REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE.

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE.

Mémoire

de fin d'études

En vue l'obtention du diplôme de MASTET II en informatique

Option : Conduite de Projets Informatique

Thème

Conception et réalisation d'une plateforme Test pour l'évaluation de la sécurité informatique des entreprises

Réalisé par :
M^{elle} .IGUERGUIT Ratiba
M^{elle} .ALIANE Hassina

Dirigé par :
M^{r} .SI MOHAMMED. M

Promotion : 2011/2012

Remerciements.

Nous remercions à prime abord DIEU le tout puissant qui nous a donné la force, la volonté et le courage pour accomplir ce modeste travail.

Nos remerciements vont conjointement et tout particulièrement à Monsieur SIMOHAMMED.M, de nous avoir proposé ce sujet de fin d'étude et aussi de nous avoir encadrés. Nous tenons également, à lui exprimer notre profonde reconnaissance pour sa disponibilité à tout moment, ses encouragements, ses conseils ainsi que pour la confiance qu'il a en nous.

Nous adressons nos remerciements aux membres du jury, devant qui nous avons l'honneur d'exposer notre travail, et qui ont pris peine de lire avec soin ce mémoire pour juger son contenu.

Nos sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet, particulièrement nos chères familles et nos amis(es).

Dédicaces

Je dédie ce travail à mon regretté Grand père « Arezki »: en souvenir de ce que tu as fait et ce que tu as été pour moi durant ton existence.

Je sais que tu serais bien content d'apprendre que ta « Hassina» va obtenir un MASTER. Que dieu t'élève au rang de ses illustres amis.

A ma Grand-mère que DIEU la garde pour nous.

À ceux qui sont la source de mon inspiration et de mon courage, à qui je dois de l'amour et de la reconnaissance, mes très chers parents.

A ma grande sœur « Lila » et mes deux frères « Nourdine » et « Toufik » que j'aime énormément.

A mes grands parents maternels, oncles et tantes, cousins et cousines maternels et paternels.

A tous mes amis, surtout mon amie « Ratiba».

A toute la promotion MASTER II Informatique.

A tous ceux qui me connaissent.

Hassina

Dédicaces

Je dédie ce travail à :

La mémoire de ma grand-mère Faroudja,

À ceux qui sont la source de mon inspiration et de mon courage, à qui je dois de l'amour et de la reconnaissance, mes très chers parents.

A mes sœurs « Rachida »et « Cilia » et mes frères «Rachid », « Sofiane » et « Hacene ».

A mes grands parents maternels, oncles et tantes, cousins et cousines maternels et paternels.

A tous mes amis, surtout mon amie « Hassina».

A toute la promotion MASTER II Informatique.

A tous ceux qui me connaissent.

Ratiba

Sommaire

Table des matières :

Chapitre II : La sécurité informatique.

Chapitre III : Analyse & Conception.

Chapitre IV : réalisation & mise en œuvre

Annexe.

La table des figures

La table des figures :

Chapitre I : Introduction aux technologies web.

Chapitre II : La sécurité informatique.

Chapitre III : Analyse & Conception.

Chapitre IV : réalisation & mise en œuvre

Introduction général

Introduction générale

Les systèmes d'information prennent de plus en plus une place stratégique au sein des entreprises. Ainsi la notion du risque liée à ces derniers devient une source d'inquiétude et une donnée importante à prendre en compte, ceci en partant de la phase de conception d'un système d'information jusqu'à son implémentation et le suivi de son fonctionnement.

La sécurité des systèmes d'information représente une tâche à satisfaire par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent d'assurer la gouvernance de son système d'information. Ainsi plusieurs méthodes d'analyse des systèmes informatiques proposent des démarches de certification afin de garantir une image consolidée aux entreprises intégrant les processus de sécurité dans la liste de leurs préoccupations managériales.

Notre travail consiste à concevoir une plateforme test pour aider les entreprises à évaluer la sécurité informatique de leurs organisations à travers des questions type.

Avant de passer à l'implémentation de notre application il est évident de définir quelques concepts de base, pour cela nous avons opté pour le plan suivant :

- Le premier chapitre intitulé « Introduction aux technologie web », présente quelques notions de base concernant les réseaux, l'internet et le modèle Client/serveur.
- Le deuxième chapitre qui s'intitule « La sécurité informatique », introduit les notions de base de la sécurité informatique, objectifs, domaines d'application, la notion de politique de sécurité et quelques outils de sécurité.
- Le troisième chapitre qui s'intitule « Analyse et conception », retracera les différentes étapes que nous avons suivies afin de réaliser l'implémentation de notre application.
- En fin le quatrième chapitre qui porte sur la réalisation et la mise en œuvre de l'application est une illustration graphique de certaines fonctionnalités et les outils avec lesquels nous avons développé.

Chapitre I

Introduction aux technologies web

I.1. Introduction : **[01]**

Lorsque nous travaillions sur une même machine, toutes les informations nécessaires au travail étaient centralisées sur celle-ci. Presque tous les utilisateurs et les programmes avaient accès à ces informations. Pour des raisons de coûts ou de performances, nous sommes venus à multiplier le nombre de machines. Les informations devaient alors être dupliquées sur les différentes machines du même site. Cette duplication était plus ou moins facile et ne permettait pas toujours d'avoir des informations cohérentes sur les machines. Nous sommes donc arrivés à relier d'abord ces machines entre elles; ce fût l'apparition des réseaux locaux. Après nous avons éprouvé le besoin d'échanger des informations entre des sites distants, il a donc été nécessaire de développer de nouveaux moyens d'échange adaptés à l'évolution de ces besoins, à la base desquels nous trouvons les réseaux moyenne et longue distance. Aujourd'hui, les réseaux se retrouvent à l'échelle mondiale. Le besoin d'échanger de l'information est en pleine évolution.

Ce chapitre a pour objectif de présenter quelques notions sur les réseaux informatiques en premier lieu, puis donnera un aperçu sur l'Internet et ses différents services.

I.2. Les réseaux informatiques :

I.2.1. Définition : [02]

D'une manière générale, un réseau est un ensemble de nœuds qui s'interconnectent par des arcs. Dans un réseau informatique les nœuds sont des machines (unités de calcul, périphériques) et les arcs sont des liaisons de transmission de données, d'où un réseau informatique est un ensemble de moyens informatiques (logiciels et matériels) mis en œuvre pour assurer une communication entre eux. Les éléments de réseau sont reliés entre eux par des câbles (coaxial, torsadé,…) ou des ondes hertziennes (wifi, Wi Max,…), selon le type des réseaux :

- ✓ ***Les réseaux de type filaire* :** c'est un ensemble d'hôtes (ordinateurs par exemple) reliés soit directement par des liaisons filaires, soit via un sous réseau de communication (ou réseaux de communication).
- ✓ ***Les réseaux sans fils :*** ce sont des réseaux filaires dans lesquels au moins une liaison filaire (câbles, fibres optiques) est remplacée par une liaison radio, permettant ainsi la mobilité de l'ordinateur concerné par cette liaison (exemple: réseaux personnels ou "Bluetooth", réseaux Ad Hoc).

- ***I.2.2. Un bref historique : [03]***

Les ordinateurs n'ont pas été créés pour communiquer. Leur fonction première est de calculer, et leur fonction secondaire de stocker l'information. Les réseaux informatiques sont donc nés bien après les ordinateurs et étaient très différents à leurs balbutiements de ce que nous utilisons sans même y penser aujourd'hui.

Dans les années 70, les ordinateurs individuels n'existaient pas et donc le besoin de communiquer non plus car, sur un mainframe, tous les terminaux sont reliés à la même unité centrale, l'information n'a donc pas besoin d'être transmise puisque tout le monde y a accès. Les seuls réseaux existant à cette période reliaient les systèmes centraux situés sur des sites différents, ce dont seuls les états et les grandes entreprises avaient réellement besoin.

C'est avec l'arrivée des ordinateurs personnels dans les années 80 que les données se sont bientôt retrouvées éparpillées aux quatre coins d'une multitude de systèmes et qu'il est devenu nécessaire de relier ces systèmes pour partager à nouveau l'information.

I.2.3. Les constituants matériels d'un réseau local [04]:

I.2.3.1. Carte réseau :

La fonction réseau est soit intégrée sur la carte mère, soit ajoutée à l'aide d'une carte additionnelle. La partie câblage vers le réseau est aujourd'hui majoritairement constituée d'un connecteur RJ45. Précédemment, nous pouvions rencontrer d'autre type de prise (BNC ou AUI). La principale caractéristique de ces cartes est la vitesse de communication (10, 100 ou 1000Mbps) ainsi que le mode de communication (half ou full duplex). La carte peut être équipée d'une Eprom (Boot-Prom) lui permettant de booter sur le réseau. Chaque carte réseau dispose d'une adresse unique (adresse MAC).

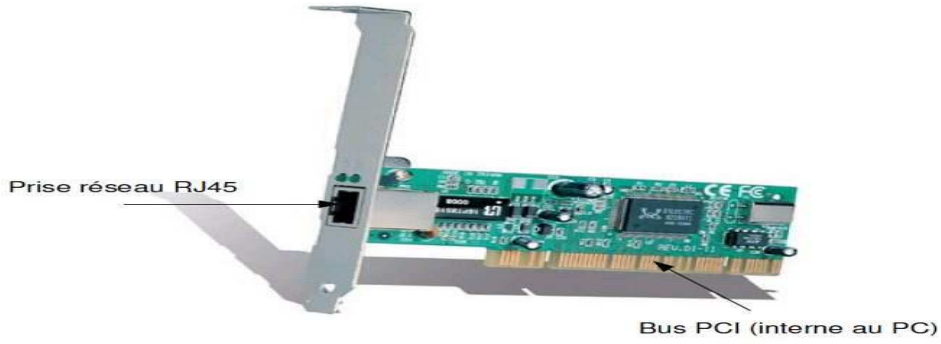


Figure I.1: Carte réseau.

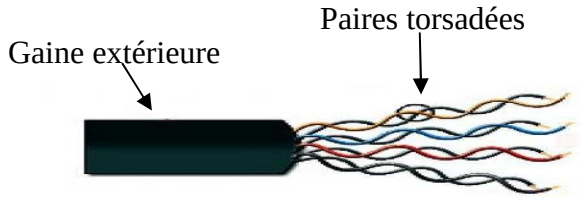
I.2.3.2. Câbles réseaux :

Les câbles réseaux permettent de relier entre eux des équipements afin de les faire communiquer. Ils doivent être adaptés en fonction des équipements en place (prise, vitesse, longueur, norme). La longueur maximale pour les câbles "RJ45" est de 100 mètres. Les câbles droits permettent de relier un périphérique (PC, imprimante) à un commutateur ou un concentrateur, les câbles croisés sont utilisés pour relier deux PC entre eux.

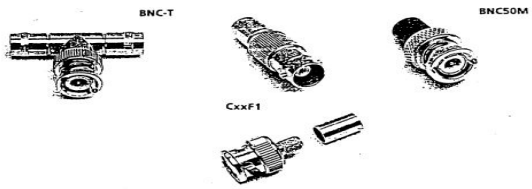
Les anciens câbles (autre que "RJ45") faisaient appel à un type de câblage particulier.

Câble équipé de prises RJ45 :

Ce câble est constitué de 8 fils de cuivre sous forme de 4 paires torsadées.



Câble coaxial avec prises BNC :



I.2.3.3. Equipements d'interconnexion :

Cela comprend tous les équipements permettant de relier entre eux les différents éléments d'un réseau.

Les principaux équipements sont :

1. ***Le répéteur :***

Le répéteur est une machine qui permet de connecter deux groupes d'ordinateurs qui sont trop éloignés l'un de l'autre. Il régénère (amplifie) les signaux du réseau de sorte qu'ils puissent circuler sur une plus longue distance.

2. ***Le concentrateur (HUB) :***

Le HUB est un boîtier qui a la fonction de répéteur, mais sa fonction principale est de connecter plusieurs lignes en une seule. Le HUB se comporte comme un bus auquel se connectent plusieurs stations ce qui fait que toute information qui y arrive est réellement reçue par toutes les stations qui sont connectées mais seule la machine concernée qui la traite.

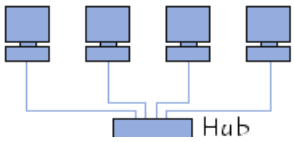


Figure I.2: Machines reliées par un HUB.

3. Le commutateur (Switch):

Un commutateur est un HUB plus performant. La différence entre ces deux est que le commutateur fait suivre les données qu'il reçoit uniquement au port connecté à l'ordinateur destinataire des informations contrairement au HUB. Plusieurs communications simultanées peuvent avoir lieu à condition qu'elles concernent des ports différents du commutateur.

4. Le pont (bridge):

Un pont est utilisé avec le but de partitionner un grand réseau en deux plus petits pour une question de performance. Un pont est une espèce de répéteur intelligent, il sait écouter le réseau et détecter automatiquement l'adresse des deux ordinateurs en communication. Son principe général est de ne pas faire traverser l'information si l'émetteur et le destinataire sont du même coté.

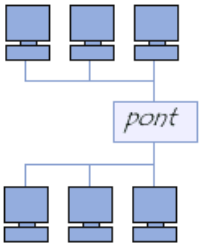


Figure I.3: Machines reliées par un pont.

5. Le routeur :

Un routeur est une sorte de pont super-intelligent car il connait non seulement les adresses de chacun des ordinateurs mais aussi celles des autres routeurs du réseau et peut choisir le chemin le plus rapide pour envoyer un message. Les routeurs disposent d'une fonctionnalité supplémentaire qui leur permet d'identifier le type du message envoyé.

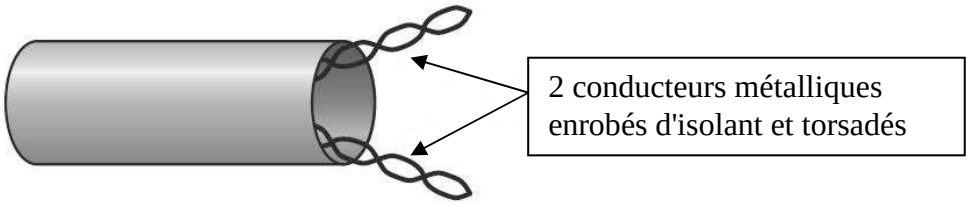
I.2.4. Les supports de transmission : [05]

Le support de transmission désigne le type du câblage utilisé pour relier l'ensemble des nœuds entre eux. Cet élément est d'une importance capitale car c'est de lui que dépendent, pour une très grande partie les performances du réseau.

Les supports de transmission les plus utilisés sont :

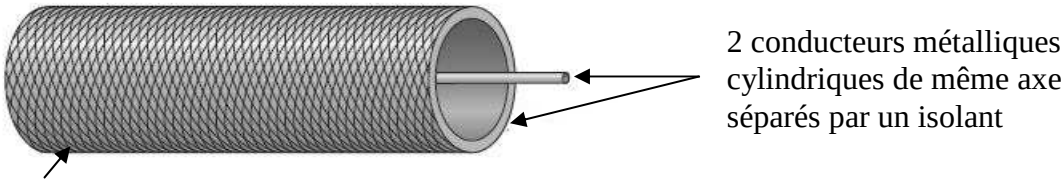
1. Câble à paires torsadées :

Une paire torsadée se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal.



2. Câble coaxial :

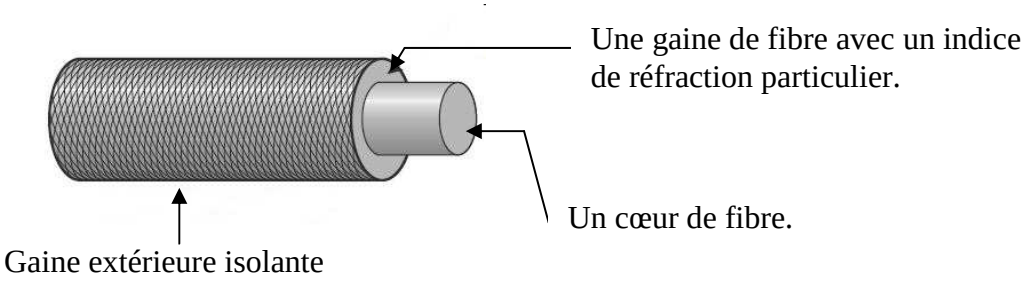
Fil conducteur mono ou multi brins, entouré d'un isolant et disposé dans l'axe d'un tube conducteur.



Gaine extérieure isolante (blindée ou non).

3. Fibre optique (FDDI : Fiber Date Distribution Interface) :

Une fibre optique est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre.



I.2.5. Objectifs des réseaux : [06]

Les principaux objectifs des réseaux sont :

- *Accès centralisé à Internet* : Un seul routeur, un seul abonnement, et tous les postes autorisés ont accès à l'internet grâce au réseau, pour la navigation, la messagerie etc.
- *Partage de ressources (matérielles, logicielles, données) :*
  - La mise en commun des ressources matérielles (imprimantes, espace disque, périphériques coûteux ou calculateurs puissants) utilisées épisodiquement est une motivation à la mise en réseau.
  - La mise en commun de ressources logicielles procède de la même logique, une licence logicielle, comme une imprimante, peut être partagée. Ces deux techniques engendrent une économie de moyens.
  - La mise en commun des données est un point essentiel au bon fonctionnement d'une organisation, car la centralisation et le partage de l'information permettent d'éviter les incohérences et la duplication.
- *Sauvegarde automatique des fichiers critiques* : il est toujours essentiel de conserver des copies de sauvegarde des fichiers importants. Il est possible d'automatiser cette procédure par recours à un programme assurant la sauvegarde des fichiers. Sans réseau, il est nécessaire d'effectuer manuellement les copies des fichiers, ce qui demande du temps.
- *La meilleure solution de partage est un serveur :* Il s'agit d'un ordinateur autonome et puissant, capable de contenir, de traiter une grande quantité d'information et de les distribuer à un grand nombre d'utilisateurs en même temps. Ces utilisateurs sont appelés clients. Le serveur règlemente également les accès des utilisateurs en fonction de leurs droits, selon la politique de sécurité. Ceci afin que les données restent confidentielles et soient accessibles ou modifiables seulement par les personnes concernées.

I.2.6. Topologie des réseaux : [07]

Il existe différentes topologies, selon la façon dont les matériels sont connectés entre eux :

1. La topologie en bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par

l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

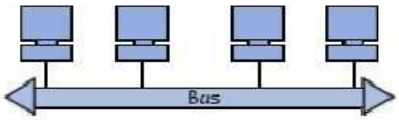


Figure I.4. Topologie en bus.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau est affecté.

2. La topologie en anneau :

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

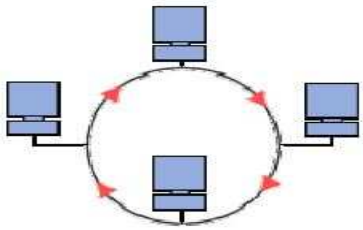


Figure I.5: Topologie en anneau.

