».

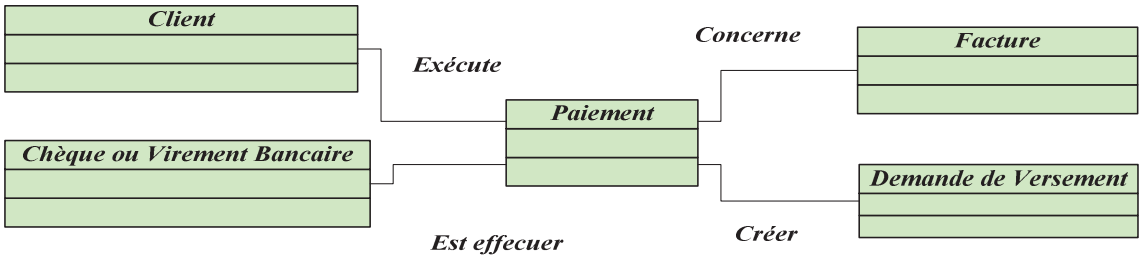

Fig12. Diagramme de Classe Participante pour « *Effectuer Payement* »

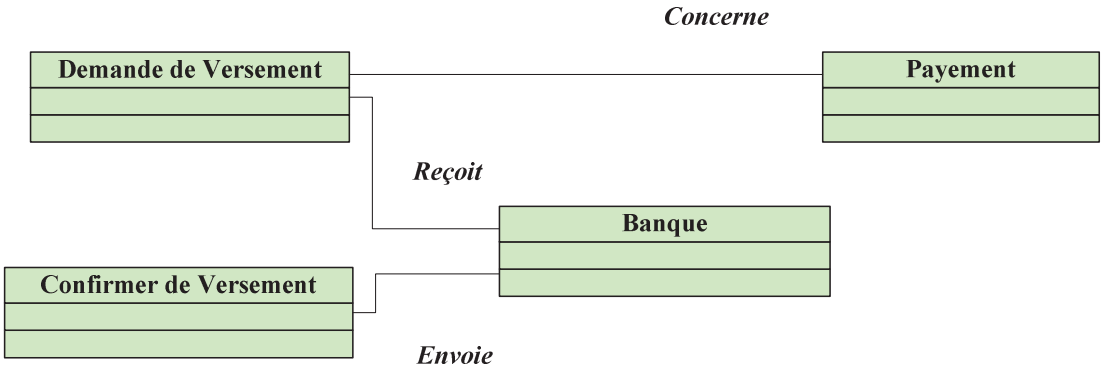

Fig13. Diagramme de Classe Participante pour « *Confirmer Versement* ».

5.2. Analyse Dynamique

Cette étape consiste à représenter les interactions entre les objets ; Elles peuvent être décrites au moyen de deux types de diagrammes : diagramme de séquence pour des opérations chronologiques des messages et diagramme de collaboration pour la dimension structurelle et le comportement.

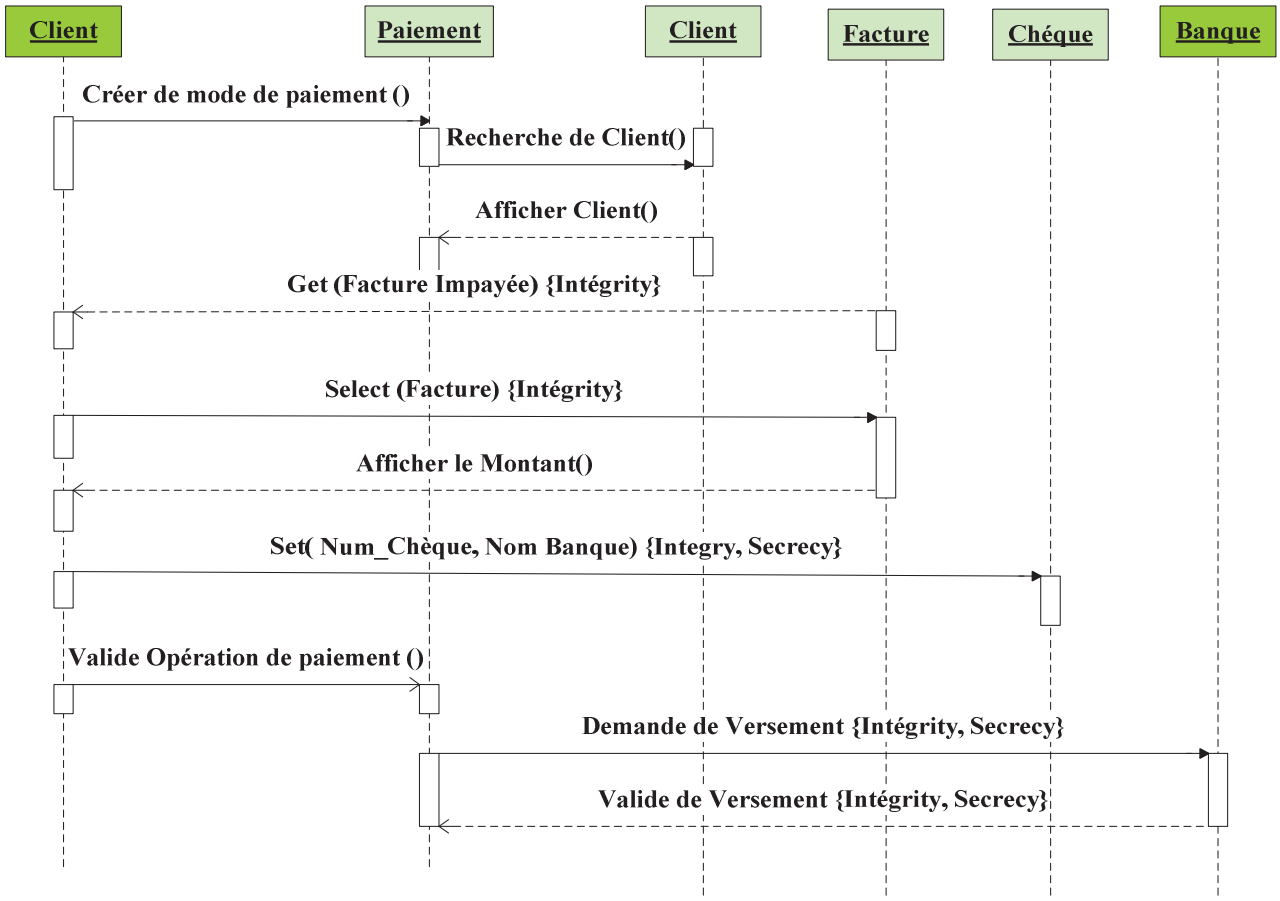

Fig14. Diagramme des interactions d'objets sécurisées pour le scénario *«Effectuer versement de paiement ».*

5.3. Diagramme de classes finales

Cette étape consiste à mettre à jour le diagramme de classe de modèle statique pour représenter les contraintes de sécurité sur les données en profitant de l'analyse de réalisation des classes participantes avec les interactions d'objets de diagramme dynamique. La figure suivante montre le diagramme de classes finales pour le système « *Groupe Metidji ».*