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé *MAU, Multistation Access Unit*) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole.

3. La topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais *hub*, littéralement *moyen de roue*). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseaux en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

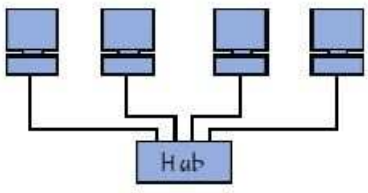


Figure I.6: Topologie en étoile.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

4. Topologie en arbre :

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connecté à plusieurs nœuds de niveau inférieur, dans la hiérarchie.

Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

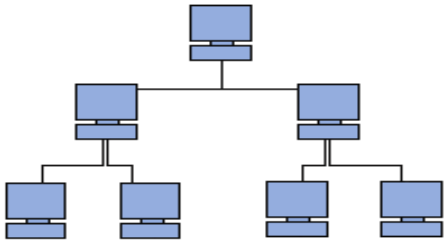


Figure I.7: Topologie en arbre.

5. Topologie maillée :

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties. L'armée utilise également cette topologie, ainsi, en cas de rupture d'un lien, l'information peut quand même être acheminée. Elle existe aussi dans le cas de couverture Wifi. On parle alors bien souvent de topologie Mesh mais ne concerne que les routeurs Wifi.

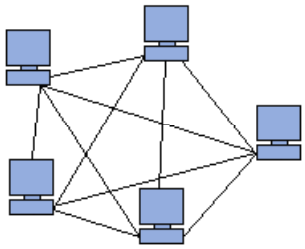


Figure I.8: Topologie maillée.

I.2.7. Type des réseaux : [08]

En fonction de la surface de couverture des ordinateurs connectés, les réseaux sont classés comme suit :

1. ***Les réseaux personnels (PAN : Personal Area Network) :***

Un réseau personnel Interconnecte sur quelques mètres des équipements personnels tels que les téléphones portables, PDA, etc.…

Technologies :

Bluetooth, Infrarouge.

2. ***Réseau local (LAN: Local Area Network):***

Un réseau local s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau.

Il est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10Mbps (pour un réseau Ethernet par exemple) et 1Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

Technologies :

Ethernet, Wifi.

3. ***Réseau métropolitain (MAN : Metropolitan Area Network) :***

Un réseau métropolitain interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

Technologies :

ATM, WI-MAX

4. Réseau étendu (WAN: Wide Area Network):

Un réseau étendu interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

Technologies :

MPLS.

I.2.8. Architecture des réseaux :

Pour assurer la connexion d'une machine, il faut réunir les supports physiques, mais pour assurer le bon transfert de l'information avec une qualité de service suffisante, il faut prévoir une architecture logicielle. Il existe deux grands modèles d'architectures réseaux, le premier est le modèle OSI "Open System Interconnections" et le second est le modèle TCP/IP « Transmission Control Protocol/Internet Protocol ».

I.2.8.1. Modèle OSI des réseaux informatiques : [09]

OSI signifie (**O**pen **S**ystem **I**nterconnections), Ce modèle a été mis en place par l'ISO (International Standard Organisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Ce modèle est un réseau basé sur un découpage en sept couches chacune de ces couches correspondantes à une fonctionnalité particulière d'un réseau. Les couches 1, 2, 3 et 4 sont dites basses et les couches 5, 6 et 7 sont dites hautes, et il fonctionne de façon que, chaque couche (n) offre un certain nombre de services à la couche (n+1) en déroulant un protocole uniquement défini à partir des services fournis par la couche (n-1). Le concept de l'OSI nécessite la compréhension de 3 concepts :

1. Le service : Ensemble d'événements et primitives pour se rendre du niveau (n) au niveau (n+1).

2. Le protocole : Ensemble de règles nécessaires pour réaliser un service.

3. Le point d'accès à un service : Point situé à la frontière entre les couches (n) et (n+1).

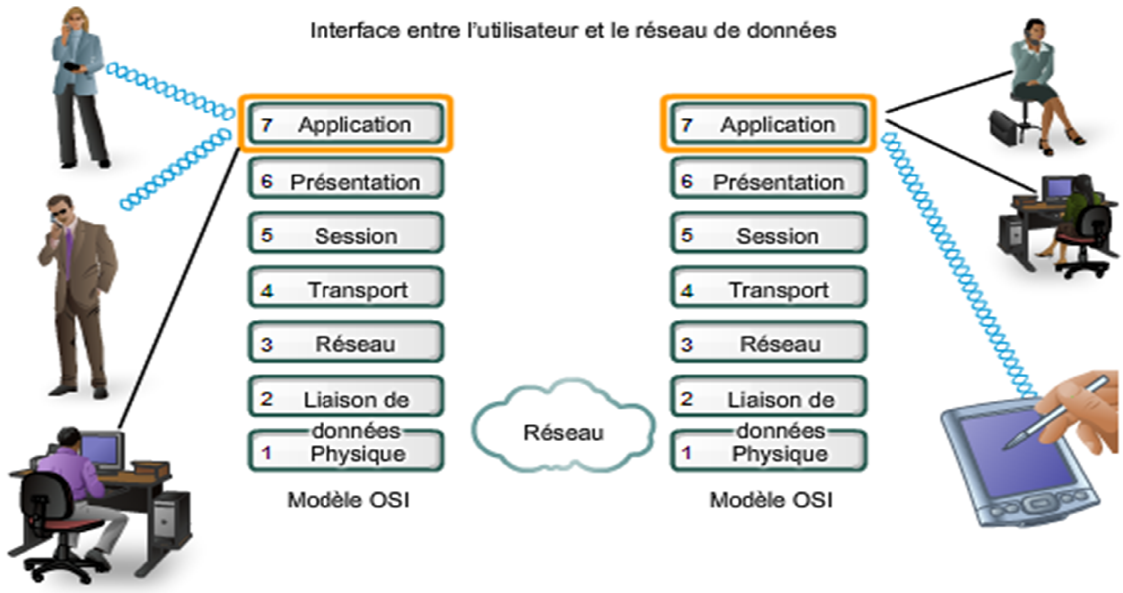


Figure I.9: Les couches du modèle OSI.

I.2.8.1.1. Les couche du modèle OSI :

- ***La couche physique :***

Cette couche offre les services de l'interface entre l'équipement de traitement informatique (ordinateur ou terminal) et le support physique de transmission. L'unité de transfert gérée par cette couche est l'information élémentaire binaire.

- ***La couche liaison de données*** :

Elle définit la manière dont les informations sont échangées entre deux matériels directement connectés par un même support physique.

La trame est l'entité transportée sur les lignes physiques. Elle contient un certain nombre d'octets transportés simultanément. Le rôle du niveau trame consiste à envoyer un ensemble d'éléments binaires sur une ligne physique de telle façon qu'ils puissent être récupérés correctement par le récepteur.

- ***La couche réseau :***

Elle doit permettre d'acheminer correctement les paquets d'information qu'elle traite jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaires ou par des passerelles, qui interconnectent deux ou plusieurs réseaux.

- ***La couche transport :***

Elle prend en charge l'acheminement des informations (messages) de bout en bout via le réseau et le transport de ce message de l'utilisateur d'une extrémité à une autre du réseau.

- ***La couche session :***

Le rôle du niveau session est de fournir aux entités de présentation les moyens nécessaires à l'organisation et à la synchronisation de leur dialogue. À cet effet, la couche 5 fournit les services permettant l'établissement d'une connexion, son maintien et sa libération, ainsi que ceux permettant de contrôler les interactions entre les entités de présentation.

- ***La couche présentation :***

Le niveau présentation se charge de la syntaxe des informations que les entités d'application se communiquent. Deux aspects complémentaires sont définis dans la norme :

- ✓ La représentation des données transférées entre entités d'application.
- ✓ La représentation de la structure de données à laquelle les entités se réfèrent au cours de leur communication et la représentation de l'ensemble des actions effectuées sur cette structure de données.

- ***La couche application :***

C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle fournit aux processus applicatifs le moyen d'accéder à l'environnement réseau. Ces processus échangent leurs informations par l'intermédiaire des entités d'application.

I.2.8.1.2. Le modèle TCP/IP : [10]

Le modèle TCP/IP s'est développé d'une façon plus empirique que le modèle OSI. Il désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

I.2.8.1.2.1. Les couches de modèle TCP/IP : [10]

- ***La couche application :***

Elle assure l'interface des applications utilisatrices avec la pile des protocoles, par exemple Tel Net (Connexion à un ordinateur distant), FTP (File Transfert Protocol).

- ***La couche transport :***

Elle établit la communication entre processus, elle assure la communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le récepteur. L'identification des processus communiquant ce fait par des ports au niveau de cette couche.

Cette couche supporte deux protocoles suivant le mode de communication, le protocole UDP et TCP.

- ***La couche routage :***

Elle fournit une adresse logique pour chaque interface physique telle que chaque ordinateur du réseau dispose d'une adresse IP (Internet Protocole) unique. Elle s'occupe aussi du routage des paquets entre les hôtes.

- ***La couche accès réseaux (physique) :***

C'est la couche la plus basse, elle représente la connexion physique avec les câbles, les circuits d'interface électrique et les protocoles d'accès aux réseaux. Elle est constituée d'un driver, d'un système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.

I.2.8.1.2.2. Les protocoles de modèle TCP/IP :

TCP/IP fait appel à plusieurs protocoles qui diffèrent selon la couche sur laquelle ils agissent. Cela est illustré dans la figure suivante :

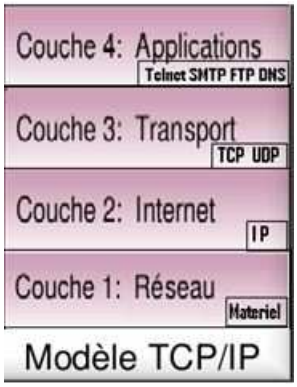


Figure I.10:Les couches du modèle TCP/IP.

Les différents protocoles auxquels fait appel cette architecture sont brièvement définis ci-dessous :

- ***IP* :** Qui signifie Internet Protocol, C'est le protocole dont on parle le plus, il est en effet directement impliqué dans la configuration réseau de l'hôte. Il reçoit les données sous forme de paquets pour les acheminer dans le réseau vers leurs destinations grâce à des algorithmes de routages et cela en utilisant un mode sans connexion.
- ***TCP* :** (qui signifie *Transmission Control Protocol*, soit en français : *Protocole de Contrôle de Transmission*) est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule

dans des datagrammes IP, en fixant le champ protocole à 6 (Pour savoir que le protocole en amont est TCP...). TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission. Les caractéristiques principales du protocole TCP sont les suivantes :

- ✓ TCP permet de remettre en ordre les datagrammes en provenance du protocole IP.
- ✓ TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau.
- ✓ TCP permet de formater les données en segments de longueur variable afin de les remettre au protocole IP.
- ✓ TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne.
- ✓ TCP permet enfin l'initialisation et la fin d'une communication de manière courtoise.

- ***UDP (User Datagram Protocol):*** agit également sur la couche transport. Il possède les mêmes fonctionnalités que le TCP à la différence de fonctionner en mode sans connexion.
- ***Telnet :*** sert à se connecter à une machine à distance. Il permet d'y travailler de la même manière que devant la machine elle-même.
- ***FTP (File Transfer Protocol) :*** est un Protocole qui permet d'assurer le transfert de fichiers de façon indépendante des spécificités des NOS (Network Operating System, pour mémoire). Ainsi, un client FTP sous Windows peut télécharger un fichier depuis un serveur UNIX.
- ***SMTP (Simple Mail Transfer Protocol)* :** permet d'échanger du courrier entre deux serveurs de messagerie. Ce protocole est complètement transparent pour l'utilisateur, les serveurs se chargeant entre eux de transférer correctement les données.
- ***DNS (Domain Name Service) :*** service de nom de domaine. Il permet de convertir le nom d'une machine en une adresse réseau (ou IP) et vice versa.

I.3. Internet :

I.3.1. Définition :

Internet signifie réseaux interconnectés (*interconnected networks)*.Constitue un réseau de réseau qui relie dans le monde entier des ordinateurs en utilisant un protocole de transmission et de communication, constituant un langage commun permettant la connexion de toutes les machines (PC, Mac, Unix).

Ce langage s'appelle : Transmission Control Protocol / Internet Protocol (**TCP-IP).** L'internet permet aux utilisateurs connectés au réseau de communiquer ainsi que d'échanger les informations et les données (image, voix, vidéo, Base de donnée, page web,…).

Pour accéder à l'internet, il faut impérativement réunir les trois conditions suivantes :

- ✓ Un ordinateur géré par un système d'exploitation qui supporte le protocole de communication internet TCP/IP (Transmission Control Protocole/Internet Protocole).
- ✓ Une carte réseau ou un MODEM correctement installé, configuré et relié au réseau téléphonique.
- ✓ Disposer d'un abonnement auprès d'un fournisseur d'accès.

Sous réserve de remplir les trois conditions citées, il suffit à présent de lancer un navigateur pour voyager à travers internet même si deux autres petites conditions restent à satisfaire: entrer le nom d'utilisateur et le code d'accès à internet que le fournisseur d'accès a attribués.

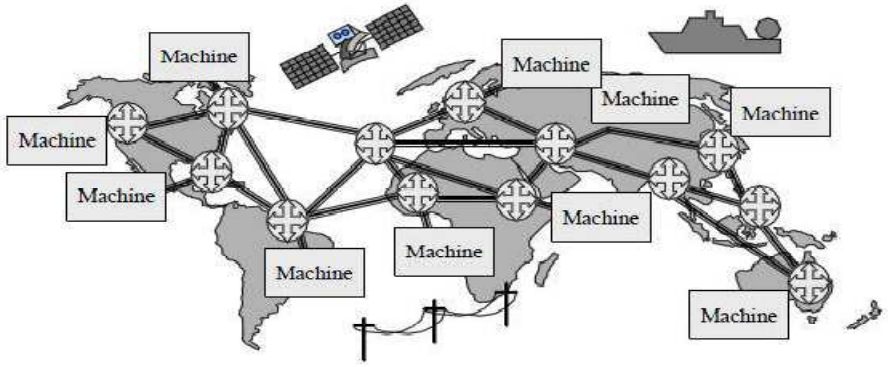


Figure I.11: La toile d'Internet.

I.3.2. Historique : [11]

Au milieu des années 60 le réseau ARPANET a été conçu par la DARPA (Defense Advanced Research Project Agency) le département américaine de la Défence, le but était de développer un réseau à commutation de paquets pour relier ses centres de recherches dans le but de partager des équipements informatiques, échanger des données, du courrier et aussi pour concevoir un réseau résistant à des attaques militaires. Il ne fallait donc pas qu'il comporte de points névralgiques dont la destruction aurait entraîné l'arrêt complet du réseau. C'est ainsi, que dès le départ le réseau ARPANET fut conçu sans nœud particulier le dirigeant, et de telle sorte que si une voie de communication venait à être détruite, alors le réseau soit capable d'acheminer les informations par un autre chemin.

C'est vers 1980 qu'est apparu le réseau Internet, tel qu'on le connaît maintenant, lorsque la DARPA commença à faire évoluer les ordinateurs de ses réseaux de recherche vers les nouveaux protocoles TCP/IP et qu'elle se mit à subventionner l'université de Berkeley, pour qu'elle intègre TCP/IP à son système d'exploitation Unix (BSD). Ainsi la quasi totalité des départements d'informatique des universités américaines ont pus commencer à se doter de réseaux locaux qui en quelques années seront interconnectés entre eux sous l'impulsion de la NSF (National Science Foundation).

Même si dès son origine Internet comprenait des sociétés privées, celles-ci étaient plus ou moins liées à la recherche et au développement, alors qu'à l'heure actuelle les activités commerciales s'y sont considérablement multipliées, et ceci surtout depuis l'arrivée du Web en 1993. Comme l'ensemble des protocoles TCP/IP n'est pas issu d'un constructeur unique, mais émane de la collaboration de milliers de personnes à travers le monde, une structure de fonctionnement originale a été imaginée dès le début.

I.3.3. Les services de l'Internet : [12]

Avant, pour pouvoir utiliser Internet nous devons apprendre à utiliser un système très complexe, contrairement aujourd'hui, il existe de nombreuses applications facilitant son utilisation telle que :

- ***Le world wide web (www)*** : C'est la partie qui marque le plus grand succès et la renommée d'Internet grâce à son aspect graphique et interactif qui permet d'accéder à des documents textes, images, sons, et vidéos en prévenant de milliers de sites web en allant d'une page à une autre par la grâce des liens hypertextes.
- ***Le courrier électronique e-mail*** : Echange de courrier via des boites aux lettres électroniques entre ordinateurs reliés à Internet.
- ***Le chat*** : Discuter en temps réel avec une ou plusieurs personnes au même temps.
- ***La visioconférence*** : discuter avec le son et l'image avec d'autres personnes en temps réel.
- ***Les forums UseNet*** : C'est une participation via Internet à des groupes d'études et de réflexion sur des sujets d'Internet communs.
- ***Le transfert de fichiers*** : Accès aux archives Internet pour télécharger notamment des logiciels gratuits.

I.4. INTRANET : [07]

Un intranet est un ensemble des services Internet (par exemple un serveur Web) interne à un réseau local, c'est à dire accessible uniquement à partir des postes d'un réseau local et invisible de l'extérieur. Il consiste à utiliser les standards clients serveurs de l'Internet(en utilisant les protocoles TCP/IP). Un intranet repose généralement sur une architecteur à trois niveaux, composée :

- ✓ De clients (navigateur internet généralement) ;
- ✓ D'un ou plusieurs serveurs d'application (middleware): un serveur web permettant d'interpréter des scriptes (PHP) ou autres, et les traduire en requêtes SQL afin d'interroger une base de données ;
- ✓ D'un serveur de base des données.

De cette façon, les machines clientes gèrent l'interface graphique, tandis que les différents serveurs manipulent les données. Le réseau permet de véhiculer les requêtes et les réponses entre clients et serveurs.

I.5. EXTRANET : [07]

Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé (authentification par nom d'utilisateur et mot de passe) dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. De cette façon, un extranet, n'est ni un intranet, ni un site Internet, il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise.

I.6. L'Intranet et l'Extranet : [07]

La notion d'Intranet ou **B2E** (Business to Employee) désigne les technologies du web utilisées à l'intérieur d'une entreprise. Ainsi on parle de réseau intranet pour désigner l'ensemble des informations partagées consultables par les employés grâce à un navigateur web. Tandis qu'Extranet ou B2B (Business to Business), moins répandu, désigne un élargissement de l'Internet aux clients ou fournisseur de l'entreprise.