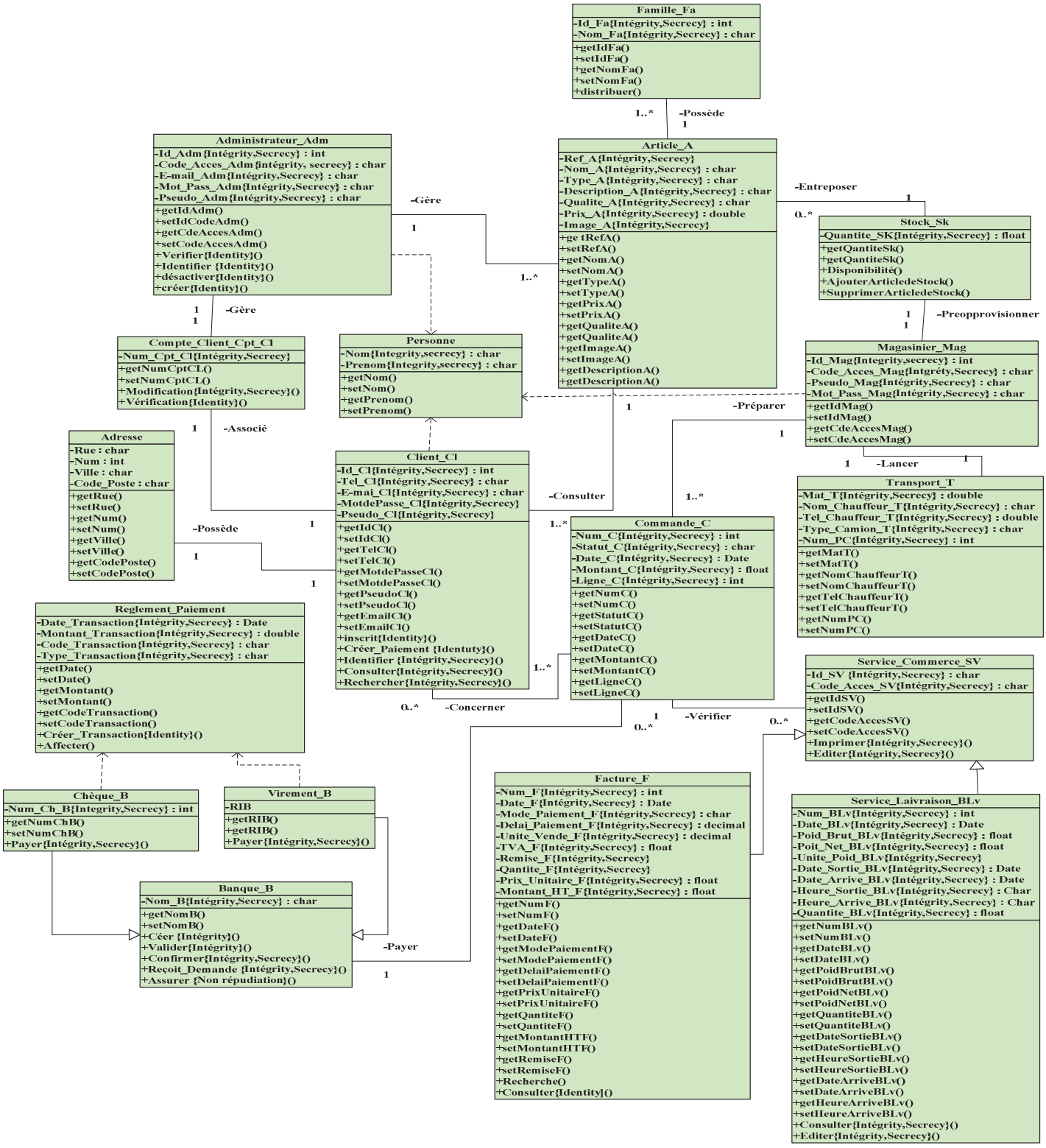

Fig15. Diagramme des classes finales du système « *Groupe Metidji* »

6. Modélisation de la navigation

Cette étape présente les diagrammes d'activité qui sont utilisés pour modéliser avec précision la navigation dans l'application web, et les conventions propres à la navigation dans le site web. Les conventions graphiques suivantes seront utilisées :

- ✓ « Page » pour une page complète du site.
- ✓ « Action » pour action simple (Exemple : Introduit le mode de paiement).
- ✓ « Exception » pour une Erreur (Exemple : Mot de passe incorrect).

La figure suivante présente les modèles de navigation pour « Demande de versement et confirmation ».

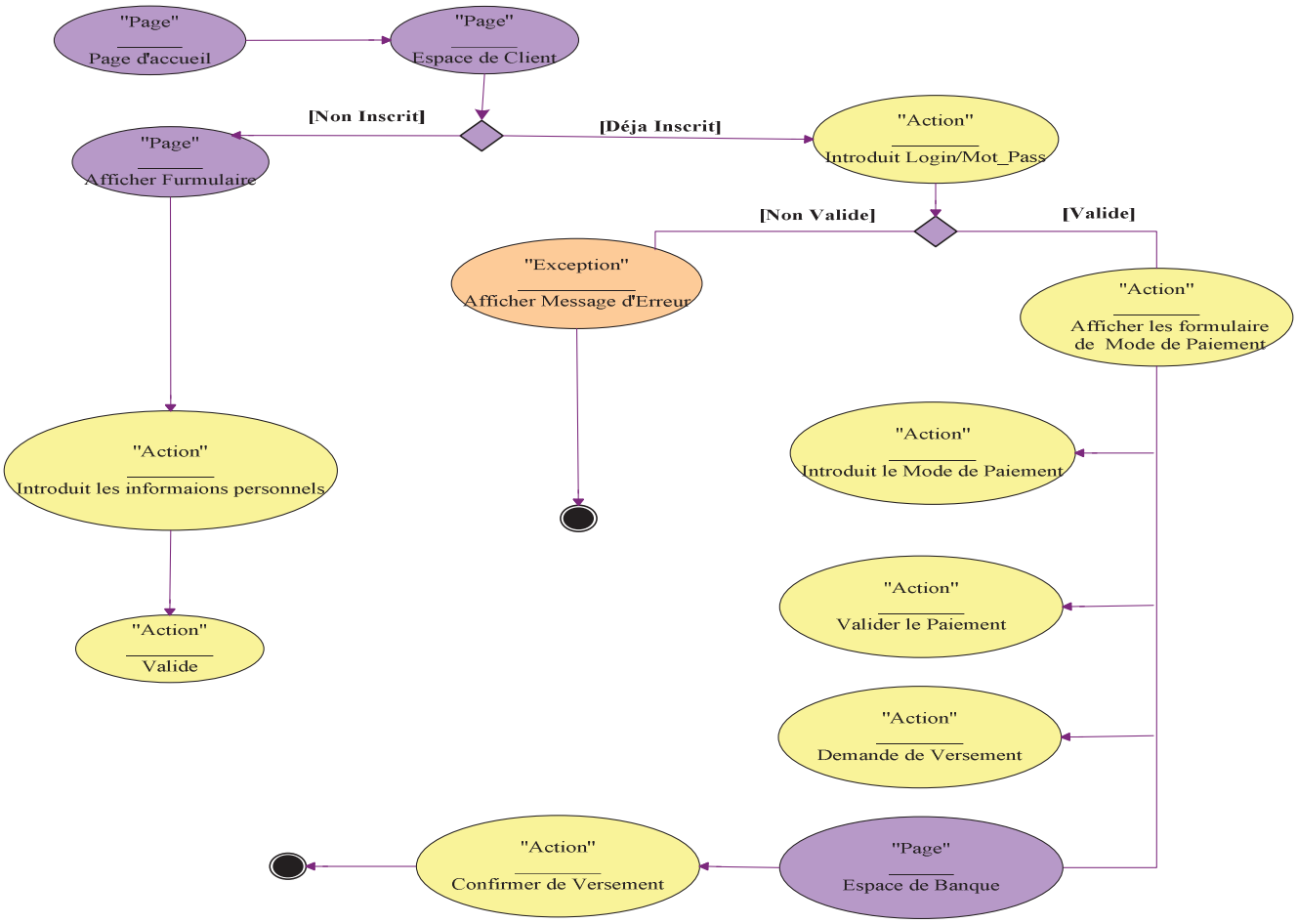

Fig16. Modélisation de la navigation du système *e-Groupe Metidji*

7. Conception technique

7.1. Composants d'Exploitation

Le diagramme de composante présente les organisations et les contraintes de sécurité sur les dépendances entre les éléments de logiciel d'un système **[36]**

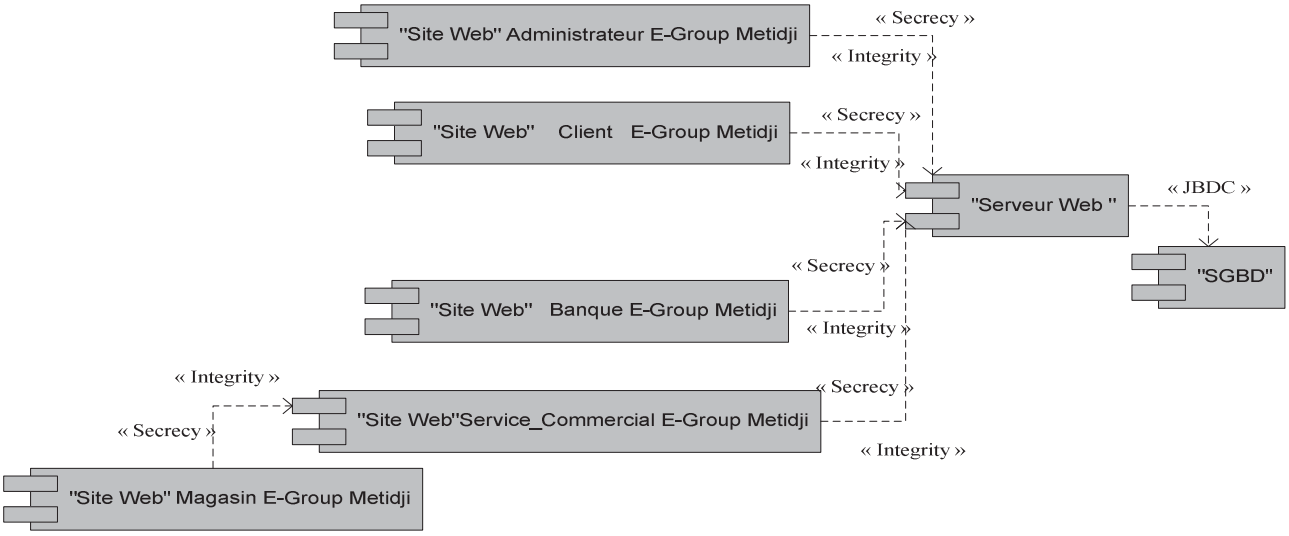

Fig17. Diagramme de Composante de système *E-Groupe Metidji* **[36]**

7.2. Développement du Modèle de Déploiement

Le modèle de déploiement consiste à définir tous les postes de travail du système. Un poste de travail représente un ou plusieurs acteurs localisés sur une machine et remplissant une fonction identifiée **[36]**