I.7. L'architecture client/serveur : [13]

I.7.1. Définition :

De nombreuses applications fonctionnent selon un environnement Client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que

des fichiers, une connexion, etc. Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur.

I.7.2. Notions de bases :

- ✓ *Client :* C'est le processus demandant l'exécution d'une opération à un autre processus par envoi d'un message contenant le descriptif de l'opération à exécuter et attendant la réponse à cette opération par un message en retour.
- ✓ *Serveur :* C'est un processus accomplissant une opération sur demande d'un client.
- ✓ *Requête :* C'est un message transmis par un client à un serveur décrivant l'opération à exécuter pour le compte d'un client.
- ✓ *Réponse :* C'est un message transmis par un serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'opération.
- ✓ *Middleware :* C'est le logiciel qui est au milieu assure les dialogues entre les clients et les serveurs souvent hétérogènes.

I.7.3. Fonctionnement d'un système client/serveur :

Un système client/serveur fonctionne selon le schéma suivant :

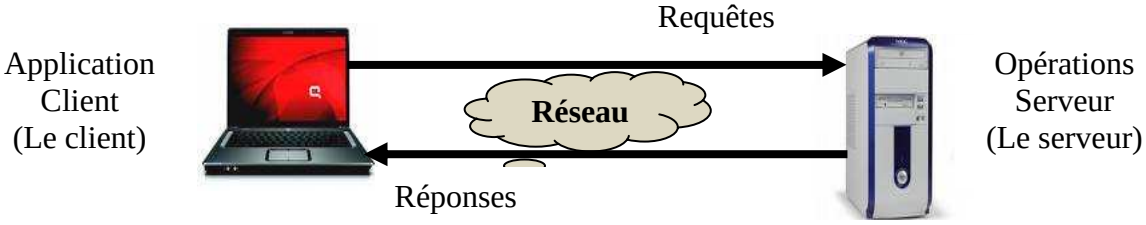


Figure I.12 : fonctionnement du client/serveur.

- Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

I.7.4. Types d'architectures Client – Serveur :

I.7.4.1. Architecture à 2 niveaux :

L'architecture à deux niveaux (aussi appelée *architecture 2-tiers, tier* signifiant *rangée* en anglais) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela

signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.

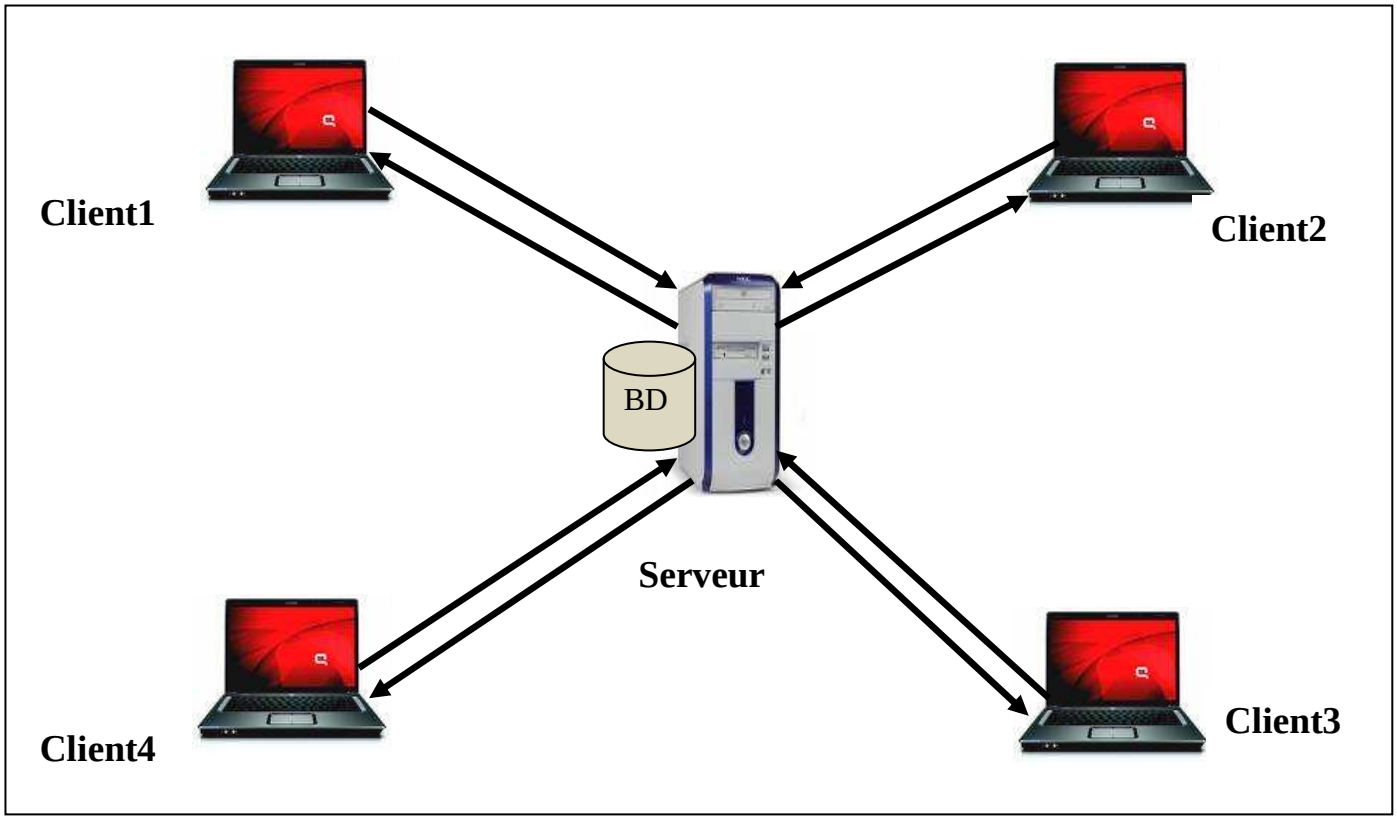


Figure I.13: Architecture à 2 niveaux

I.7.4.2. Architecture à 3 niveaux :

Dans l'architecture à 3 niveaux (appelée *architecture 3-tier*), il existe un niveau intermédiaire, c'est-à-dire que nous avons généralement une architecture partagée entre :

- ✓ Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web) chargée de la présentation ;
- ✓ Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur ;
- ✓ Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

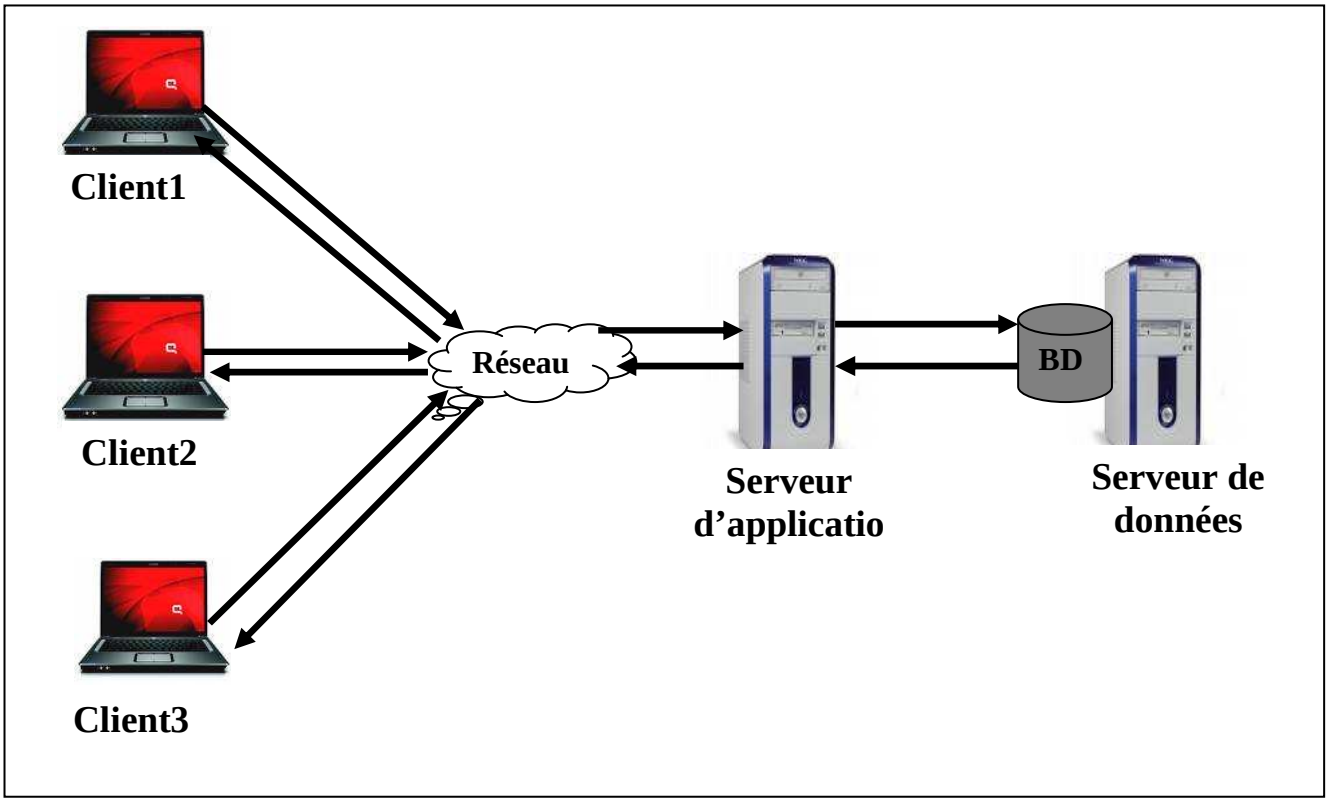


Figure I.14: Architecture à 3 niveaux.

I.7.5. Comparaison des architectures à deux et trois niveaux :

L'architecture à deux niveaux est donc une architecture client/serveur dans laquelle le serveur est polyvalent, c'est-à-dire qu'il est capable de fournir directement l'ensemble des ressources demandées par le client.

Dans l'architecture à trois niveaux par contre, les applications au niveau serveur sont délocalisées, c'est-à-dire que chaque serveur est spécialisé dans une tâche (serveur web/serveur de base de données). L'architecture à trois niveaux permet :

- ✓ Une plus grande flexibilité/souplesse ;
- ✓ Une sécurité accrue, car la sécurité peut être définie indépendamment pour chaque service et à chaque niveau ;
- ✓ De meilleures performances, étant donné le partage des tâches entre les différents serveurs.

I.8. Conclusion :

Au cours de ce chapitre, nous avons présenté la notion des réseaux informatiques qui sont un moyen pour minimiser les coûts de transport des informations et d'augmenter les performances des systèmes, ensuite nous avons parlé des architectures OSI et TCP/IP, ainsi que l'internet et son objectif pour réaliser un système d'information interne à une organisation ou une entreprise.

Enfin nous avons illustré le paradigme client/serveur, son fonctionnement et les différentes architectures possibles.

Pour assurer le bon fonctionnement de l'organisation nous avons besoin de la sécurité des données qui circulent à l'intérieur de cette dernière, qui sera le but du prochain chapitre.

Chapitre II

La sécurité informatique

II.1. Introduction : [WEB 01]

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise à internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnes sont amenés à transporter une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les objectifs de sécurité à atteindre.

II.2. Définition de la sécurité informatique : [14]

La sécurité informatique c'est l'ensemble des moyens, outils, techniques et méthodes mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

II.3. Les objectifs de la sécurité informatique :

La sécurité informatique vise généralement cinq principaux objectifs :

- ***L'intégrité :*** qui assure que la donnée reçue est la même que celle qui a été émise, c'est à dire qu'elle n'a pas été corrompue.
- ***La confidentialité :*** qui assure que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de traiter la donnée.
- ***La disponibilité :*** qui assure que la donnée est présente et accessible à tout moment.
- ***La non-répudiation :*** qui permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire.
- ***L'authentification :*** consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

II.4. Les notions de base de la sécurité informatique : [15]

II.4.1. Les menaces :

Une menace informatique représente le type d'actions susceptibles de nuire dans l'absolu à un système informatique. En termes de sécurité informatique les menaces peuvent être le résultat de diverses actions en provenance de plusieurs origines :

- ***Origine opérationnelle:***

Ces menaces sont liées à un état du système à un moment donné. Elles peuvent être le résultat d'un bogue logiciel (Buffer Overflows, format string …etc.), d'une erreur de conception dans le logiciel ou le matériel, erreur de fonctionnement dans le matériel.

- ***Origine physique:***

Elles peuvent être d'origine accidentelle, naturelle ou criminelle. On peut citer notamment les Catastrophes naturelles, les pannes ou casses matérielles, le feu ou les coupures électriques.

- ***Origine humaine:***

Ces menaces sont associées seulement aux erreurs humaines, que ce soit au niveau de la conception d'un système d'information ou au niveau de la manière dont on l'utilise. Ainsi elles peuvent être le résultat d'une erreur de conception ou de configuration comme d'un manque de sensibilisation des utilisateurs face au risque lié à l'usage d'un système informatique.

II.4.2. La vulnérabilité : [16]

La vulnérabilité est une faille dans les actifs (les équipements, les matériels, les logiciels, les processus, etc..), les contrôles techniques de sécurité ou les procédures d'exploitation ou d'administration utilisés dans un réseau. Elle consiste en une faiblesse dans la protection du système, sous la forme d'une menace qui peut être exploitée pour intervenir sur l'ensemble du système, ou d'un intrus qui s'attaque aux actifs. Elles peuvent être de plusieurs origines :

1. Les vulnérabilités organisationnelles :

- Manque de ressources humaines et de personnels qualifiés.
- Manque d'information des utilisateurs : même si des procédures de sécurité des systèmes d'information et de communication existent, souvent les utilisateurs et les gestionnaires des systèmes semblent ne pas en avoir connaissance.
- Absence de contrôles périodiques, documents de procédures adaptés à l'entreprise et moyens adaptés aux risques encourus.
- Mauvaise utilisation des moyens en place : même si des règles ont été mises en place au niveau de la gestion des accès (mot de passe), l'absence de contrôles effectifs a pour conséquence beaucoup d'utilisateurs ayant tendance à ne pas changer leur mot de passe et à en utiliser certains de type « faibles».

2. Les vulnérabilités physiques :

- Manque de ressources au niveau équipement.
- Accès aux salles informatiques non sécurisé.
- Absence ou mauvaise stratégie de sauvegarde de données.

3. Les vulnérabilités technologiques :

- Failles nombreuses dans les services et applicatifs Web et les bases de données.
- Pas de mises à jour des systèmes d'exploitation et des correctifs.
- Pas de contrôles suffisants sur les logiciels malveillants.
- Récurrence des failles et absence de supervision des événements.
- Réseaux complexes, non protégés.
- Mauvaise utilisation de la messagerie.

II.4.4. Les principales attaques:

Avant d'illustrer les déférentes attaques, nous abordons la différence entre accident et malveillance.

- ***Accident :*** Cette catégorie regroupe tous les sinistres comme les incendies, dégâts des eaux, explosions, catastrophes naturelles, etc. Certains de ces risques ne peuvent être raisonnablement pris en compte (par exemple, un effondrement causé par la présence d'une ancienne carrière souterraine), d'autres peuvent être prévenus ou combattus (par exemple, un incendie), l'informatique n'étant alors qu'un des aspects du problème.
- ***Malveillance*** **:** que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation de données ou de leurs supports, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données.

Les attaques se divisent, selon leurs types en quartes catégories :

1. Les attaques par programmes malveillants :

Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire un système informatique. Vous pouvez récupérer un malware via :

- Une pièce-jointe dans un mail ;
- L'échange de clés USB ;
- Le téléchargement de logiciels.
- Etc.

Voici quelques exemples de programmes malveillants :

- ***Virus : [17]***

C'est un programme informatique qui se réplique par lui-même au sein d'un même ordinateur en infectant d'autres fichiers, c'est-à-dire en se cachant dans leur code. Il s'exécute lorsque nous allons ouvrir ou exécuter le fichier.

- ***Vers : [WEB 02]***

Un ver informatique est un programme malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

Contrairement à un virus informatique, un ver n'a pas besoin d'un programme pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

- ***Cheval de Troie : [WEB 02]***

Un cheval de Troie est un programme d'apparence légitime conçu pour exécuter de façon cachée des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

- ***Logiciel espion : [WEB 02]***

Un logiciel espion est un programme malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. Un logiciel espion est généralement composé de trois mécanismes distincts: Infection, collecte et transmission.

- ***Rootkit : [WEB 02]***

Un rootkit ("jeu de démarrage" en français) est un programme malveillant, dont la principale fonctionnalité est de dissimuler la présence de son activité et celle des autres programmes néfastes aux yeux de l'utilisateur du système et des logiciels de sécurité (antivirus, pare-feu, IDS). Certains rootkit peuvent en plus de cette fonctionnalité principale, installer des backdoors (porte dérobée).

Les rootkits ont deux caractéristiques principales :

- ✓ Ils modifient profondément le fonctionnement du système d'exploitation ;
- ✓ Ils se rendent invisibles (difficile à les détecter).

- ***Porte dérobée : (Les backdoors) [WEB 02]***

Une porte dérobée n'est pas un programme, mais une fonctionnalité d'un programme permettant de donner un accès secret au système. Ce genre de fonctionnalité est souvent ajouté à un logiciel par l'éditeur, afin de lui permettre de surveiller l'activité du logiciel, ou de prendre le contrôle en cas de sollicitation.

2. Les attaques par messagerie : [WEB 03]

En dehors des nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques à celle-ci :

- ***Le Pourriel (spam en anglais) :***

Le pourriel ou spam en anglais, désigne les communications électroniques massives, notamment de courriers électroniques, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes.

- ***L'Hameçonnage (phishing en anglais) :***

L'hameçonnage est une technique de fraude visant à obtenir des informations confidentielles, telles que des mots de passe ou des numéros de carte de crédit sous forme de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales;

- ***Le Canular informatique (hoax en anglais) :***

Un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Ils encombrent le réseau et font perdre du temps à leurs destinataires.

3. Les attaques sur le réseau : [WEB 03]

- ***Intrusion :***

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident, chantage…

Le principal moyen pour prévenir les intrusions est le pare-feu (firewall). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés.

- ***Écoute du réseau (sniffing) :***

Il existe des logiciels qui, permettent d'intercepter certaines informations qui transitent sur un réseau local, en retranscrivant les trames dans un format plus lisible (Network packet sniffing). C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en « broadcast » sur le réseau local peuvent être interceptées.

De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute. L'utilisation de Switch (commutateurs) réduit les possibilités d'écoute mais en inondant le commutateur, celui-ci peut se mettre en mode « HUB » par sécurité.