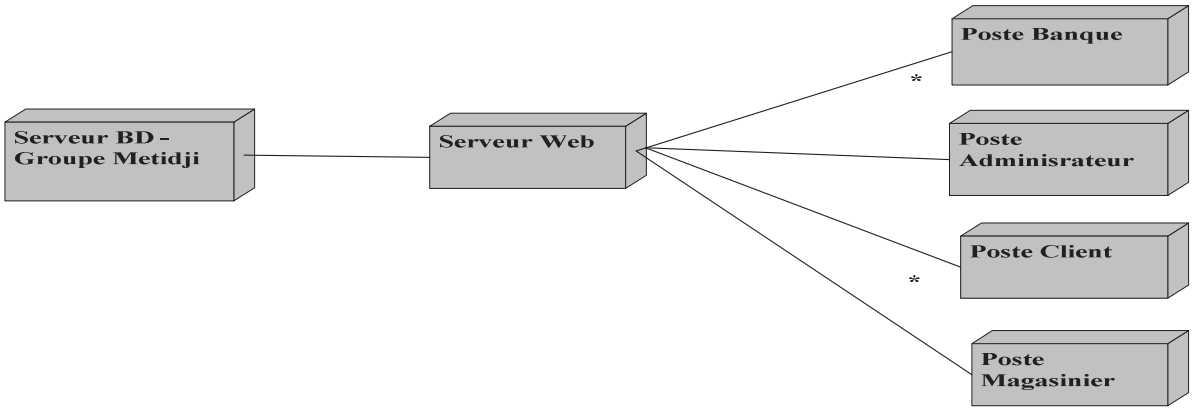

Fig18. Modèle de déploiement du système du *Groupe Metidji.* **[36]**

7.3. Configuration Matérielle Sécurisée

Pour garder une bonne sécurité des données de l'entreprise (coté matériel ou logiciel), il existe différents outils sur le marché qui sont utilisés, à savoir : les Firewall, les pare-feu applicatifs, les DMZ,…..

Pour notre système nous avons proposé les outils suivants : **[37]**

Pare-feu ou bien *Firewall : c'*est un diapositif matériel et/ou logiciel de sécurisation qui sera placé entre le réseau local et le réseau public (Internet) afin de filtrer les accès et nous protéger contre les intrusions. Il analyse les en-têtes des paquets IP et les flux entrants ou sortants. Il existe trois types de *Pare-feu :*

- ✓ *Firewall routeur* (*stateless)*: qui analyse les paquets selon un ensemble de règles de filtre.
- ✓ *Firewall circuit (stateful) :* est un pare-feu qui est utilisé entre deux connexions pour vérifier que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens pour conserver le traçage.
- ✓ *Firewall applicatif (proxy):* est le point de passage de toutes les applications qui nécessitent l'internet pour réaliser le masquage d'adresse par relais applicatif et établir la connexion avec le serveur externe. Ces mécanismes sont : Authentification et/ou autorisation des accès, surveillance, gestion, identification…..ex.

L'utilisation du mode de *Firewall applicatif* permet d'assurer une protection contre : **[38]**

- Les attaques par saisie contraires au formulaire web.
- Les attaques par le protocole *http*.
- Les attaques par déni de service.
- Les attaques par modification du contexte de transaction (champs cachés, champs pré-saisie, cookies,…).
- Les attaques déjà connues (fonction type *IDS* à l'aide de signatures).

Il est utilisé dans la Zone Démilitarisée DMZ[4] (privet/public) pour le trafic de réseau d'internet.

- ✓ *IDS (Intrusion Détection Système) :* pour écouter le réseau et générer des alertes comme (Network IDS, Host IDS), et IPS pour bloquer l'intrusion.

[4] DMZ est une partie du système d'Information présentant un niveau de sécurité homogène.

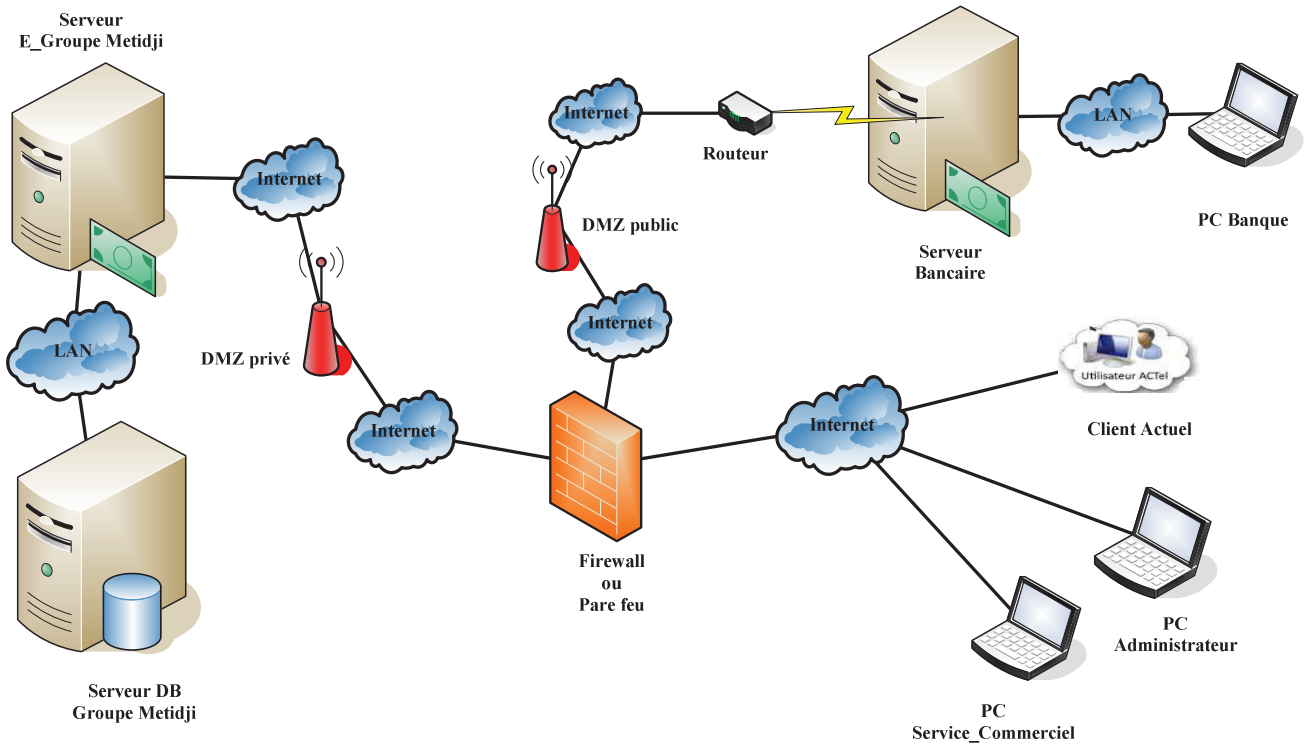

Fig19. Modèle de configuration matérielle sécurisée du système *E-Groupe Metidji.*

8. Conclusion

Dans ce chapitre nous avons défini la spécification des besoins fonctionnels avec les contraintes de sécurité puis l'analyse et la conception du système en définissant la structure et le comportement des objets en se basant sur le langage UML pour la modélisation formelle et l'intégration des approches à priori de la sécurité.