- ***Le déni de service (Denial of service):***

L'attaquant n'obtient pas un accès au système informatique sur le réseau mais il parvient à mettre en panne certains composants stratégiques (le serveur de messagerie, le site web, etc.). Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser un service ou un réseau complet. Les utilisateurs ne peuvent plus alors accéder aux ressources. Les deux exemples principaux, sont le «ICMP flood » ou l'envoi massif de courriers électroniques pour saturer une boîte aux lettres. La meilleure parade est le firewall ou la répartition des serveurs sur un réseau sécurisé.

- ***IP Spoofing :***

Usurpation d'adresse IP, nous faisons croire que la requête provient d'une machine autorisée. Une bonne configuration du routeur d'entrée permet d'éviter qu'une machine extérieure puisse se faire passer pour une machine interne.

4. Les attaques sur les mots de passe : [WEB 03].

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe. Dans ce cadre, notons les deux méthodes suivantes:

- ***L'attaque par dictionnaire :***

Le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin, etc.). Ces listes sont généralement dans toutes les langues les plus utilisées, contiennent des mots existants, ou des diminutifs (comme par exemple "powa" pour "power", ou "G0d" pour "god").

- ***L'attaque par force brute :***

Toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution (par exemple de "aaaaaa" jusqu'à "ZZZZZZ" pour un mot de passe composé strictement de six caractères alphabétiques).

II. 5. Les services de sécurité : [18]

II.5.1. Définition :

Un service de sécurité est une réponse à un besoin de sécurité, exprimée en termes fonctionnels décrivant la finalité du service, généralement en référence à certains types de menaces.

Un service de sécurité décrit une fonction de sécurité. Cette fonction est indépendante des mécanismes et solutions concrètes permettant la réalisation effective du service.

Exemple : le service « Contrôle d'accès », dont la finalité ou fonction, décrite implicitement par son titre, est de contrôler les accès, c'est à dire de ne laisser passer que les personnes autorisées.

II.5.2. Services et sous-services de sécurité :

La fonction assurée par un service de sécurité peut, elle même, nécessiter plusieurs éléments complémentaires, qui peuvent être considérés comme des « sous-fonctions ». Dans l'exemple ci-dessus, le contrôle d'accès nécessite la connaissance de ce qui est autorisé, ce qui fait appel à une fonction d'autorisation, la reconnaissance d'une personne, ce qui fait appel à une fonction d'authentification, et le filtrage des accès, ce qui fait appel à une troisième fonction de filtrage.

Un service de sécurité peut ainsi lui-même être constitué de plusieurs autres services de sécurité pour répondre à un besoin ou une finalité déterminée. Chacun des constituants est un sous-service de sécurité du service en question, tout en conservant, vis-à-vis d'une fonction qui lui est propre.

II.5.3. Mécanismes et solutions de sécurité :

Un Mécanisme est une manière particulière d'assurer, totalement ou partiellement, la fonction du service ou du sous-service. Il s'agit d'une procédure spécifique, d'algorithme, de technologie, etc. Pour le sous-service d'authentification abordé précédemment, les mécanismes possibles pour l'authentification aux systèmes d'information sont les mots de passe, les jetons, les processus reposant sur des algorithmes contenus dans des cartes à puce, les systèmes biométriques, etc. Pour un sous-service donné, plusieurs mécanismes sont généralement possibles. Leur choix a très souvent un effet direct sur la qualité du sous-service concerné. Une solution de sécurité est la réalisation concrète d'un mécanisme de sécurité et comprend les matériels et logiciels nécessaires à son déploiement, les procédures de déploiement et de support opérationnel ainsi que les structures organisationnelles nécessaires.

II.5.4. Mesure de la qualité des services de sécurité :

Les services de sécurité peuvent avoir des niveaux de performance très différents selon les mécanismes employés. Il est donc essentiel de pouvoir mesurer la qualité ou la performance d'ensemble d'un service de sécurité :

II.5.4.1. Paramètres à prendre en compte :

Pour mesurer la performance d'un service de sécurité, plusieurs paramètres devront être pris en compte **:**

- L'efficacité du service ;
- Sa robustesse ;
- Les moyens de contrôle de son bon fonctionnement.

1. ***L'efficacité du service de sécurité :***

Pour les services dits techniques, l'efficacité mesure leur capacité à assurer effectivement la fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou des circonstances plus ou moins courantes.

Pour prendre l'exemple du sous-service "Gestion des autorisations d'accès au système d'information", qui attribue des droits à des utilisateurs, la fonction du service est de faire en sorte que seules les personnes dûment habilitées par leur hiérarchie aient effectivement les droits correspondants.

L'efficacité d'un service contrôlant des actions humaines est ainsi la mesure des compétences nécessaires pour qu'un acteur puisse passer à travers des contrôles mis en place ou pour les abuser.

2. ***Robustesse d'un service de sécurité :***

La robustesse d'un service mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber (bloquer). La robustesse ne concerne que les services dits techniques.
Dans l'exemple précédent de gestion des autorisations, la robustesse du sous-service dépend, en particulier, des possibilités d'accès direct à la table des droits attribués aux utilisateurs et donc de se faire attribuer des droits sans passer par les processus normaux de contrôle mis en place.

3. ***Mise sous contrôle d'un service de sécurité :***

La qualité globale d'un service de sécurité doit enfin prendre en compte sa permanence dans le temps. Pour cela, il convient que toute interruption de service soit détectée et que des mesures palliatives soient alors décidées. La qualité de ce paramètre dépend donc de la capacité et de la rapidité de détection et des moyens de réaction.

Pour les mesures générales, la mise sous contrôle représente d'une part leur aptitude à être mesurées en termes de mise en œuvre ou d'effet, et d'autre part la mise en place effective d'indicateurs et de systèmes de contrôle.

II.6. Les domaines de la sécurité : [19]

Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique se décline en :

- Sécurité physique ;
- Sécurité de l'exploitation ;
- Sécurité logique ;
- Sécurité des télécommunications.

1. La sécurité physique :

La sécurité physique a pour but de protéger les bâtiments et les équipements :

- Délimitation de zone de sécurité pour l'accès aux bâtiments (attention aux accès par les livreurs).
- Mise en place de sécurité physique comme la lutte contre l'incendie ou le dégât des eaux.
- Mise en place de locaux de sécurité avec contrôle d'accès et alarmes, notamment pour les salles machines.
- Mise en place de procédures de contrôle pour limiter les vols ou les compromissions.
- Mise en place de procédures pour la gestion des documents dans les bureaux.

2. La sécurité de l'exploitation :

Rapport à tous ce qui touche au bon fonctionnement des systèmes.

Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

La sécurité de l'exploitation dépend fortement de son degré d'industrialisation qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches

Quelques points clés de cette sécurité :

- Inventaire réguliers et dynamique.
- Gestion du parc informatique, des configurations et des mises à jour.
- Contrôle et suive de l'exploitation.
- Maintenance doit être préventive et régulière.

- Risque d'exploitation : remplacement des équipements, interruption de service, perte de données.

3. La sécurité logique :

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel. Elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation.

Elle repose également sur :

- Les dispositifs mis en place pour garantir la confidentialité dont la cryptographie.
- Une gestion efficace des mots de passe et des procédures d'authentification.
- Des mesures antivirus et de sauvegarde des informations sensibles.

Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secrète, ...)

4. La sécurité des télécommunications :

- Offrir à l'utilisateur une connectivité fiable et de qualité de « bout en bout ».
- Un environnement de communication sécurisé implique la sécurisation de tous les éléments de la chaîne informatique.

Il faut donc mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires. Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.

II.7. Politique de sécurité : [web 04]

II.7.1. Définition :

La politique de sécurité est un document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.

II.7.2. Les domaines abordés par la Politique de sécurité : [18]

Quatre domaines doivent être considérés et abordés par la Politique de sécurité :

- L'organisation et les structures impliquées dans le management de la sécurité :

- Rôles et fonctions des responsables de la sécurité au sein des entités (fonction centrale, fonctions locales, correspondants, etc.) ;
- Rôles et responsabilités des responsables opérationnels et de la hiérarchie ;
- Responsabilités individuelles de chaque membre du personnel ;
- Structures de conseil et d'expertise (formelle ou informelle) au sein de l'entreprise et partage des compétences.

- Les éléments fondateurs d'une culture sécurité d'entreprise :

L'énoncé d'un certain nombre de principes de base qui doivent être communs à toutes les entités. Parmi ces principes et notions communes peuvent figurer :

- La nécessité d'agir en fonction de la sensibilité des informations et ressources et donc de définir une classification de ces éléments ;
- L'existence et le rôle de propriétaires d'information ou de ressources.
- Les conditions dans lesquelles sont accordés les droits et privilèges.
- Le principe d'auditabilité de toute action.
- La possibilité de surveiller le travail de toute personne responsable, les droits et devoirs de la hiérarchie dans ce domaine.

- Les éléments fédérateurs et de maintien de la cohérence dans le domaine des solutions techniques mises en œuvre :

Dans le domaine des techniques de sécurité mises en œuvre, deux points sont à considérer particulièrement :

- La sécurité des éléments communs par nature, comme le réseau étendu d'entreprise et certaines infrastructures qui ne peuvent être que partagées.
- Le choix d'éléments d'architecture de sécurité qui orientent le Groupe dans une voie de structuration des solutions et qui peuvent, de ce fait, avoir un impact stratégique sur les capacités d'évolution future des systèmes d'information.

- Les moyens et méthodes de pilotage et de management de la sécurité.

- Le choix de méthodes de management de la sécurité.
- Les moyens et structures d'audit de la sécurité au sein de l'entreprise.
- La structure de pilotage éventuelle de la sécurité et l'élaboration de tableaux de bord au niveau des entités et de l'entreprise

II.8.Les outils de sécurité : [WEB 05]

Le système de sécurité d'une entreprise se construit à l'aide de nombreux outils complémentaires et techniques existant sur le marché. Un seul ne suffit pas: la sécurité est assurée par une utilisation correcte d'un ensemble d'outils à choisir, paramétrer et/ou développer en fonction de l'objectif de sécurité fixé.

II.8.1. Cryptographie, signature électronique et certificats :

L'utilisation des techniques de la cryptographie, de signature électronique et des certificats sont la base d'un commerce électronique sécurisé:

- ***La cryptographie:***

Elle consiste à transformer les informations électroniques au moyen d'un algorithme mathématique afin de les rendre inintelligibles, sauf pour celui qui possède le moyen (une clé) de les décoder. La cryptographie des informations qui transitent par le réseau est utilisée pour assurer la confidentialité, l'intégrité et l'authenticité des transactions et du courrier électronique. A titre d'exemple, le logiciel de la cryptographie gratuit Pretty Good Privacy(PGP) est très largement employé pour protéger le courrier électronique.

- ***La signature électronique:***

C'est un code digital (une réduction du document électronique à envoyer) qui, associé aux techniques de la cryptographie, garantit l'identité de la personne qui émet le message et assure la non-répudiation et l'intégrité de l'envoi;

- ***Le certificat:***

Document électronique (carte d'identité) émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique de la cryptographie et fournit des informations de gestion complémentaires sur le certificat et le détenteur.

II.8.2.L'authentification :

L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).

Plusieurs solutions simples sont mises en œuvre pour cela, comme l'utilisation d'un identifiant (login) et d'un mot de passe (password). L'authentification peut s'effectuer par un numéro d'identification personnel, comme le numéro inscrit dans une carte à puce, ou code PIN (Personal Identification Number).

Des techniques beaucoup plus sophistiquées, comme les empreintes digitales ou rétiniennes(Biométrie), les authentifier (clé USB, I Phone…etc.) se développent de façon industrielle au début des années 2000. Cependant, leur utilisation est assez complexe et ne peut être mise en place que dans un contexte particulier, comme un centre de recherche de l'armée par exemple.

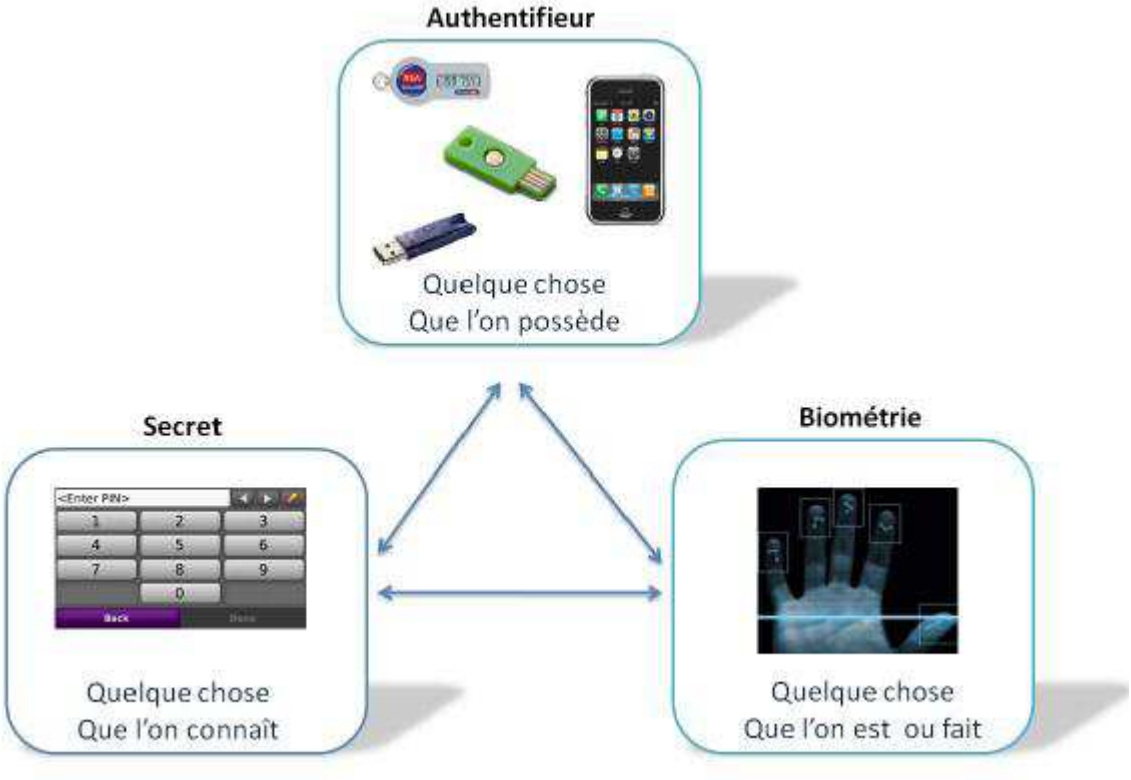


Figure II-1 : Modalités d'authentification.

II.8.3. Le firewall :

Le firewall est un ensemble informatique du réseau d'entreprise comprenant du matériel hardware (un ou des routers, un ou des serveurs) et des logiciels (à paramétrer ou à développer).

Son objectif est de protéger le réseau interne contre les accès et actions non autorisés en provenance de l'extérieur, en contrôlant le trafic entrant. Le firewall peut également contrôler le trafic sortant.

Le firewall est localisé entre le réseau externe et le réseau interne. Pour être efficace, le firewall doit être le seul point d'entrée-sortie du réseau interne (pas de modem sur un serveur ou PC pour accéder à l'extérieur sans passer par le firewall) et surtout doit être correctement configuré et géré en fonction des objectifs spécifiques de sécurité. Sans ces précautions, un firewall ne remplit pas son rôle et est complètement inutile.

Le firewall est un élément de la sécurité, il ne couvre pas tous les risques (par exemple le firewall n'assure pas la confidentialité des informations, n'authentifie pas l'origine des informations, ne vérifie pas l'intégrité des informations, ne protège pas contre les attaques internes).

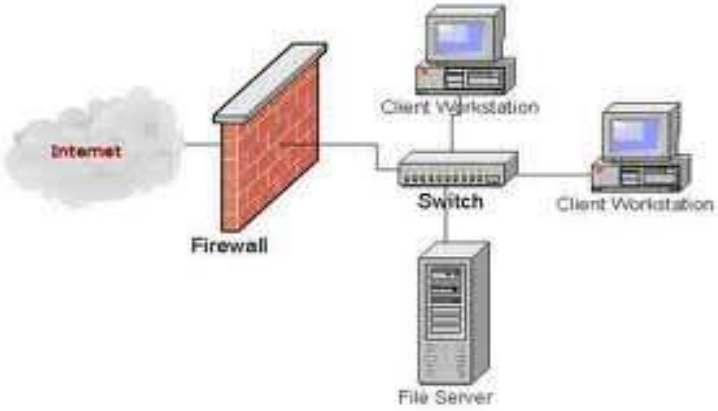


Figure II.2. Les firewalls.

II.8.4.Les fichiers historiques

Des outils de traçabilité doivent être mis en œuvre pour garder une trace des événements, comme par exemple:

- qui est venu, quand, quelle a été la durée de la transaction?
- qu'a-t-on consulté ou modifié?
- quelles on été les ressources utilisées?

La consultation régulière des fichiers historiques constitués doit notamment permettre de vérifier les anomalies dans le trafic des transactions (par exemple les messages répétitifs en provenance d'une même adresse extérieure et rejetés par le firewall peuvent être un signe d'essai d'intrusion).

II.8.5.Les copies de sauvegarde :

Les copies de sauvegarde (back-up) créées régulièrement et stockées dans des endroits sécurisés permettent de protéger les informations essentielles pour l'entreprise et permettent également de redémarrer rapidement en cas de problème.

II.8.6.Réseau Privé Virtuel :

Le VPN (Virtual Private Network) est un service disponible chez les fournisseurs de services Internet (**ISP** : Internet Service Provider) qui permet d'établir des connexions sécurisées privées (un réseau privé) sur un réseau public comme l'Internet.

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un

principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées. Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la toile (l'Internet), dans le sens où aucune qualité de service n'est garantie.

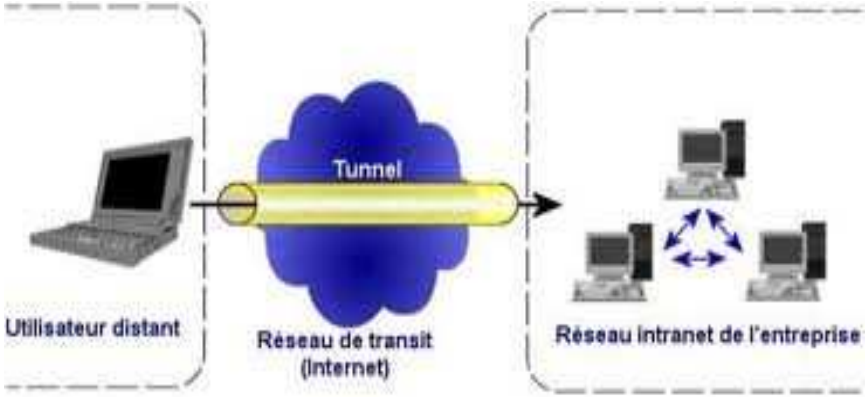


Figure II.3. Les réseaux prive virtuel (VPN).