1. Introduction

Après la conception du système E-commerce du groupe Metidji, on va présenter dans ce chapitre les outils et les technologies de développement employés pour réaliser notre système. On présentera par la suite les différentes interfaces de l'application.

2. Choix de la Plate-forme

J2EE (Java 2 Platform, Enterprise Edition) est une plate-forme conçue pour les mainframes[1] qui sont utilisés dans les grandes entreprises. C'est une plate-forme fortement utilisée par des serveurs d'applications Java (*Tomcat, JBoss, GlassFish* ;…) pour le développement et l'exécution des applications distribuées. Elle vise les applications d'entreprise et bénéficie des avantages des différentes technologies qui la composent. Son objectif est l'amélioration de la sécurité et la fiabilité des programmes ainsi que la simplification des besoins fonctionnels de l'entreprise. Elle est composée de deux parties essentielles : **[39]**

- Partie1 : c'est un ensemble de spécifications pour une infrastructure dans laquelle s'exécutent les composants écrits en Java : un tel environnement se nomme Application.
- Partie2 : ensemble d'API (Application Programmation Interface) qui peuvent être utilisées séparément. Certaines applications nécessitent une implémentation de la part d'un fournisseur tiers.

Les avantages de J2EE sont: **[40]**

- ✓ Une architecture d'applications basée sur les composantes (Servlet, JSP, JSF,..) qui permet un découpage de l'application et donc une séparation des rôles lors du développement.
- ✓ L'intégration d'interfaces avec le système d'information existant grâce à de nombreuses *API* : JBDC, JNDC, JMS,…
- ✓ La possibilité de choisir les outils de développement et/ou les serveurs des applications utilisées qu'ils soient commerciaux ou libres. Elle permet pour les applications « critique » de l'entreprise la disponibilité, la tolérance aux pannes, la sécurité, ….)

[1] Mainframe (Big Iron) : est un ordinateur de haute performance utilisée à des fins de calcul à grande échelle.

3. Choix des outils et des Technologies de Développement

Nous avons choisi le langage de programmation *Java,* l'environnement IDE *NetBeans* et le serveur d'application *Glass Fish.* Nous avons utilisé la technologie des *JSF* pour réaliser les pages web de type *JSP/Servlet* et le modèle *MVC* qui réserve toutes les parties de « Traitement » aux *Servlet* et les aspects de « présentation » aux *JSP (Java Server Page).*Pour la gestion de notre base de données nous avons opté pour le *SGBD MySQL.* Tous ces outils seront utilisés pour la réalisation de notre système *E-Commerce de Metidji.*

3.1. Java

Java est un langage de programmation informatique orienté objet et un environnement d'exécution portable créé par ***Sun Microsystems*** et présenté officiellement le 23 mai 1995 au *SunWorld ; C'e*st un langage facilement portable sur plusieurs systèmes d'exploitation tels que : *Unix, Microsoft Windows, Mac Os ou Linux.*

Java est un langage qui reprend en grande partie la syntaxe du langage C++ qui est très utilisé par les informaticiens. Néanmoins, Java a été épurée des concepts les plus subtils du C++ et à la fois les plus déroutants, tels que l'héritage multiple remplacé par l'implémentation des interfaces. Les concepteurs ont privilégié l'approche orientée objet de sorte qu'en Java, tout est objet à l'exception des types primitifs (nombres entiers, nombres à virgule flottante, etc.). **[41]**

Java est un langage plus sécurisé, rapide et fiable parce qu'il possède la technologie sous-jacente qui permet l'exécution des programmes avec sécurité. Il comprend d'importantes améliorations en termes de performance. Les applications java peuvent être développées sur n'importe quel système d'exploitation**.**

3.1.1. Java Script

Java Script est un langage de programmation de Script principalement utilisé pour les pages web interactives. Il est exécuté uniquement sur le navigateur. Il a été créé en 1995 par *Brendan Eich* ; C'est un langage orienté objet à prototypes, c'est à dire que le prototypage permet de générer des objets à héritage personnalisé**.** Il s'intègre dans les documents HTML et peut fournir des niveaux d'interactivité aux pages Web. Le développeur peut créer *des objets* sur la page, avec *des propriétés et des méthodes* et leur associer *des actions* en fonction d'événements déclenchés par l'utilisateur. **[42]**

3.2. Technologie de *JSF*

JSF (Java Server Face) est une technologie de développement des applications web relativement récente dans le monde de J2EE. Elle est basée sur les technologies *JSP* et *Servlet*. C'est une technologie utilisée pour faciliter la mise en œuvre des composants web qui permettent la création des interfaces utilisateurs tout en respectant le modèle d'architecture *MCV* des applications web. Il autorise le fonctionnement entre les JavaBeans et la page du navigateur **[43].**

JSP permet : **[44]**

- ✓ une séparation nette entre la couche de présentation et les autres couches
- ✓ le mapping HTML/Objet.
- ✓ un modèle riche de composants graphiques réutilisables
- ✓ une liaison simple entre les actions côté client de l'utilisateur et le code Java correspondant côté serveur.
- ✓ Le support de différents clients (HTML, WML, XML,...) grâce à la séparation des problématiques de construction de l'interface.

3.3. Modèle *MVC*

MVC (Model View Controller) est un modèle de conception logicielle très répandu et fort utile. MVC est une architecture et une méthode de conception qui a pour objectif d'organiser une application interactive en séparant les données, la présentation des données et le comportement de l'application **[45].**

Le Scénario d'exécution de *MVC* est :

- ✓ L'utilisation émet une requête.
- ✓ Le Contrôleur intercepte la requête de l'utilisateur.
- ✓ le Contrôleur détermine quelle partie du modèle est concernée et quelle vue y est associée
- ✓ Le modèle traite les interactions avec les données, applique les règles métier et renvoie les données au contrôleur.
- ✓ Le contrôleur sélectionne la vue et lui renseigne les données.
- ✓ Le vue présente les données à l'utilisateur qui les implémente par classes de *JSP*

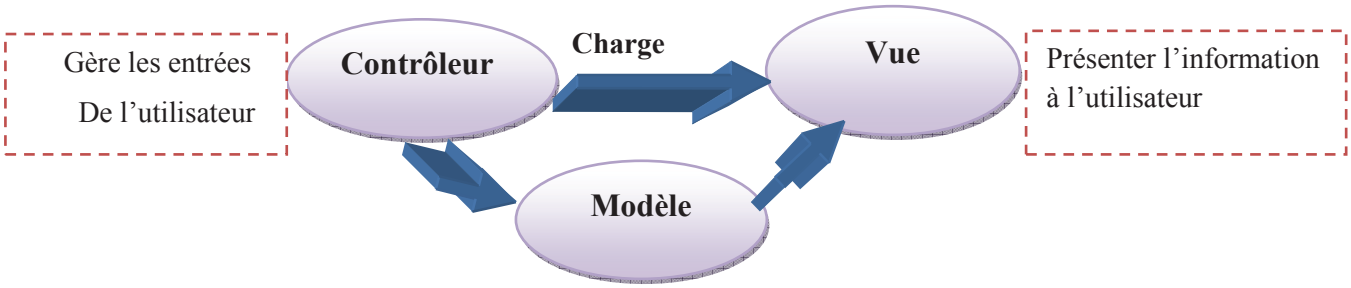

Fig20. L'architecture *de MVC*

3.4. NetBeans

Nous avons choisi l'IDE *NetBeans*, qui est un environnement de développement intégré, placé en Open source par Sun Microsystems. NetBeans permet d'écrire, de compiler, de déployer des programmes et également supporter n'importe quel langage de programmation. Il est disponible sous *Windows, Linux, Solaris, Mac OS* ou sous toute autre version indépendante de systèmes d'exploitation.

NetBeans comprend toutes les caractéristiques d'un *IDE* moderne (coloration syntaxique, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages web,…) et prend en charge la technologie du *JSF /Facelets* **[46]**

3.5. MySQL

MySQL (My Structured Query Langage ou Mon langage de requête Structuré) est utilisé comme *SGBD (Système de gestion de bases de données)*. C'est un serveur de bases de données relationnelles développé dans un souci de performances élevées en lecture des données. Il comporte plusieurs tâches multiutilisateur. Il est rapide pour les petites bases de données. Il permet : **[47]**

- ✓ La Satisfaction des contraintes d'évolutivité et de performance des sites Internet les plus visités et des applications les plus exigeantes
- ✓ Possède un ensemble d'options de programmation qui permet de faciliter l'accès aux données.
- ✓ Explorateur qui facilite l'administration de bases de données pour la création, la visualisation et la mise à jour de celles-ci.

3.6. Serveur GlassFish

GlassFish est le nom de serveur d'application Open Source *Java EE 5 et déformé Java EE6* avec la version 3 qui sert de base au produit *Oracle GlassFish Server* (anciennement *Sun Java, System Application Server de Sun Microsystems)*, sa partie persistante *Toplink* provient d'Oracle. C'est la réponse aux développeurs Java désireux d'accéder aux sources et de contribuer au développement des serveurs d'applications de la nouvelle génération.

Notre serveur d'application est :

- ✓ Basé sur l'architecture modulaire (Modèle Spiracle, V,..)
- ✓ Le temps de démarrage est rapide pour l'exécution. **[48]**

4. Présentation de l'Application

4.1. Fenêtre d'accueil

C'est la fenêtre principale de l'application qui offre l'accès à la liste des familles de produit, la présentation de l'entreprise du Groupe Metidji, le menu des espaces (panier, client et les informations de contact de la société).

Fig21. Page de profil de la société *Groupe Metidji*

4.2. Fenêtre d'Inscription

Si un client veut visiter le site, il doit cliquer sur *Espace Client* afin de s'inscrire dans le système pour pouvoir commander les produits dont il a besoin.

Fig22. Validation de l'Inscription du Client

4.3. Fenêtre de gestion des articles

L'administrateur devra toujours vérifier tous les articles de la société et leur promotion. Il doit effectuer la gestion des articles (ajouter, supprimer ou modifier les prix), en détaillant les coordonnées de chacun d'eux.

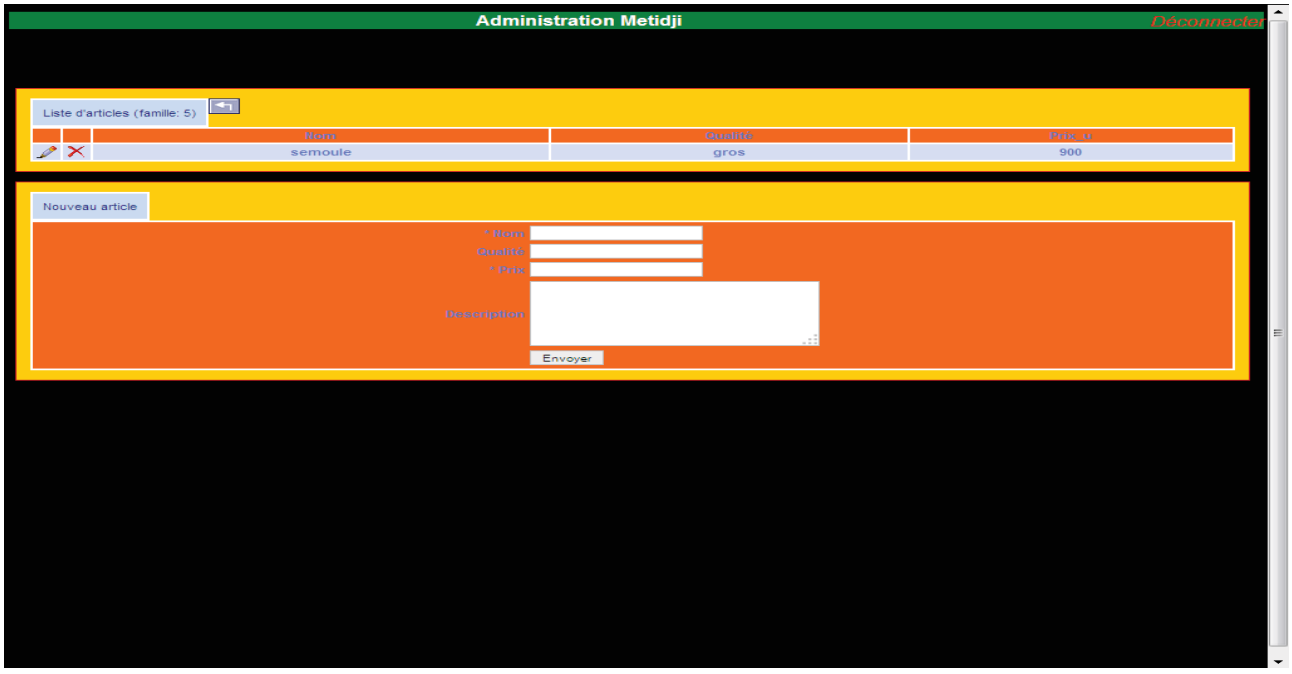

Fig23. Validation de la gestion d'articles par l'administrateur

4.4. Fenêtre de gestion du compte client

L'administrateur devra vérifier sans cesse les tableaux récapitulatifs de tous les clients inscrits afin de saisir le compte de chaque client pour lui permettre de choisir le mode de paiement désiré.

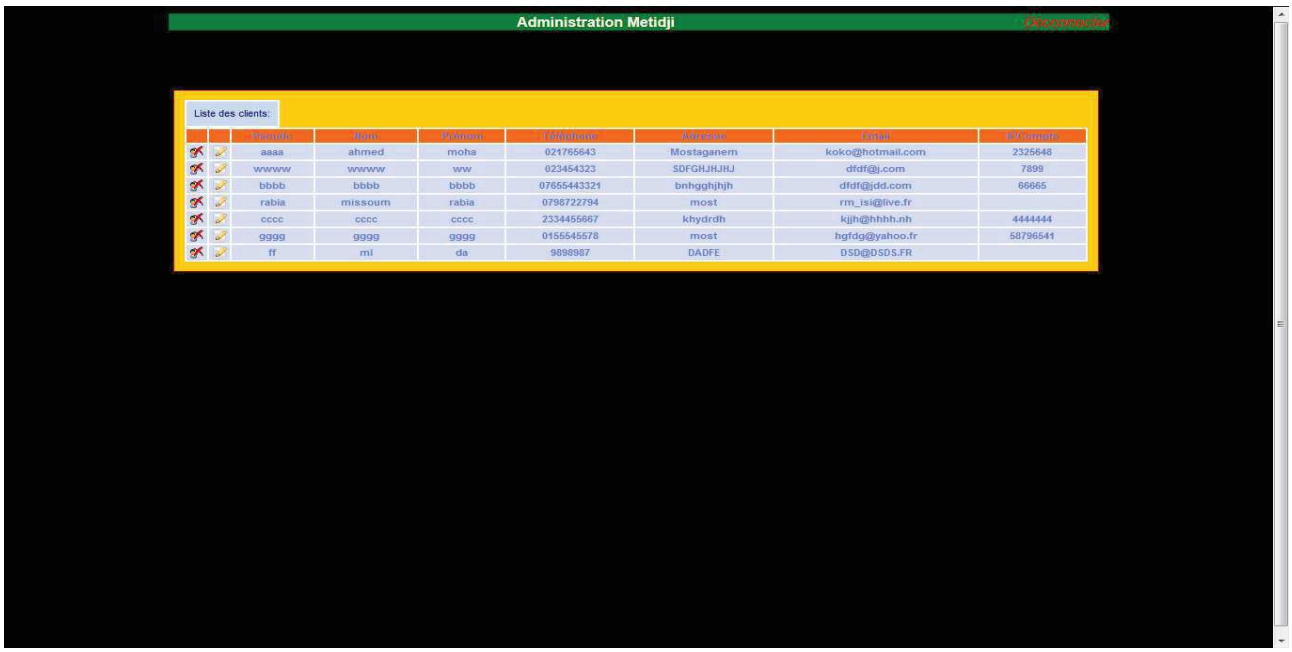

Fig24. Page de validation le compte de client par l'administrateur

4.5. Fenêtre du mode de Paiement

Après le choix des produits dont il a besoin, le client choisit et valide le mode de paiement (chèque ou virement) dans *l'Espace Panier.*