II.8.7. L'anti virus :

Utilitaire capable de rechercher et d'éliminer les virus informatiques et autres malwares. La détection se fait selon deux principes :

Une analyse par signatures qui permet de détecter avec d'excellents résultats les virus connus pour peu que les définitions de virus soient régulièrement mises à jour, ou une analyse heuristique qui permet de détecter avec des résultats variables les virus inconnus à partir de leur logique de programmation et le cas échéant de leur comportement à l'exécution.

Les antivirus fonctionnent eux-mêmes selon deux principes :

Un scanner qui permet à l'utilisateur de lancer une analyse d'un disque ou d'un fichier lorsqu'il le souhaite ou un moniteur qui surveille le système en temps réel et empêche l'utilisateur d'ouvrir un fichier infecté.

II.10. Conclusion :

Au cours de ce chapitre, nous avons abordé les différents aspects liés à la sécurité informatique et son environnement, en suite on a cité quelques solutions retenues actuellement pour faire face aux différents risques et menaces rencontrés et quelques outils de sécurité. Ces différents concepts traités nous aiderons à mieux comprendre notre mode d'opération et les notions fondamentales pour mener à bien notre application.

Chapitre III
Analyse
&
Conception

III.1.Introduction :

La conception de toute solution informatique est d'une grande importance, elle doit être traitée avec rigueur et précision, car elle constitue la base du système à développer.

Avant de s'engager dans la conception, il est impératif de passer par la phase d'analyse qui permet d'identifier les différents acteurs qui interagissent avec le système ainsi que leurs besoins. Puis nous passons à la conception qui, en s'appuyant sur les résultats de la phase d'analyse, donnera la description détaillée du système cible et des objectifs à atteindre.

En fin, nous aborderons les bases de données, ou nous expliquerons les différentes tables implémentées et le fonctionnement du schéma conceptuel.

Pour ce faire, notre démarche va s'appuyer sur le langage UML étendu pour le web, qui permet une bonne représentation des aspects, statique et dynamique, d'une application.

III.2. Analyse :

Cette partie comprend l'identification des besoins fonctionnels du système, ainsi une description du problème et la solution proposée.

III.2.1. Problématique :

Avec l'évolution des technologies, les entreprises sont obligées d'ouvrir leur système d'information à leurs partenaires ou leurs fournisseurs, et cela met leur système face aux intrusions, ce qui provoque l'insécurité de leur organisation.

Malgré que la plupart des entreprises disposent des moyens et outils pour sécuriser leurs systèmes. Mais la question qui se pose : Est-ce que ces moyens et outils sont fiables et bien suivis ?

III.2.2. Objectif de l'application :

L'objectif de notre application est d'aider les entreprises à répondre à la question posée précédemment, à travers un test d'évaluation de la sécurité informatique de leur organisation, les principales fonctionnalités de notre application sont schématisées dans la figure suivante :

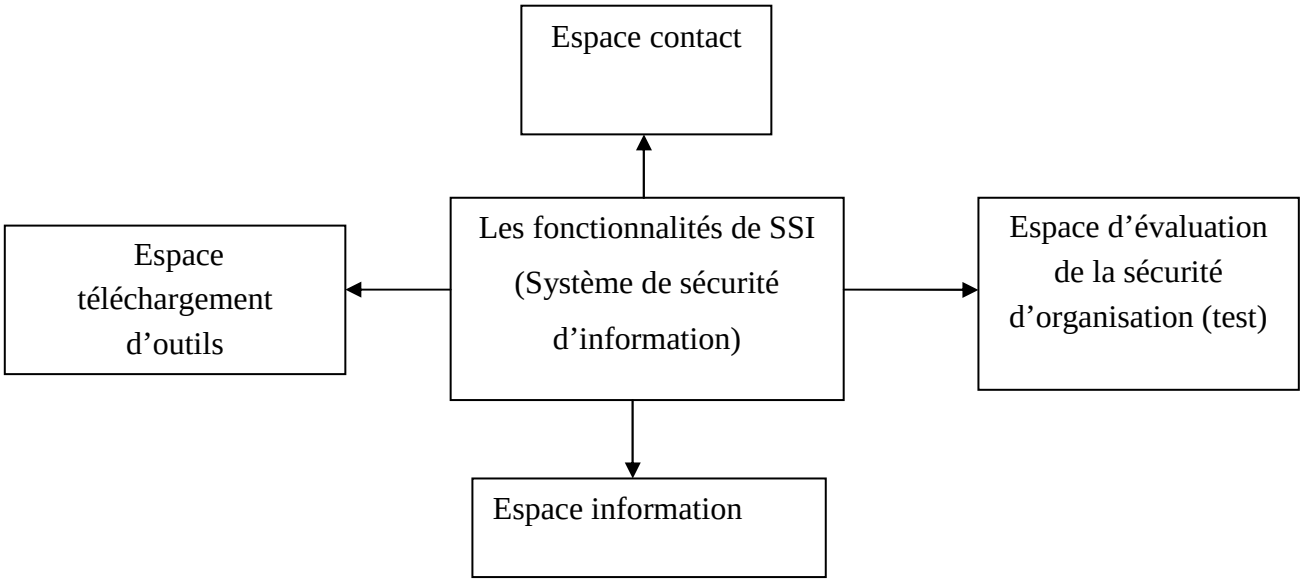


Figure III.1 : Les principales fonctions de SSI.

- ***Espace information :***

  Qui comprend des documents pour s'informer sur la sécurité informatique.

- ***Espace téléchargement d'outils :***

  Qui comprend des outils a téléchargé ?

- ***Espace Test :***

  Qui comprend un lot de questions. Pour certain il devait répondre par Oui/Non ou Aucune, s'il ne connaît pas la réponse, dans ce cas nous la considérons a fausse. Pour certains d'autres de coucher une ou plusieurs réponses et s'il n'a pas de réponse il a qu'a couché la case « Aucune ».

III.2.3. Spécification des besoins :

La spécification des besoins doit décrire sans ambigüité le système à développer. L'expression des besoins doit donc proposer ce que le système devrait accomplir et non comment le faire.

III.2.3.1. Les cas d'utilisation :

Les cas d'utilisation sont des outils formels qui permettent de consigner et d'exprimer les interactions et les dialogues entre les utilisateurs (Acteurs) d'un système et le système lui-même. Ils constituent une technique qui permet de déterminer les besoins des utilisateurs et de capturer les exigences fonctionnelles d'un système. Un cas d'utilisation doit exprimer ce que le système doit faire sans préjuger de façon dont cela sera fait.

Avant de décrire les différents cas d'utilisation, il est nécessaire de mettre en évidence les acteurs utilisant le système ainsi que leurs tâches respectives et les scénarios qui les décrivent. En regroupant l'ensemble de ces scénarios nous obtenons les différents cas d'utilisation.

III.2.3.2.Identification des acteurs :

Un acteur représente un rôle joué par une personne ou une chose qui interagit avec un système. Les acteurs se déterminent en observant les utilisateurs directs du système, ceux qui sont responsables de son exploitation ou de sa maintenance, ainsi que les autres systèmes qui interagissent avec le système en question.

Les acteurs de notre système sont :

- ***Administrateur :*** Personne possédant les droits d'accès à l'espace administrateur.
- ***Visiteur :*** Personne qui se connecte pour consulter ou s'inscrire comme un nouveau client.
- ***Client :*** Personne déjà enregistrée dans la base de données qui se connecte pour utiliser les services de l'application.

III.2.3.3. Spécification des tâches :

Pour chaque acteur nous spécifierons les tâches qu'il assure. Le tableau suivant résume ces tâches.

- ✓ Les tâches associe aux visiteurs sont :

Acteur	Tâches
Visiteur	**T01 :** Accéder au site.
	T02 : Naviguer dans le site.
	T03 : S'inscrire.
	T04 : s'informer.

- ✓ Les tâches associe aux clients sont :

Acteur	Tâches
Client	**T05 :** Idem que le visiteur.
	T06 : Contacter l'administrateur.
	T07 : S'authentifier
	T08 : Télécharger un logiciel.
	T09 : Utiliser les services de l'application.
	T10 : Se déconnecter.

- ✓ Les tâches associent à l'administrateur :

Acteur	Tâches
Administrateur	**T11 :** S'authentifier.
	T12 : Gérer les clients.
	T13 : Gérer le questionnaire.
	T14 : Gérer les outils.
	T15 : Gérer les documents.
	T16 : Consulter la messagerie.
	T117 : Se déconnecter.

III.2.3.4 .Spécification des scénarios :

III.2.3.4.1.Définition d'un scénario :

Un scénario est une description narrative de comment le système pourrai être utilisé. Les scénarios doivent être décrits par les utilisateurs eux même, chacune des tâches effectuées par un ou plusieurs acteurs sera décrite par un ensemble de scénarios. Les scénarios décrivant chacune des tâches définies auparavant sont représentés dans les tableaux suivant :

Acteur	Tâche	Scénarios
Visiteur	**T01 :** Accéder au site.	**S01 :** Saisir l'URL du site dans le navigateur choisi.

	T02 : Naviguer dans le site.	**S02 :** visualiser les liens et les textes apparaissant dans la page d'accueil.
	T03 : S'inscrire.	**S03 :** Cliquer sur le lien « s'inscrire ». **S04:** Remplir le formulaire d'identification **S05 :** Cliquer sur le lien «Valider ».
	T04 :S'informer.	**S06** : Cliquer sur le lien « S'informer » et consulter les documents disponibles.

Acteur	Tâche	Scénarios
Client	**T05 :** Idem que le visiteur.	**S01 :** **:** Idem que le visiteur. **S06 :**
	T06: Contacter « l'administrateur »	**S07 :** Cliquer sur le lien « Messagerie » puis le lien « Contacter administrateur ». **S08 :** Rédiger un message. **S09 :** Envoyer le message.
	T07 : S'authentifier.	**S10:** Saisir le login et le password. **S11 :** Cliquer sur le lien « Se connecter ».
	T08 : Télécharger un logiciel.	**S12 :** Cliquer sur le lien «Télécharger »et choisir le logiciel voulu.
	T09 : Utiliser les services de l'application (test)	**S13 :** Cliquer sur le lien « test ». Passer le test en répondant aux questions, puis les valider.
	T10 : Se déconnecter	**T14 :** Cliquer sur le lien « Déconnexion ».

Acteur	Tâches	Scénarios
administrateur	**T11** : S'authentifier.	**S15:** Saisir le login et le password. **S16 :** cliquer sur le lien «Se connecter ».
	T12 : Gérer les clients.	**S17 :** Cliquer sur le lien « Gérer les clients ». **S18:** Visualiser la liste des clients. **S19 :** Supprimer un client.
	T13 : Gérer le questionnaire.	**S20 :** Cliquer sur le lien « Gérer le questionnaire». **S21:** Visualiser la liste des questions. **S22 :** Ajouter/Supprimer/mettre à jour une question.
	T14 : Gérer les outils.	**S23:** Cliquer sur le lien « Gérer les outils». **S24:** Visualiser la liste des outils. **S25 :** Ajouter/Supprimer/mettre à jour un outil.
	T15 : Gérer les documents.	**S26 :** Cliquer sur le lien « Gérer les documents». **S27:** Visualiser la liste des documents. **S28 :** Ajouter/Supprimer/mettre à jour un document.
	T16 : Consulter la messagerie	**S29 :** Cliquer sur le lien « messagerie ». **S30 :** Visualiser le contenu de la page.
	T17 : Se déconnecter**.**	**S31 :** Cliquer sur le lien « Déconnexion ».

III.2.3.5.Spécification des cas d'utilisation :

III.2.3.5.1. Définition d'un cas d'utilisation : [WEB 06]

Un cas d'utilisation (en anglais use case) permet de mettre en évidence les relations fonctionnelles entre les acteurs et le système étudié. Nous présenterons ci dessous quelques cas d'utilisations :

III.2.3.5.2. Les cas d'utilisation détaillés :

Les figures qui suivent représentent une description de certains cas d'utilisation de notre système :

- ✓ Cas d'utilisation « S'inscrire » :

Utilisation : S'inscrire.

Scénario: S03, S04, S05.

Acteur: Visiteur.

Résumé : Cette fonctionnalité permet aux utilisateurs qui ne sont pas inscrits d'ouvrir un compte.

Description :

1. Saisir l'URL du site.
2. Le système affiche la page d'accueil du site.
3. Cliquer sur le lien « S'inscrire ».
4. Le système affiche le formulaire d'inscription.
5. Remplir le formulaire et « Valider ».
6. Le système vérifie le formulaire rempli et affiche la page de confirmation.

Figure III.2 : Cas d'utilisation « s'inscrire ».

- ✓ Cas d'utilisation « S'authentifier ».

Utilisation: S'authentifier.

Scenario: S10, S11, S15, S16.

Acteur : Client/Administrateur.

Résumé : cette fonctionnalité permet aux utilisateurs du site d'accéder à leurs espaces personnels.

Description :

1. Saisir l'URL du site.
2. Le système affiche la page d'accueil.
3. Saisir le login et le password puis validation en cliquant sur le bouton « Se connecter ».
4. Le système vérifie les données, les compare avec celles de la base de données puis affiche l'interface utilisateur correspondante, ou renvoie un message d'erreur si le login et/ou le password ne sont pas valides.

Figure III.3 : Cas d'utilisation « s'authentifier ».

✓ Cas d'utilisation « S'informer ».

Utilisation: S'informer.

Scénario : S06.

Acteur : Visiteur/Client.

Résumé : Cette fonctionnalité permet aux utilisateurs de s'informer sur les différentes généralités sur la sécurité informatique.

Description :

1. Saisie l'URL du site.
2. Le système affiche la page d'accueil.
3. L'utilisateur clique sur le lien « S'informer ».
4. Le système affiche la page d'informations.
5. Si l'utilisateur veut consulter le contenu de document il clique sur le titre de document voulu, le système lui télécharge le document.

Figure III.4 : Cas d'utilisation « S'informer».

✓ Cas d'utilisation « Contacter l'administrateur » :

Utilisation : « Contacter l'administrateur » :

Scenario: S07, S08, S09.

Acuter: Visiteur.

Résumé : cette fonctionnalité permet au visiteur d'envoyer un message à l'administrateur :

Description :

1. Saisir l'URL du site dans le navigateur.
2. Le système affiche la page d'accueil.
3. Clique sur le lien « contact».
4. Le système affiche la page pour rédiger le message.
5. Rédiger le message et cliquer sur « envoyer ».

Figure III.5. Cas d'utilisation « Contacter l'administrateur».

✓ Cas d'utilisation « Test» :

Utilisation : « Test».

Scénario : S13.

Acteur : Client.

Résumé : cette fonctionnalité permet au client de passer le test d'évaluation afin de voir un rapport qui décrit les fonctions et procédures à prendre en compte pour bien suivre la sécurité de son organisation.

Description :

1. Saisir l'URL du site dans le navigateur.
2. Le système affiche la page d'accueil.
3. Atteindre l'espace personnel du client.
4. Cliquer sur le lien « Test».
5. Le système affiche la page concernant le test à passer.
6. Une fois le test est passé le client clique sur le lien « valider ».
7. Le système affiche la page de résultat de test passé par le client qui contient un rapport qui décrit les fonctions et procédures à prendre en compte.

***Figure III.6 : Cas d'utilisation «*Test».**

III.2.3.5.3. diagramme de cas d'utilisation général :

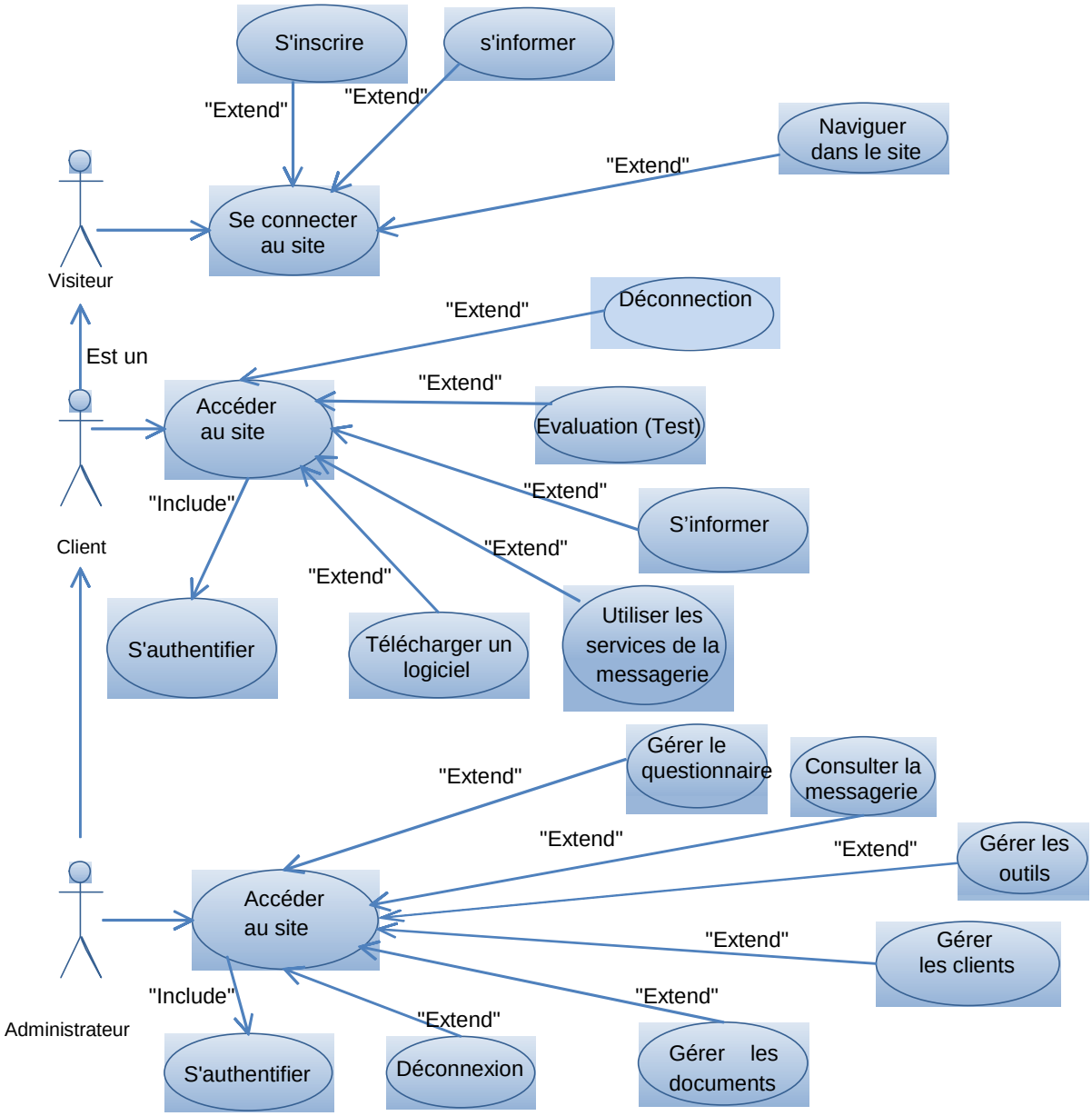


Figure III.7: Cas d'utilisation général.