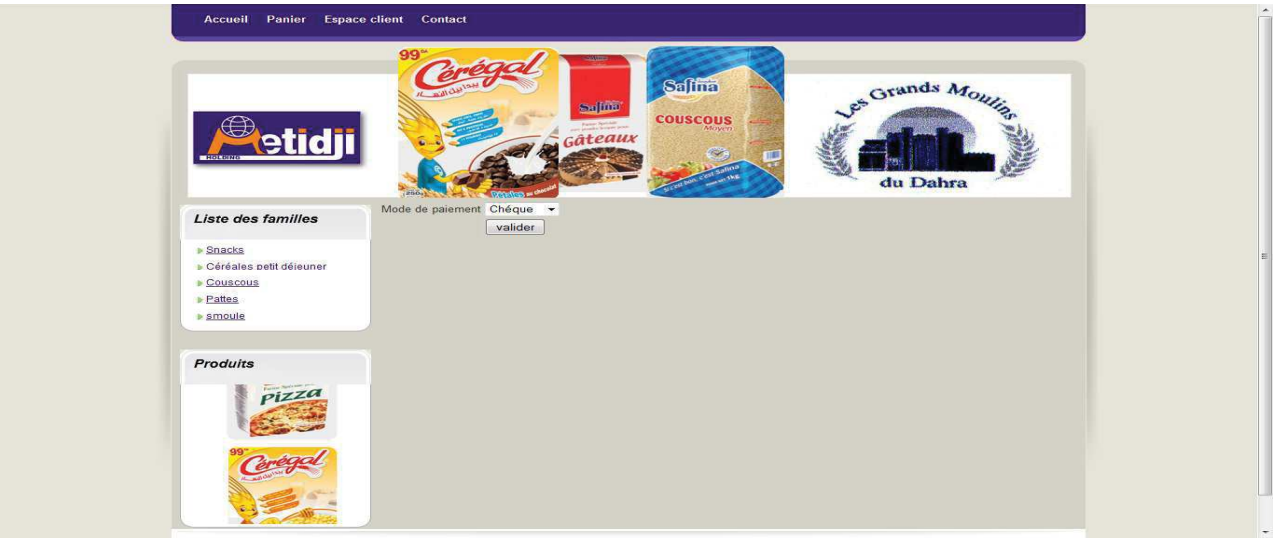

Fig25. Page de confirmation du Mode de Paiement

4.6. Fenêtre des commandes du Client

Le Client, après la commande des produits, consulte le tableau récapitulatif des commandes en cours d'attende pour savoir si sa commande a été validée ou non par le système.

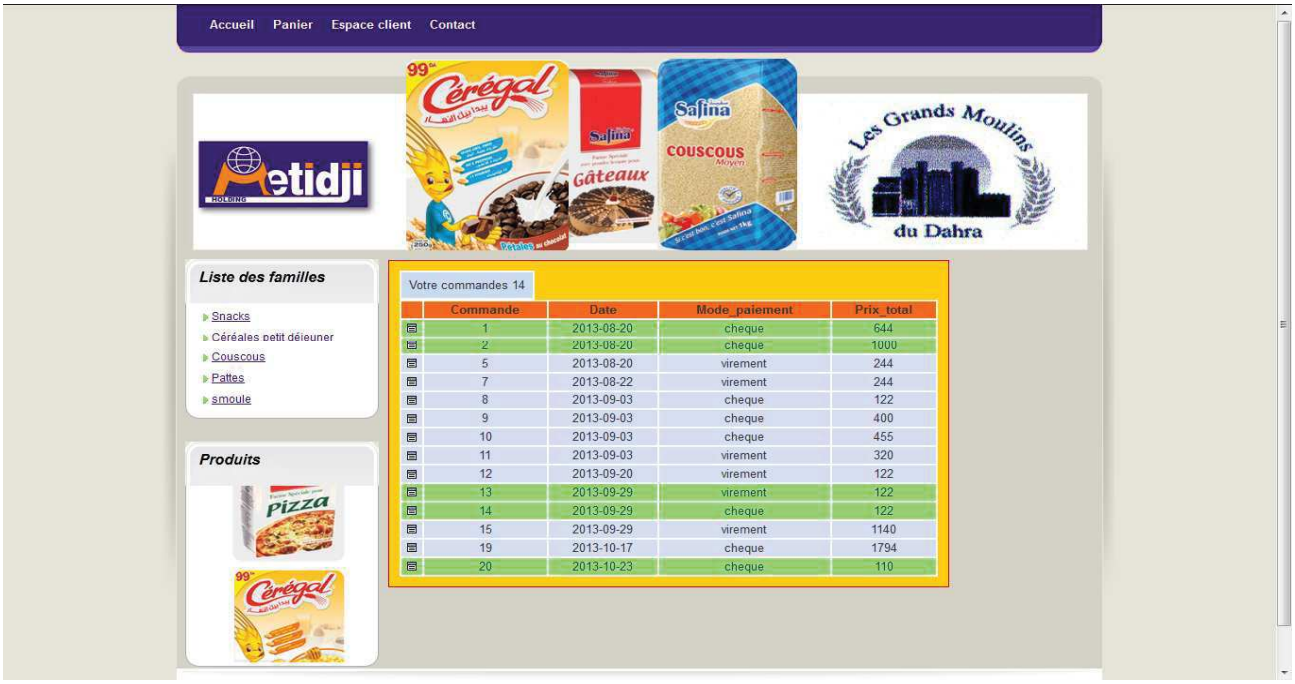

Fig26. Page d'affichage des commandes de chaque client

4.7. Traitement des commandes du client

Dans l'espace administration, le magasinier vérifie sans cesse le tableau récapitulatif des commandes passées par les clients pour lancer le traitement sur les commandes non valides.

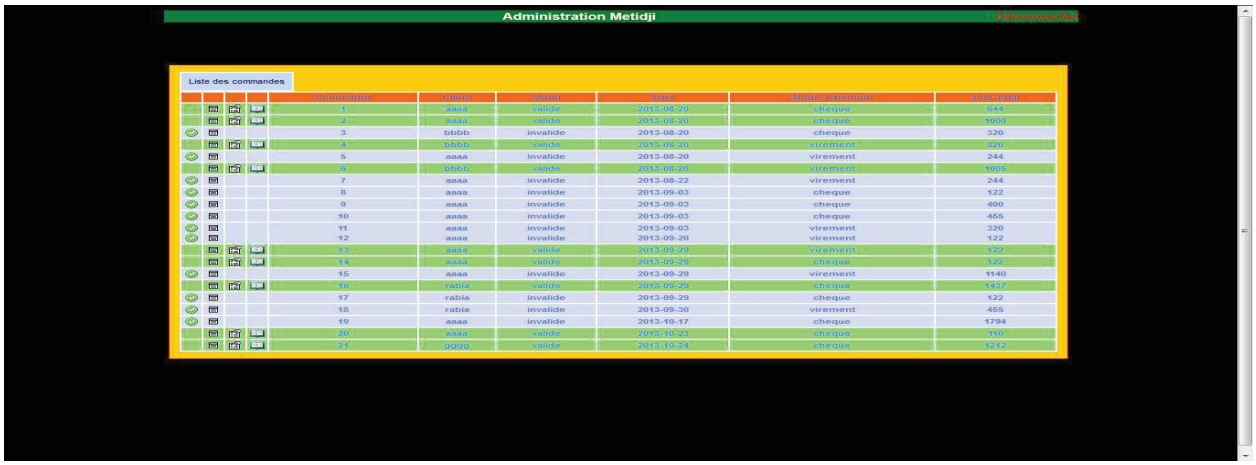

Fig27. Page d'affichage du traitement des commandes par le Magasinier

4.8. Fenêtre de Transport

Après avoir validé les commandes de chaque client, le Magasinier vérifie si le client a besoin du transport ou non. Dans le cas positif il lance la commande de transport tout en saisissant les coordonnés relatives au chargement des produits.

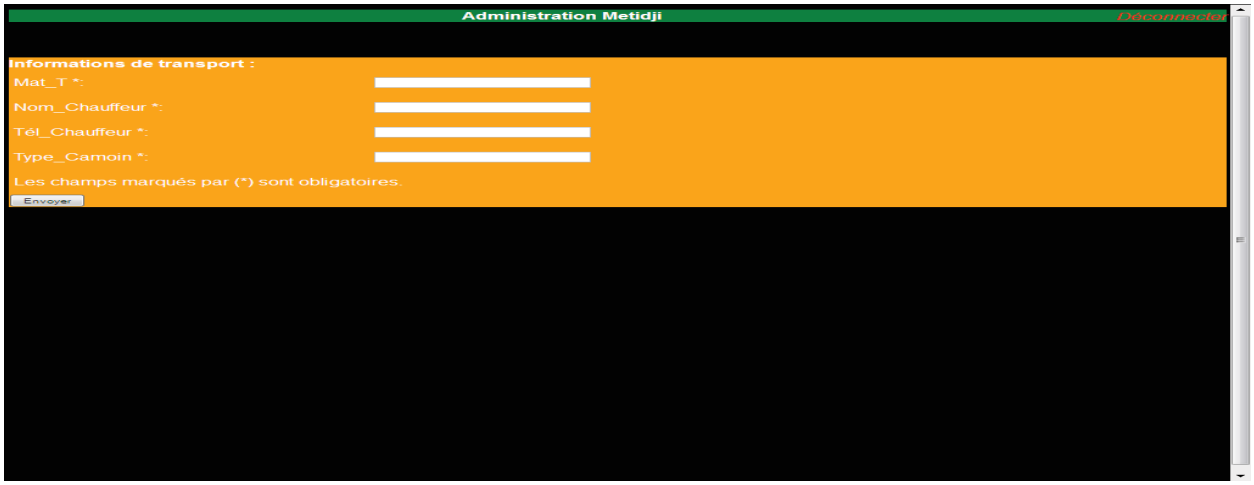

Fig28. Page d'affichage des coordonnées de transport par le Magasinier

4.9. Bon de Livraison et Facture

Après la validation des commandes des produits et la sélection des applications de transport choisies pour chaque client, le magasinier édite le Bon de Livraison et la Facture correspondants à cette opération.

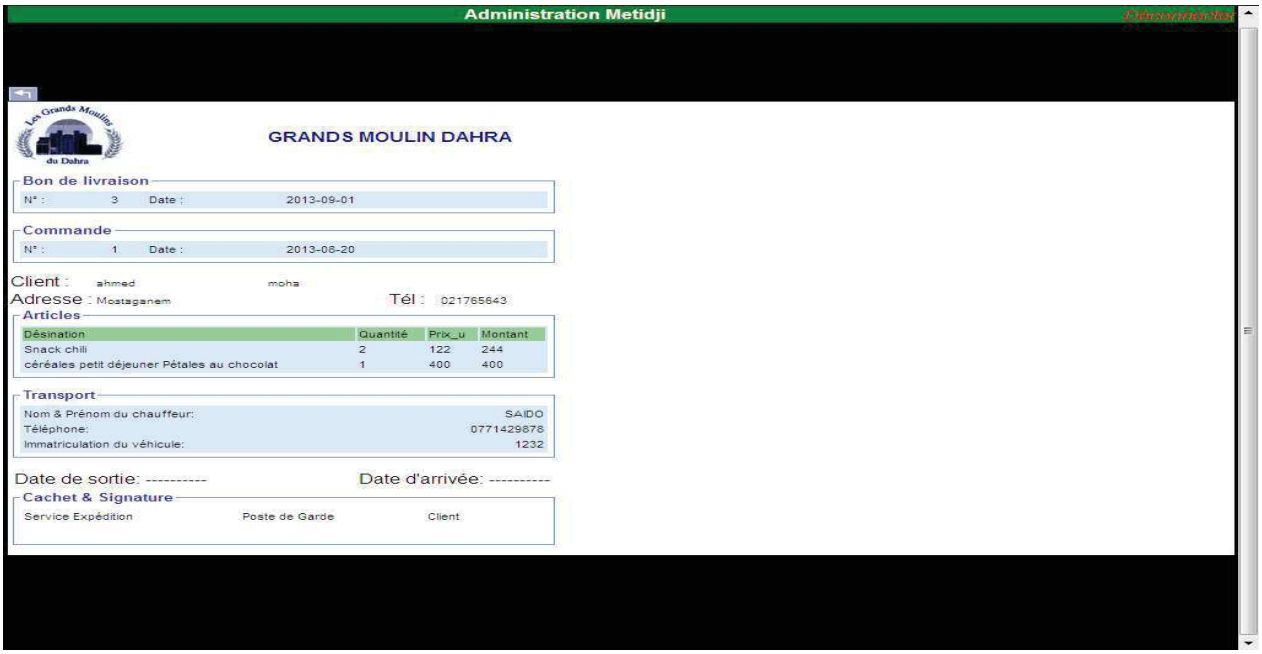

Fig29. Page Bon de Livraison

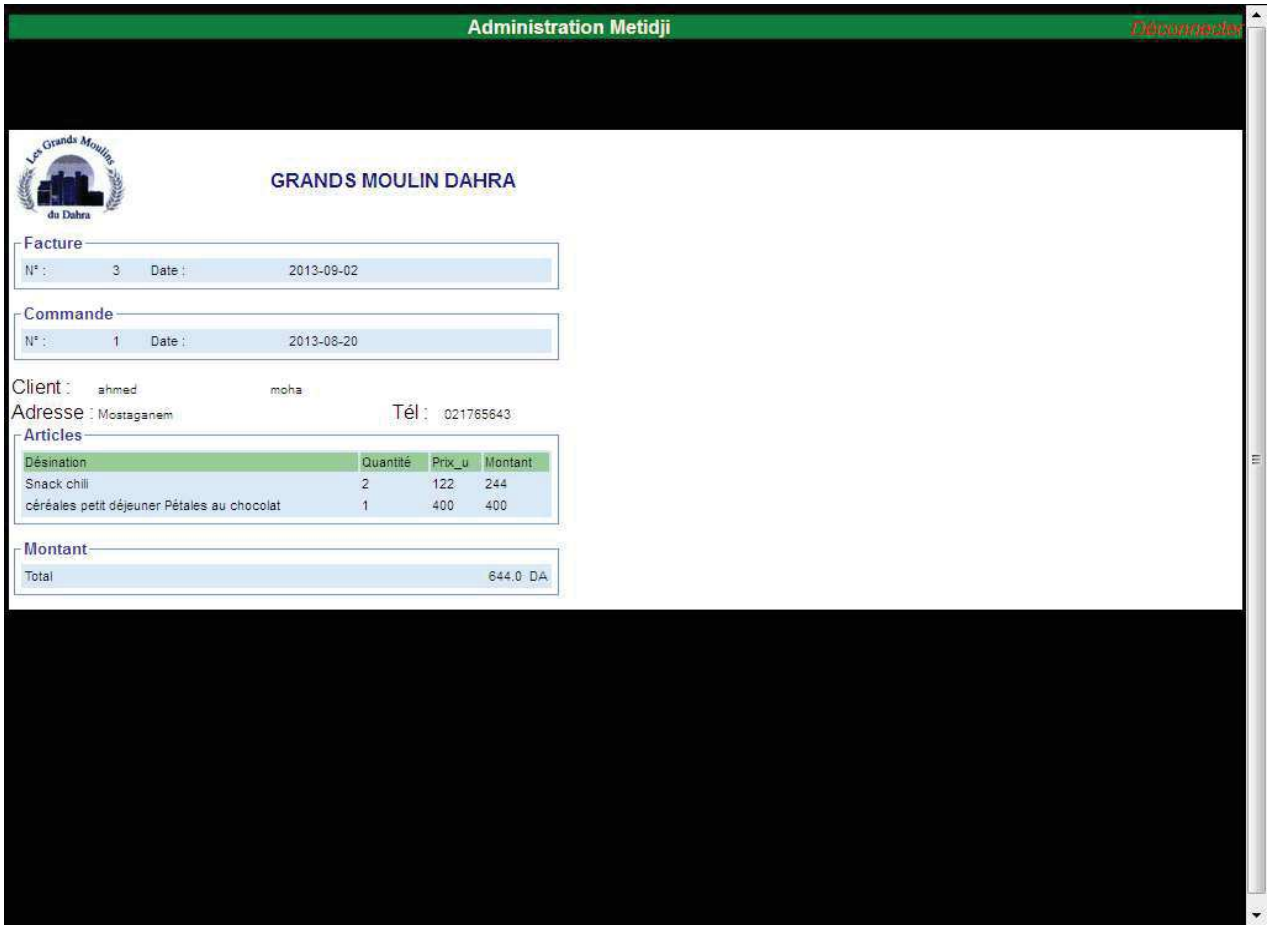

Fig30. Page Facture

5. Conclusion

Au cours de ce chapitre nous avons présenté les étapes de réalisation des interfaces du Système E-Commerce du *Groupe Metidji* ainsi que les outils de développement. Nous avons développé une application web qui répond aux besoins de la société d'E-commerce. De même nous avons intégré une solution de sécurité entre les points d'accès contre les intrusions.

Conclusion Générale

Ce projet de fin d'étude nous a permis de développer un système e-commerce pour le groupe Metidji de la wilaya de Mostaganem.

En plus de la phase conception et de la phase implémentation, nous avons introduit la notion de sécurité des systèmes d'information : chose qui est nécessaire et importante pour toute application développée sur le net. Le piratage, les intrusions, l'usurpation d'identité, les virus, ainsi que d'autres maux du net nous obligent à consacrer une bonne partie de notre travail à la surveillance et à la sécurité des transactions commerciales et bancaires électroniques.

Dans les dernières années, la sécurité des applications Web est une préoccupation majeure. Dans ce travail, nous avons développé une application Web de commerce électronique en tenant compte les besoins fonctionnels et les contraintes de sécurité durant toutes les phases de la démarche de développement.