III.3. Conception : [WEB 06]

La conception d'un système d'information n'est pas évidente, car il faut réfléchir à l'ensemble de l'organisation que nous devons mettre en place. La phase de conception nécessite des méthodes permettant de mettre en place un modèle sur lequel nous allons s'appuyer. La modélisation consiste à créer une représentation virtuelle d'une réalité de telle façon à faire ressortir les points auxquels nous nous intéressons.

Après avoir décrit textuellement les différents cas d'utilisation de notre système, nous allons les représenter formellement à l'aide des diagrammes de séquences.

III.3.1. Diagramme de séquence :

L'objectif de ce type de diagramme offert par UML est de représenter les interactions entre les objets en mettant l'accent sur le classement chronologique des messages échangés. Les scénarios sont des instances des cas d'utilisation et sont traduits en diagrammes de séquences.

Dans ce qui suit nous allons présent quelques cas d'utilisation :

- Inscription ;
- Informer ;
- Evaluation (test).

III.3.1.1. Diagramme de séquences simple :

III.3.1.1.1. Diagramme de séquences simple de cas d'utilisation « S'inscrire » :

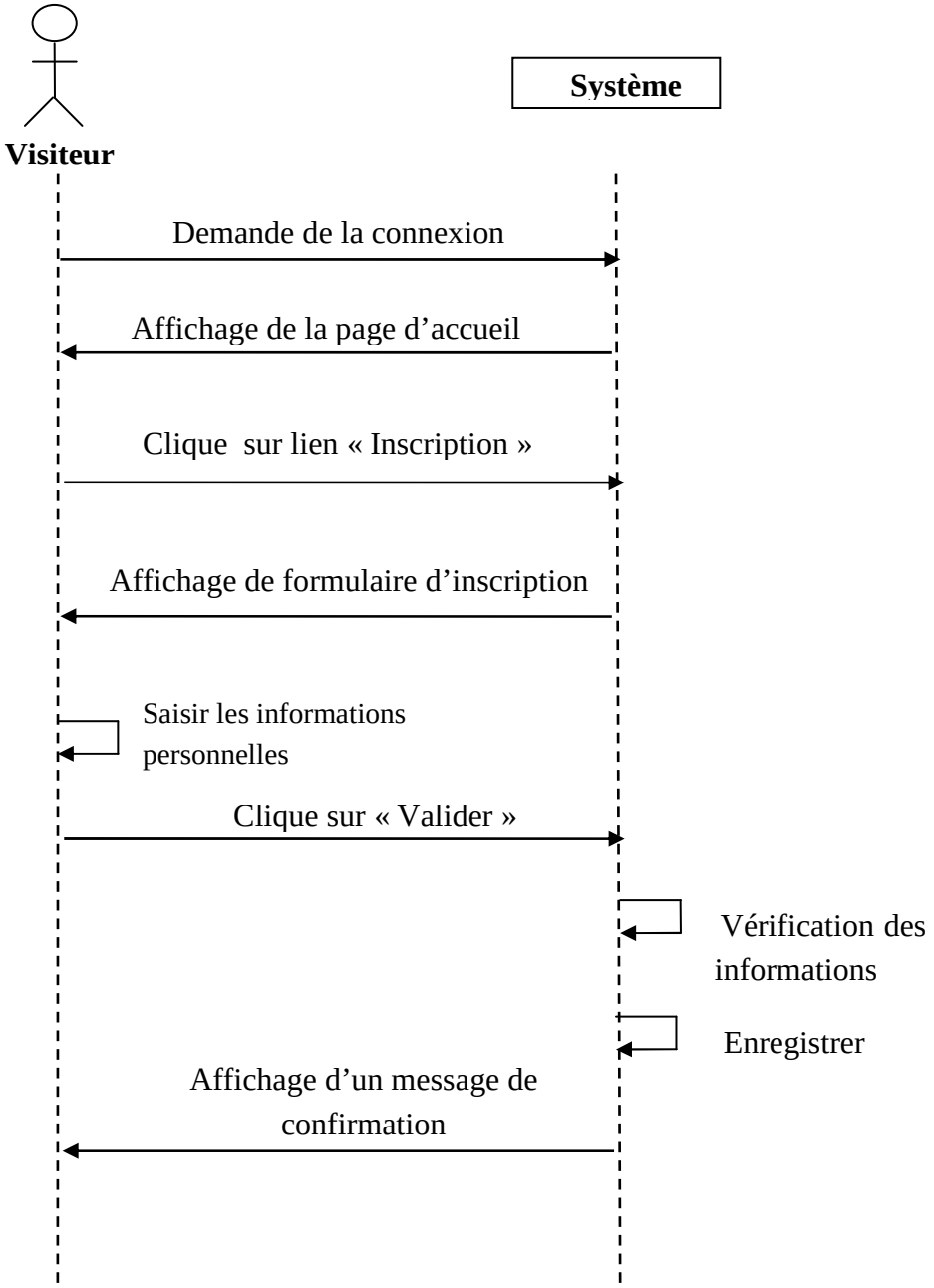


Figure III.8: Diagramme de séquence simple pour le cas d'utilisation «S'inscrire ».

III.3.1.1.2. Diagramme de séquences simple de cas d'utilisation « S'informer »

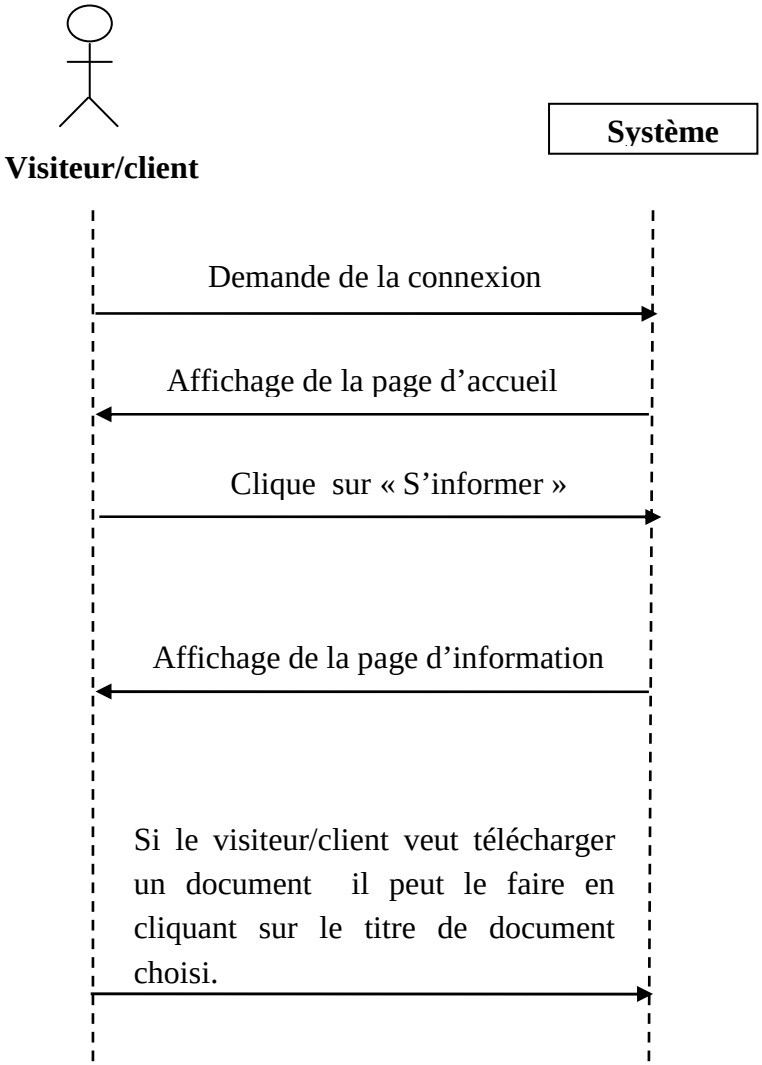


Figure III.9: Diagramme de séquence simple pour le cas d'utilisation « S'informer ».

III.3.1.1.3. Diagramme de séquences simple de cas d'utilisation «Test ».

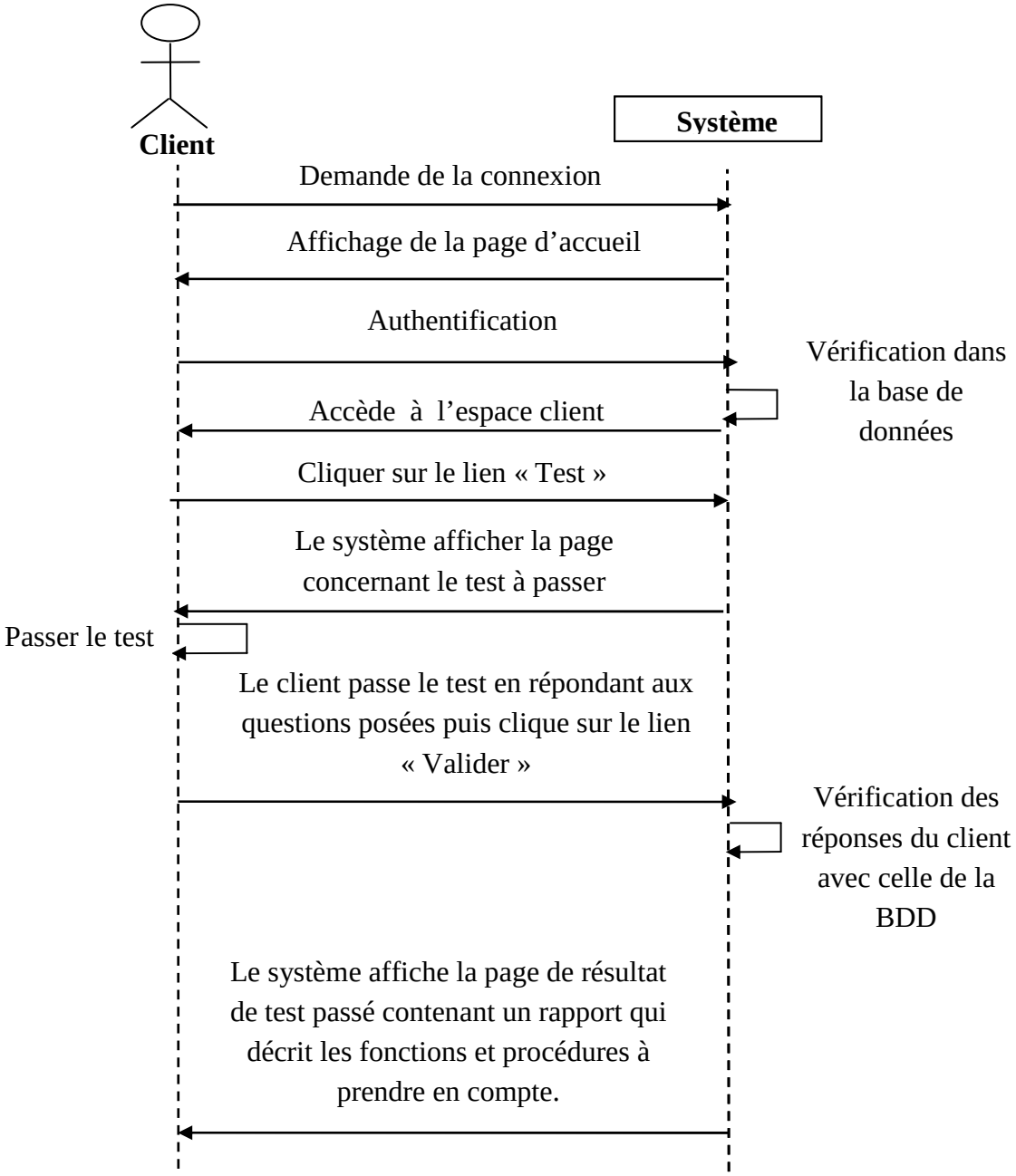


Figure III.10: Diagramme de séquence simple pour le cas d'utilisation «Test ».

III.3.1.2. diagramme de séquence de réalisation des cas d'utilisation :

III.3.1.2.1. Diagramme de séquence de réalisation du cas d'utilisation « S'inscrire » :

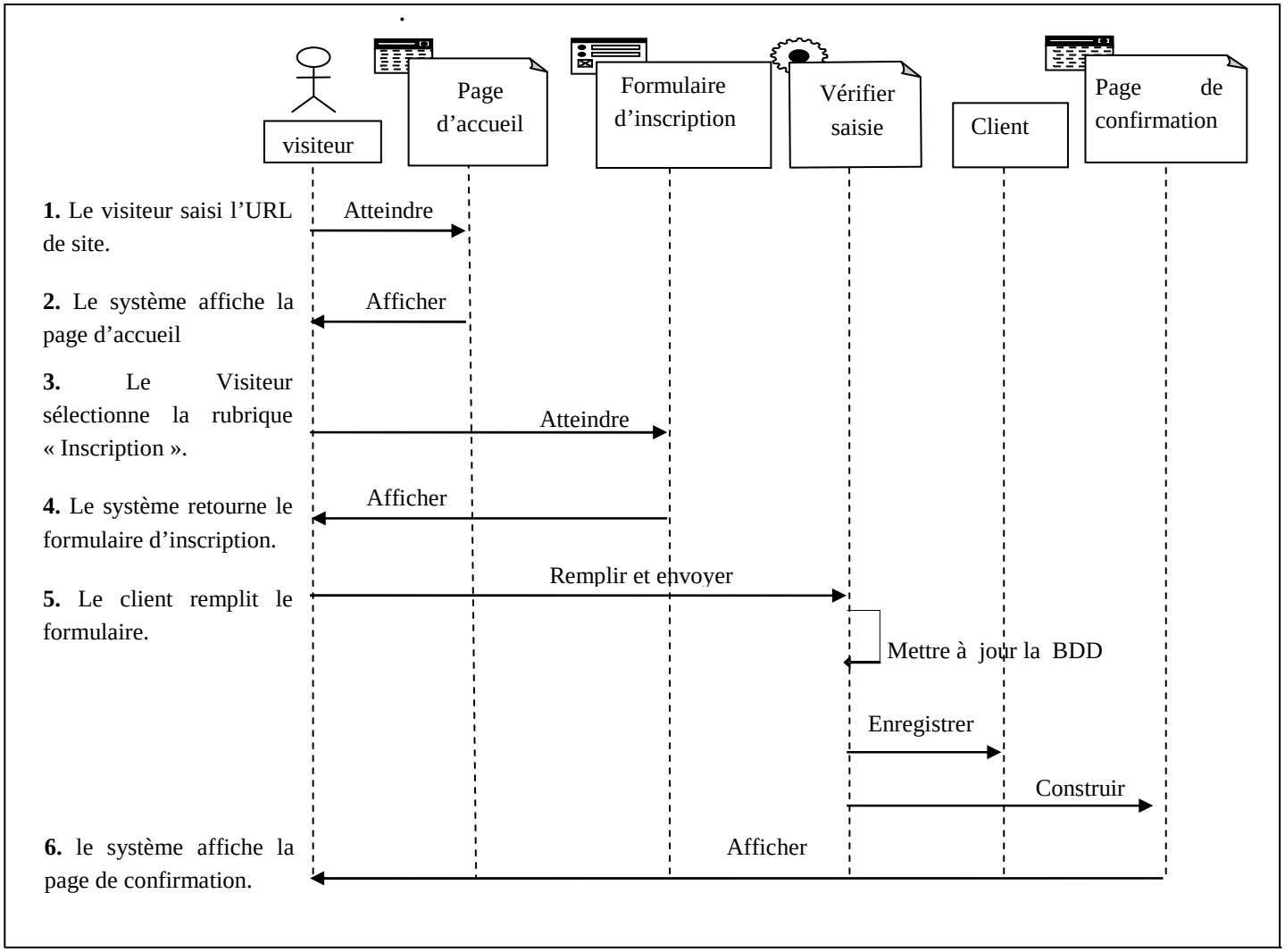


Figure III.11. Diagramme de séquence du cas d'utilisation « S'inscrire ».

III.3.1.2.2. Diagramme de séquence de réalisation du cas d'utilisation «S'informer » :

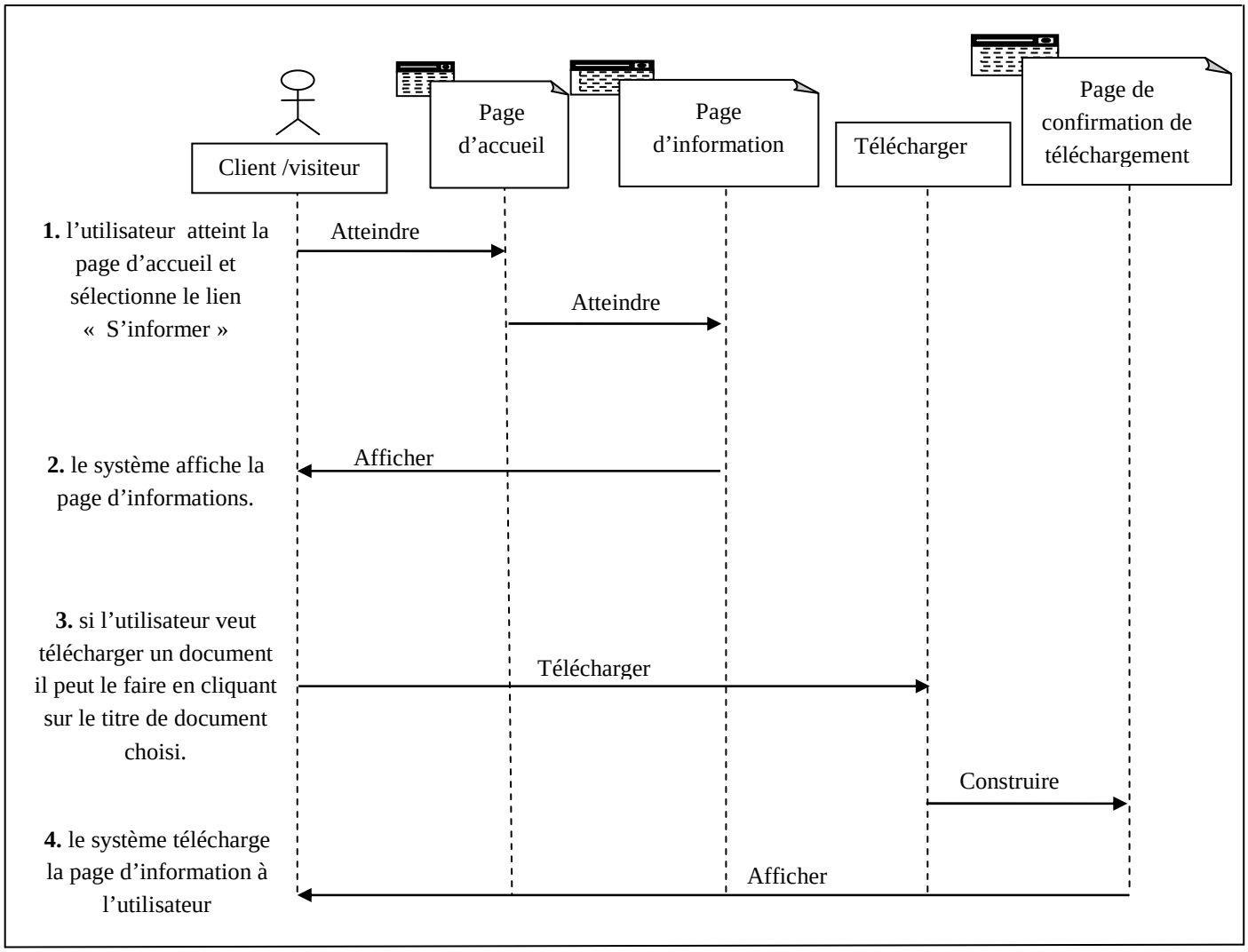


Figure III.12 : Diagramme de séquence du cas d'utilisation *«S'informer ».*

III.3.1.2.3. Diagramme de séquence de réalisation du cas d'utilisation « Test » :

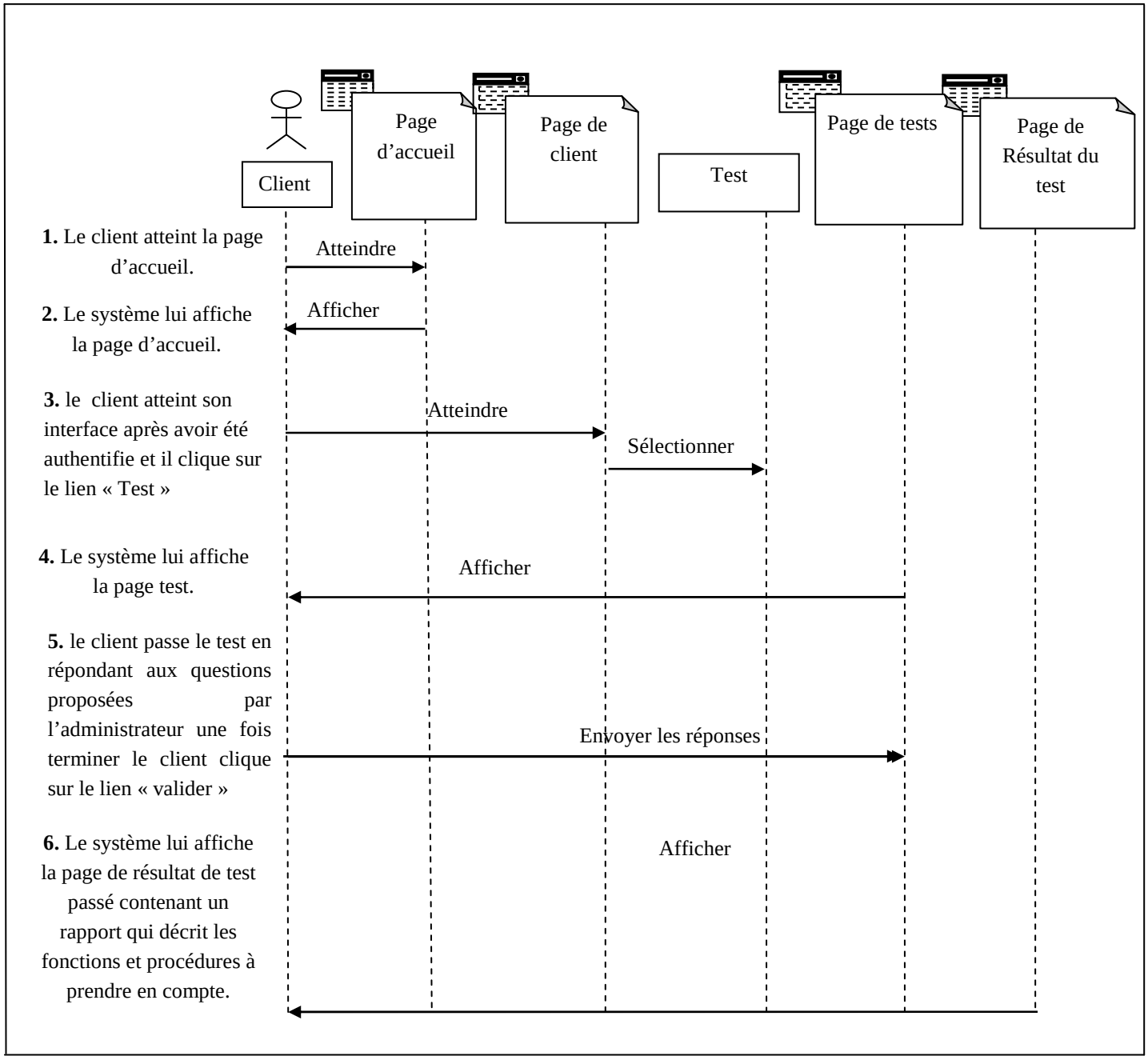


Figure III.13: Diagramme de séquence du cas d'utilisation *«Test ».*

III.3.2. Les diagrammes de classes :

Les diagrammes de classes sont les plus courants dans la modélisation des systèmes orientés objet. Ils représentent un ensemble de classes, d'interfaces et de collaborations ainsi que leurs relations. Ces diagrammes sont utilisés pour modéliser la vue de conception statique.

Vue le nombre élevé de cas d'utilisation, nous nous contentons de quelques exemples de diagrammes de classes.

III.3.2.1. Diagramme de classe généraux :

1. Diagramme de classe général du cas d'utilisation « S'inscrire ».

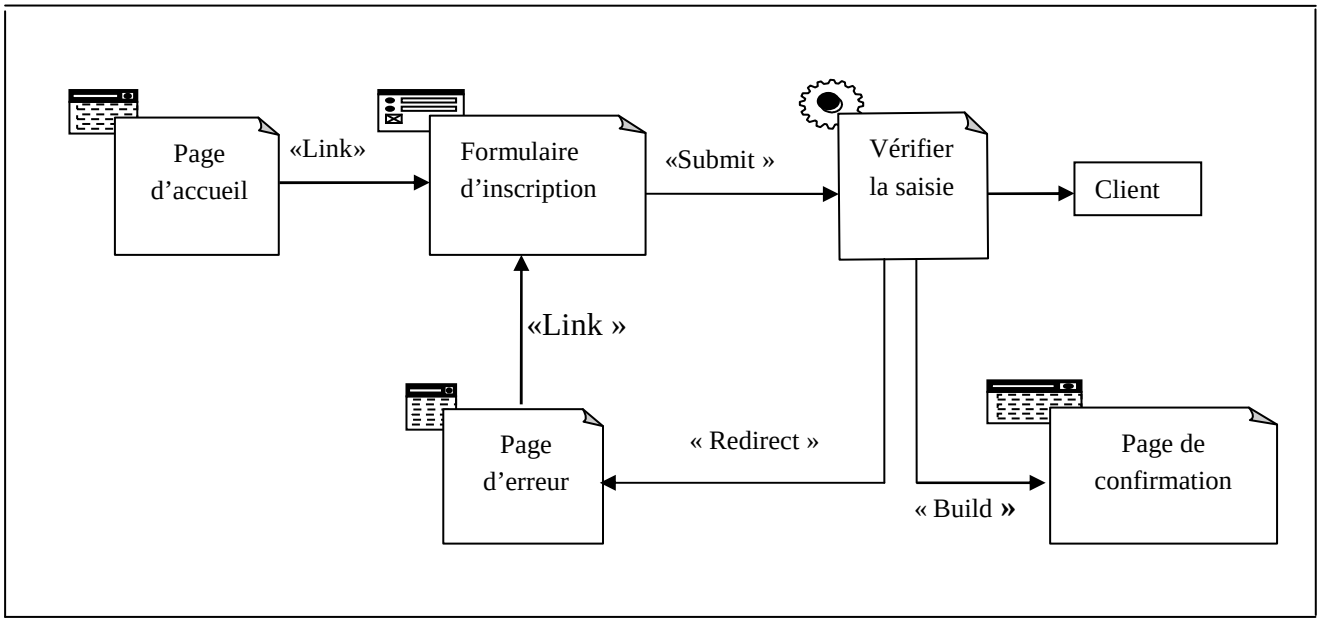


Figure III.14: Diagramme de classe général du cas d'utilisation *« S'inscrire »*.

2. Diagramme de classe général du cas d'utilisation « S'informer ».

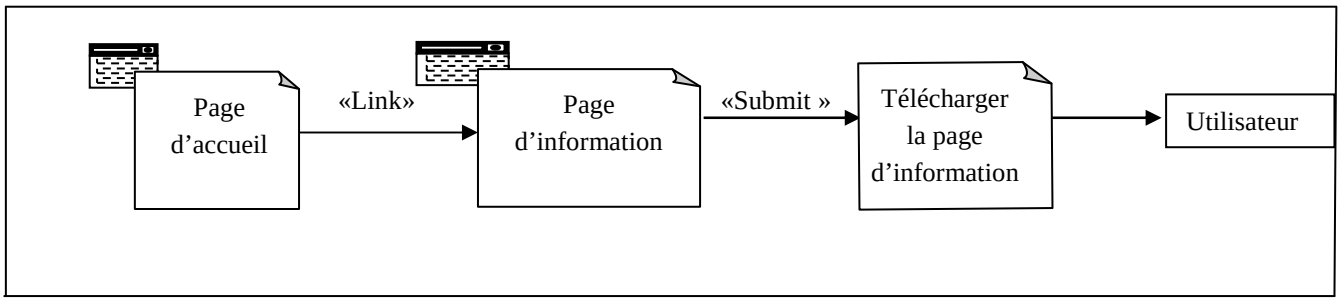


Figure III.15: Diagramme de classe général du cas d'utilisation « S'informer ».

3. Diagramme de classe général du cas d'utilisation « Test».

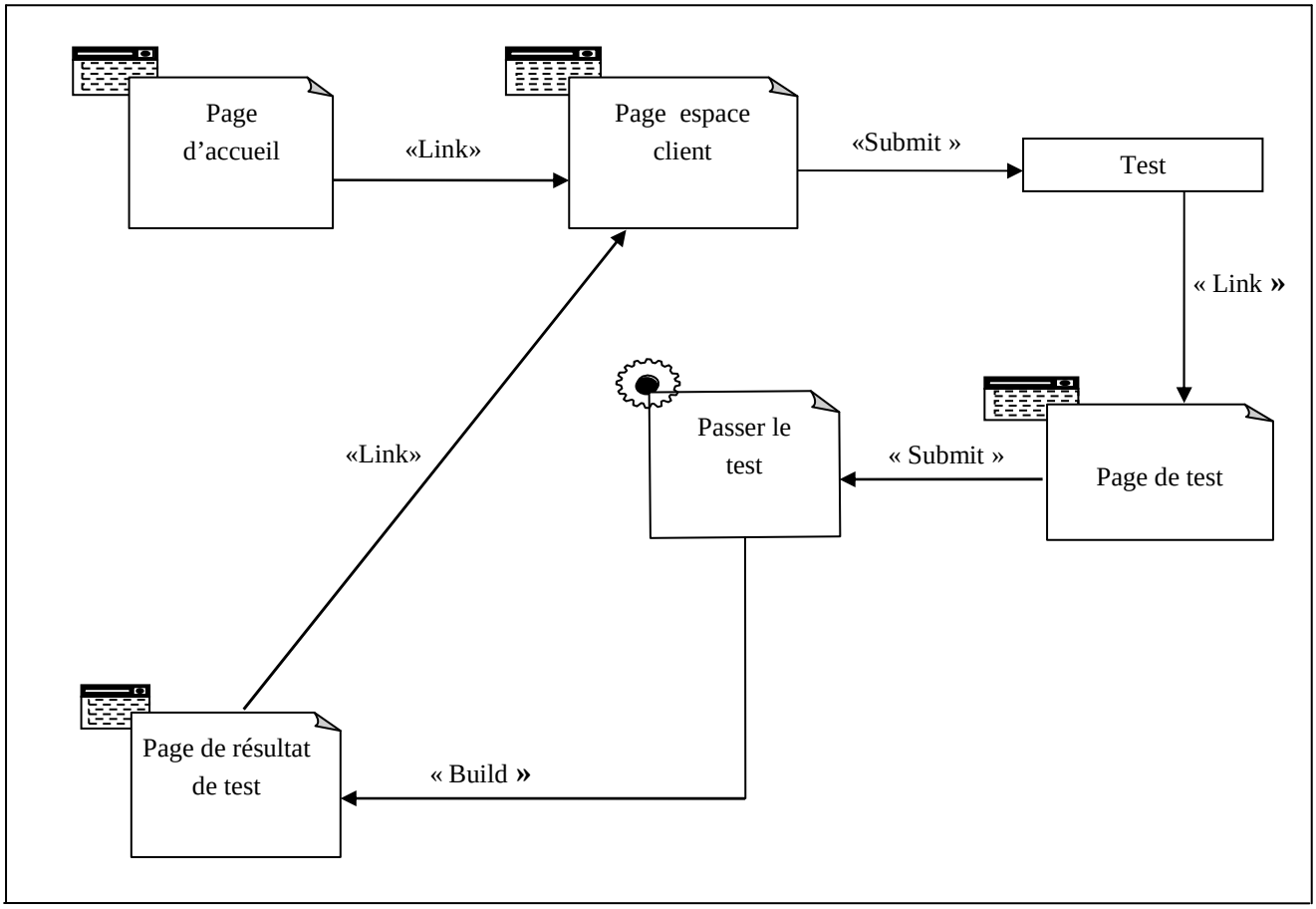


Figure III.16: Diagramme de classe général du cas d'utilisation « Test ».

III.3.2.2. Diagramme de classe détaillée :

Une fois que les pages web et les principales collaborations et responsabilités ont été identifiés, nous pouvons passer à la conception des pages proprement dites. En effet nous aboutirons aux diagrammes de classe détaillés.

1. *Diagramme de classe détaillée du cas d'utilisation « S'inscrire » :*

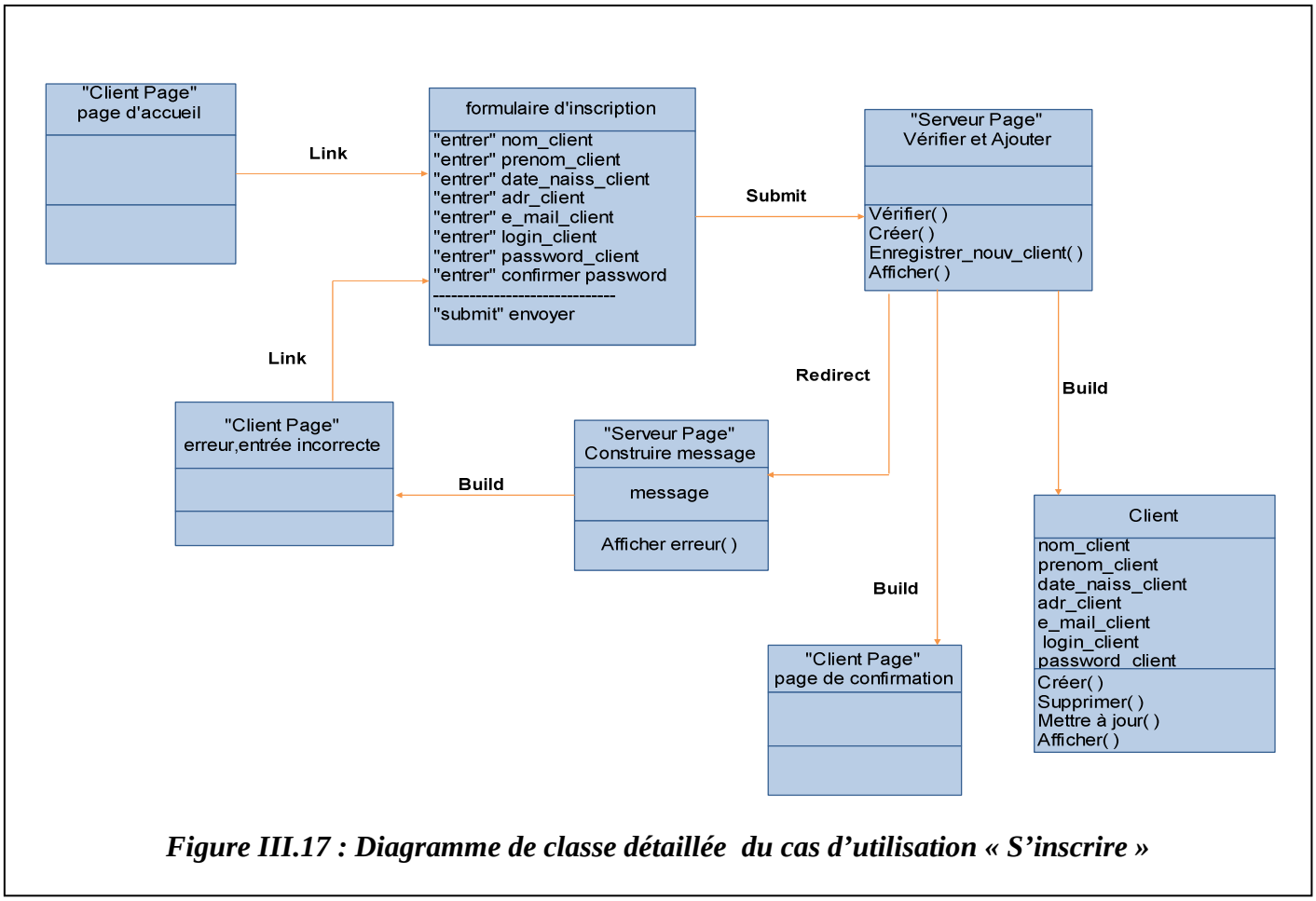


Figure III.17 : Diagramme de classe détaillée du cas d'utilisation « S'inscrire »

2. Diagramme de classe détaillée du cas d'utilisation « S'informer» :

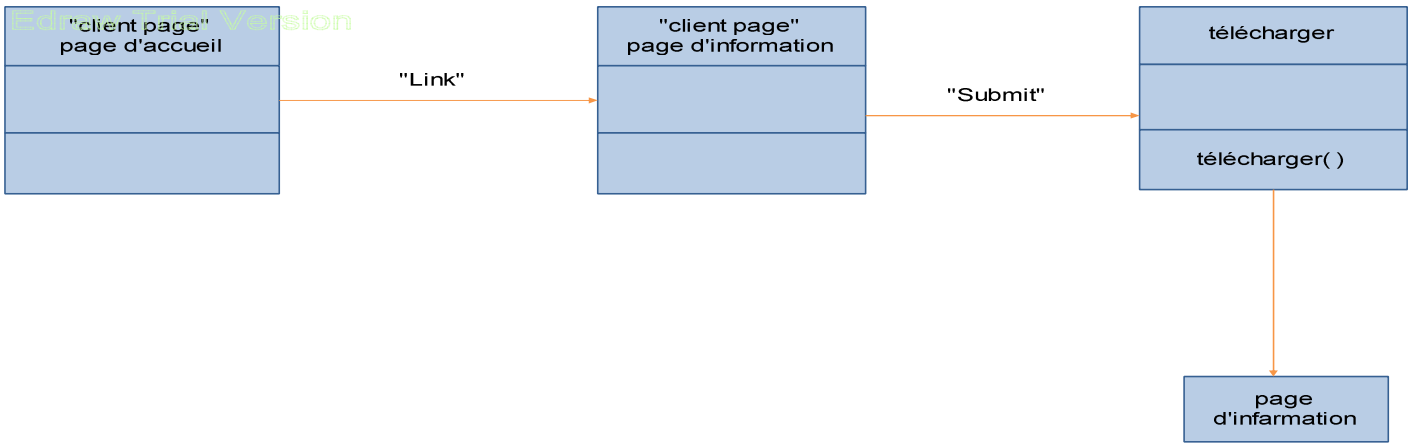


Figure III.18 : Diagramme de classe détaillée du cas d'utilisation « S'informer».