La réussite des projets réside en premier lieu dans l'existence d'une démarche de développement. Dans ce contexte, nous avons proposé une démarche de conception sécurisée (*DCS*) basée sur le processus *RUP*; Cette démarche a permis une bonne modélisation formelle des besoins fonctionnels du système d'information du *Groupe Metidji* par ses différents diagrammes de conception (*digramme de cas d'utilisation, diagramme de classes, diagramme de contexte,...)* ainsi que par ses critères de sécurité (*disponibilité, authentification, intégrité, confidentialité, non-répudiation, ...*).

Pour le côté sécurité du système e-commerce nous avons introduit la méthode AuthUML dans la partie modélisation formelle des besoins fonctionnels du contrôle d'accès.

Pour la réalisation de la partie implémentation, nous avons choisi les technologies de *JAVA* pour sa puissance dans le développement d'applications e-commerce ou autres. Le traitement des risques au niveau du développement sur web s'effectue grâce à la technologie des *JSF* qui proposent un Framework puissant en termes de sécurité et de performance. *Le NetBeans,* les *JSF*, GlassFish ainsi que MySQL ont été utilisés pour le développement de notre application sur le web.

Bibliographie

[1] : Economie - Commerce, Internet ; http://actualite-economique.lalibre.be/commerce-internet.html

[2] : De Statistics Explained. Aller à : Navigation, rechercher *Données de février 2012.* *Données plus récentes: Informations supplémentaires Eurostat, Principaux tableaux et Base de données*
http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics_at_regional_level/fr

[3] : Définition E-commerce par Bertrand Bathelot. 24 juin 2012 http://www.definitions-marketing.com/Definition-E-commerce/

[4] : Jajodia, Pierangela Samarati, Maria Luisa Sapino, V. S. Subrahmanian, ``Flexible support for multiple access control policies,"

[5] : comment construire la séparation des taches :http://www.compliancetutorial.com/i/segregation_of_duties_ERP_security_tutorial3934.htm

[6] : E - COMMERCE Content site.nimonweb.com/e-learning/.../E-COMMERCE.doc

[7] : **Introduction au e-Commerce Semaine du 31 mai - 9 Juin** www2.muw.edu/.../introduction_to_ecommerce.doc

[13] : application web Par Jennifer Kyrnin , Guide About.com http://webdesign.about.com/od/web20/g/web-application-definition.htm

[14] : Sécurité des Applications Web —Comment Minimiser les Risques d'Attaques les plus Courants Rapport IBM ISS X-Force sur les tendances et risques pour 2008 http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

[15] : http://securite.developpez.com/faq/?page=dispo **« Les dispositifs de sécurité »**

[16] : Les questions de sécurité et de confidentialité dans le commerce électronique Partie I Introduction et Motivation Peixian LI pl9a@cs.virginia.edu *www.cs.virginia.edu/~pl9a/resume/**ECommerce.doc***

[17] : Ahmed Mehaoua « Cryptographie et services de sécurité ».

[23] : Antivirus software for Linux Une liste d'antivirus qui fonctionnent sous Linux ainsi qu'une mini-FAQ en anglais. http://www.ce.is.fh-furtwangen.de/~link/security/av-linux.php3

[24] : UML pour la sécurité à priori des Applications Web Salim CHEHIDA, Zohra CHERGUI, Fatima KREDOUDA Département d'Informatique, Université de Mostaganem, Algérie.

[25] : Le Processus Unifié de Rational Laurent Henocque ,http://laurent.henocque.free.fr/ Enseignant Chercheur ESIL/INFO France http://laurent.henocque.perso.esil.univmed.fr/ mis à jour en Novembre 2006
[26] : De M-UML vers les réseaux de Pétri « Nested Nets » : Une approche basée transformation de graphes, HETTAB ABDELKAMEL université de Constantine www.umc.edu.dz/theses/informatique/HET5535.pdf
[27] : PHP nuck , Productivity Software Microsoft Office Visio Professional 2013 https://telecharger.phpnuke.org/fr/download-item-view-g-b-g-l-v/microsoft-office-visio-professional.htm

[28] : Groupe Metidji http://www.groupe-metidji.com/historique.php?lg=fr

[29] :Monia LOULOU ALOULOU « Approche Formelle pour la Spécification, la Vérification et le Déploiement des Politiques de Sécurité Dynamiques dans les Systèmes à base d'Agents Mobiles » **Université de Bordeaux 1** ÉCOLE DOCTORALE DE MATHÉMATIQUES ET D'INFORMATIQUE et **Université de Sfax** FORMATION DOCTORALE EN INFORMATIQUE 13 Novembre 2010

[30] : Cas d'utilisation Ivar Jacobson, http://fr.wikipedia.org/wiki/Diagramme_des_cas_d%27utilisation

[31]: H. Zhu and M. Zhou, "Roles in information systems: A survey," *IEEE Trans. Syst. Man Cybern. C: Appl. Rev.*, vol. 38, no. 3, pp. 377–396, May 2008.

[32] : S.CHEHIDA, *« La modélisation des aspects de sécurité avec UML : Elaboration des extensions, d'une démarche et d'un outil »*, Mémoire magister en informatique, Université Abdelhamid Ibn Badiss de Mostaganem, (2010).
[33]: J. Jurjens, « Secure Systems Development with UML: a Foundation », Thèse de doctorat, Munich University of Technology, (2003).

[34]: K. Alghathbar, D. Wijesekera, AuthUML: a three-phased framework to analyze access control specifications in Use Cases, Washington, DC, in: Proceedings of the Workshop on Formal Methods in Security Engineering (FMSE), ACM Press, New York, 2003.

[36]: Y.ELMAZOURI, *« UML : Diagramme de composants, Diagramme de déploiement »*, Cours, Site : www.freewebs.com/fresma , (2006)

[37] : http://www.guill.net , Les attaques d'internet et les moyens de s'en protéger, Programmez ! n°37-« Halte aux intrus ! »-novembre 2001, Sécurité Internet – Stratégie et technologies Solange Ghernaouti-Hélie Dunod

[38] : P.CHAMET, *«Vulnérabilité et sécurisation des applications web : pourquoi les firewalls sont impuissants face à certaines attaques »*

[39] : ANTONIO GONCLAVES, Java EE 6 et GlassFish 3 « Tour d'horizon de Java EE 6 », Pearson Education France, (2010).

[40] : Définition J2EE (Java 2 Platform, Enterprise Edition) http://searchsoa.techtarget.com/definition/J2EE

[41] : Définition de Langage JAVA & JAVA SCRIPT Stagiaires de L' IPETI http://ipeti.forumpro.fr/t21-definition-de-langage-java-java-script**.**

[42] : Introduction à javascript Tout JavaScript.com > Tutoriaux > Introduction à javascript http://www.toutjavascript.com/savoir/savoir00.php3

[43] : BARON Mickaël « Java pour le développement d'applications Web : Java EE, JSF : Java Server Faces », 2007 (Rév. Janvier 2009).

[45] : D.Laurent, *«Module UV java »*, Cours, (2002).

[47] : Kofler,« MySQL 5 guide de l'administrateur et du développeur »

[48] : Serge Tahe « Introduction à Java EE 5 avec Netbeans 6.8 et le serveur d'applications Glassfish V3 » istia.univ-angers.fr juin 2010

Webographie

[8] : http://www.netissime.info/e-commerce/avantages-et-inconvenients-du-commerce-electronique-1406/

[9] : http://www.commentcamarche.net/faq/9668-les-paiements-en-ligne

[10] : http://www.parlonsebusiness.com/quel-moyen-de-paiement-choisir-pour-son-site-e-commerce/

[11] : http://www.commentcamarche.net/contents/secu/secuintro.php3

[12] : https://www.cases.lu/index.php?headingid=47

[18] : http://www.commentcamarche.net/contents/crypto/certificat.php3

[19]: http://www.commentcamarche.net/contents/crypto/ssl.php3 Cryptographie - Secure Sockets Layers (SSL).

[20] : http://www.astrosurf.com/luxorion/piratage-informatique-prevention2.htm

[21] : http://www.astrosurf.com/luxorion/piratage-informatique-prevention2.htm

[22] : http://www.cru.fr/securite/CRUGB/principe.html

[35]: http://www.adullact.org/documents/grc_modelisation_developpement_v1.3

[44] : http://gardeux-vincent.eu/Documents/ProjetJEE/HPV_JSF_Castor/jsf.html

[46] : http://netbeans.org/features/index.html