3. Diagramme de classe détaillée du cas d'utilisation « Test» :

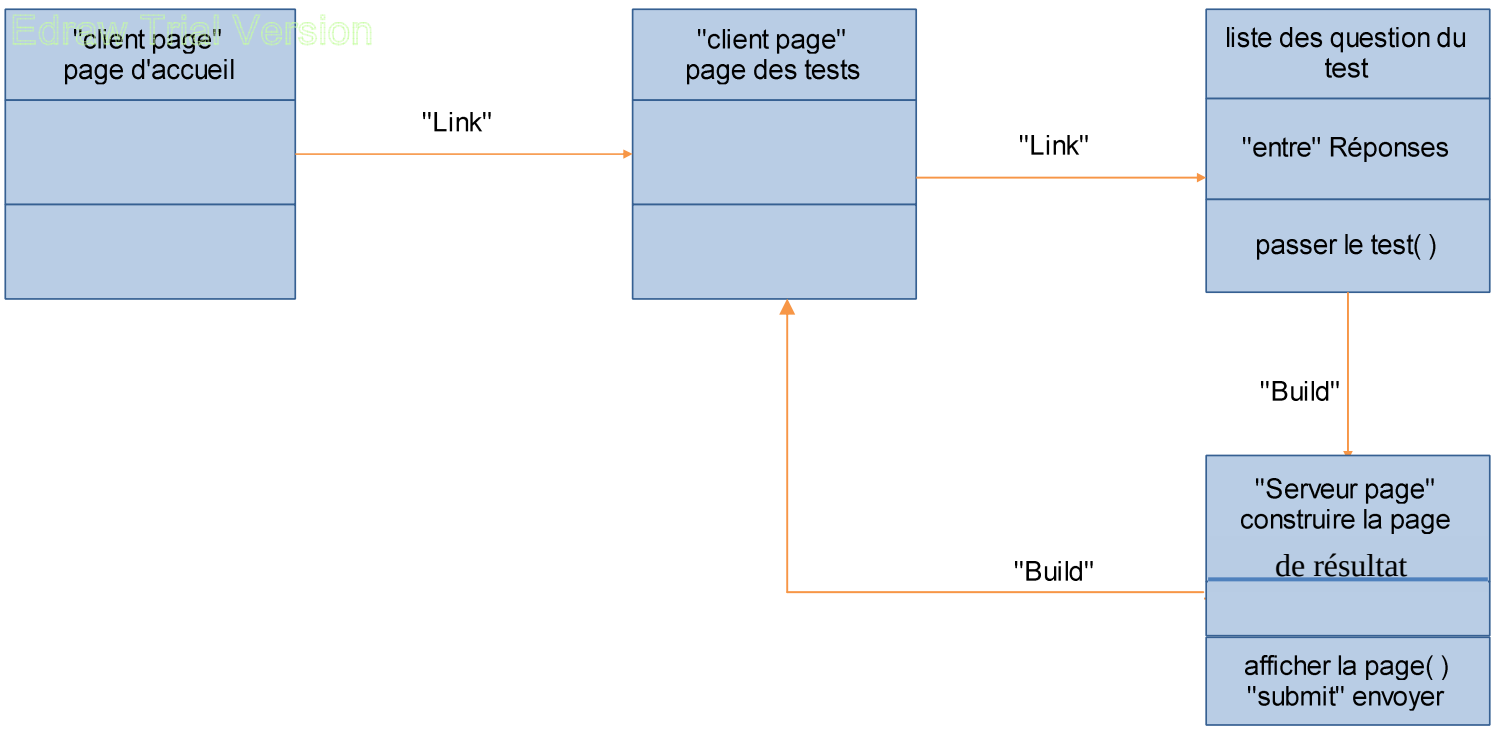


***Figure III.19: Diagramme de classe détaillé du cas d'utilisation* « Test ».**

Après avoir modélisé notre application avec les différents diagrammes offerts par le langage de modélisation UML, nous avons suivi le déroulement de chaque cas d'utilisation et nous avons utilisé les diagrammes de classes pour en extraire les différentes données nécessaires.

Pour l'implémentation de la base de données, nous aurons besoin d'élaborer un modèle logique de données qu'est l'architecture MVC (Modèle Vue Contrôle).

III.4. Le modèle vue contrôle (MVC): [WEB 08]

L'architecture Modèle/Vue/Contrôleur (MVC) est une façon d'organiser une interface graphique d'un programme. Elle consiste à distinguer trois entités distinctes qui sont, le modèle, la vue et le contrôleur ayant chacun un rôle précis dans l'interface.

L'organisation globale d'une interface graphique est souvent délicate. Bien que la façon MVC d'organiser une interface ne soit pas la solution miracle, elle fournit souvent une première approche qui peut ensuite être adaptée. Elle offre aussi un cadre pour structurer une application.

Dans l'architecture MVC, les rôles des trois entités sont les suivants.

- modèle : données (accès et mise à jour) ;
- vue : interface utilisateur (entrées et sorties),
- contrôleur : gestion des événements et synchronisation.

III.4.1. Le rôle du modèle :

Le modèle contient les données manipulées par le programme. Il assure la gestion de ces données et garantit leur intégrité. Dans le cas typique d'une base de données, c'est le modèle qui la contient.

Le modèle offre des méthodes pour mettre à jour ces données (insertion suppression, changement de valeur). Il offre aussi des méthodes pour récupérer ses données.

III.4.2. Rôle de la vue :

La vue fait l'interface avec l'utilisateur. Sa première tâche est d'afficher les données qu'elle a récupérées auprès du modèle. Sa seconde tâche est de recevoir toutes les actions de l'utilisateur (clic de souris, sélection d'une entrées, boutons, …). Ses différents événements sont envoyés au contrôleur.

III.4.3. Rôle du contrôleur :

Le contrôleur est chargé de la synchronisation du modèle et de la vue. Il reçoit tous les événements de l'utilisateur et enclenche les actions à effectuer. Si une action nécessite un changement des données, le contrôleur demande la modification des données au modèle et ensuite avertit la vue que les données ont changé pour que celle-ci se mette à jour. Certains événements de l'utilisateur ne concernent pas les données mais la vue. Dans ce cas, le contrôleur demande à la vue de se modifier.

Les différentes interactions entre le modèle, la vue et le contrôleur sont résumées par le schéma de la figure suivante :

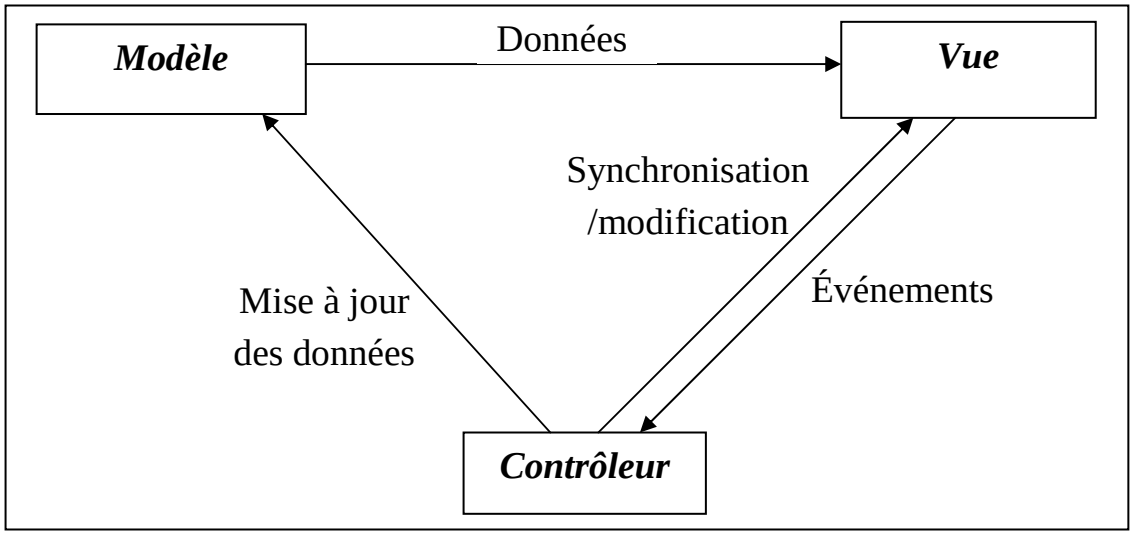


Figure III.20 : Le modèle vue contrôle (MVC)

III.5. Les tables de la base de données :

- ***Table Administrateur :***

Nom du champ	***Type***	***Description***	***Clés***
Id_admin	Int(11)	Identifiant de l'administrateur	Primaire
Login_admin	Text	Login de l'administrateur	
Password_admin	Text	Password de l'administrateur	

- ***Table Client :***

Nom du champ	***Type***	***Description***	***Clés***
Id_clt	Int(11)	Identifiant du client	Primaire
Nom_ clt	Text	Nom du client	
prenom_clt	Text	Prénom du client	
Date_naiss	Date	Date de naissance du client	
Num_Tel	Text	Numéro de téléphone du client	
Adresse	Text	Adrèsse du client	
E_mail	Text	E_mail du client	
Login	Text	Login du client	
Password	Text	Password du client	

- ***Table Message :***

Nom du champ	***Type***	***Description***	***Clés***
Id_mess	Int(11)	Identifiant du message	Primaire
Recepteur	Text	Récepteur	
Emeteur	Text	Emetteur	
Objet	Text	Objet du message	
Message	Text	Message	
Date_mess	Date	Date d'envoi	

- ***Table Document :***

Nom du champ	***Type***	***Description***	***Clés***
Id_doc	Int(11)	Identifiant du document	Primaire
Titre_doc	Text	Titre du document	
URL_doc	Text	URL du document	
Date_m_jr	Date	Date de mise à jour du document	

- ***Table Question :***

Nom du champ	***Type***	***Description***	***Clés***
Id_quest	Int(11)	Identifiant de la question	Primaire
Enoncé_quest	Text	Enoncé de la question	
Reponse	Text	La réponse à la question	
Correction	Text	La correction de la question	

- ***Table Logiciel:***

Nom du champ	***Type***	***Description***	***Clés***
Id_log	Int( )	Identifiant du logiciel	primaire
Description_log	Text	Description du logiciel	
URL_log	Text	URL du logiciel	
Date_m_jr	Date	Date de mise à jour du logiciel	

❖ Diagramme de classe globale :

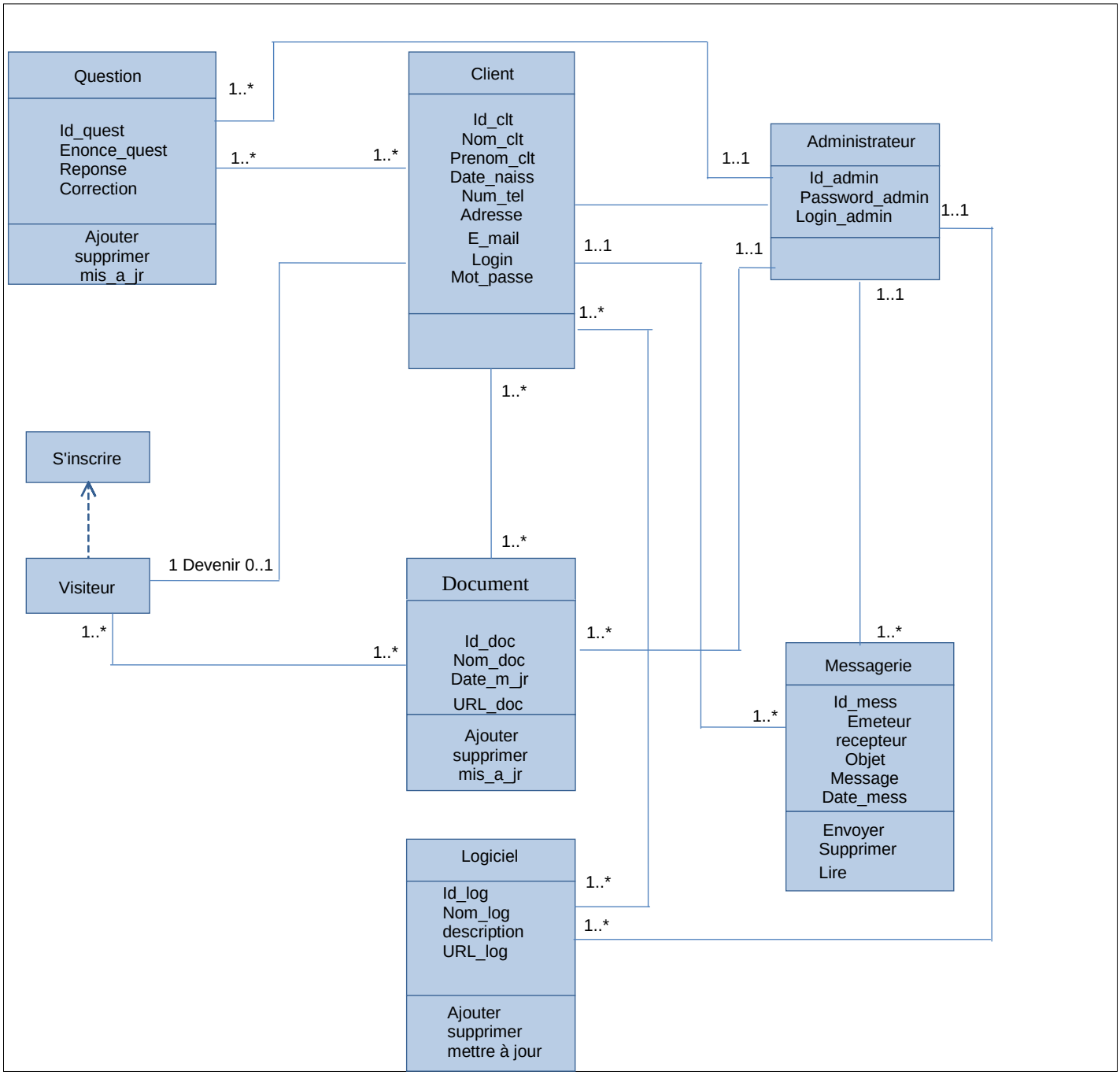


Figure III.21. Diagramme de classe général.

III.6.Conclusion :

Dans ce chapitre nous avons présenté une démarche de modélisation pour développer notre application, cette démarche est basée sur le langage de modélisation UML pour le Web. Nous avons abordé cette démarche par la spécification des besoins et les divers cas d'utilisations, en suite la conception des diagrammes de séquences en phase d'analyse. Pour la conception nous nous somme attelées à construire les diagrammes de séquences et les diagrammes de classes, et en fin le diagramme de classe final du schéma conceptuel de la base de données, il ne reste qu'à mettre en œuvre une plate forme qui nous permettra la réalisation de notre application, ce qui sera l'objet du prochain chapitre.

Chapitre IV
Réalisation
&
Mise en œuvre

VI.1. Introduction :

Après avoir explicité dans le chapitre précédent la conception de notre application, nous allons présenter dans ce chapitre la méthode MEHARI qui a été la base de notre démarche, l'environnement de développement et d'implémentation et les langages de programmations qui nous ont servi d'appui pour le développement de notre application.

IV.2. Présentation de la méthode MEHARI : [WEB 09]

Dans le but de réaliser notre application, nous nous sommes appuyés sur les questionnaires de la méthode MEHARI (**ME**thode **H**armonisée d'**A**nalyse de **Ri**sques),

IV.2.1. Historique :

La méthode MEHARI a été élaborée par la Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français) en 1992. La méthode d'analyse des risques MEHARI hérite des connaissances acquises après plus de quinze ans d'analyse des résultats de la méthode MARION.

IV.2.2. Principe de la méthode :

Les questionnaires de la méthode MEHARI sont basés sur 12 scénarii, pour modeler un questionnaire d'environ 400 questions, découpé en six domaines et pour donner un léger aperçu de ce que pourrait être un audit. Voici les six domaines identifiés :

- Domaine d'Organisation ;
- Domaine des Locaux ;
- Domaine du Réseau Local (LAN) ;
- Domaine de l'Exploitation des Réseaux ;
- Domaine de la sécurité des Systèmes et de leur architecture ;
- Domaine de la Protection de l'Environnement de Travail ;

Pour chaque question, le responsable devait répondre par « oui » ou par « non ».

IV.2.3. Les objectif de la méthode MEHARI :

MEHARI est une démarche d'analyse et de gestion des risques, qui fournit un cadre méthodologique, des outils et les bases de connaissance pour :

1. ***L'analyse des enjeux :***

L'analyse des enjeux de MEHARI permet d'évaluer la gravité des dysfonctionnements potentiels pouvant être causés ou favorisés par une faille ou un défaut de sécurité.

2. ***L'analyse des vulnérabilités :***

L'analyse des vulnérabilités fournit une évaluation de la qualité (robustesse, efficacité, mise sous contrôle) des mesures de sécurité en place.

3. L'identification et le traitement des risques :

Avec MEHARI, l'analyse des risques permet d'identifier les situations susceptibles de remettre en cause un des résultats attendus de l'entreprise, ou de l'entité et d'évaluer la probabilité de ces situations, leurs conséquences possibles et leur caractère, acceptable ou non.

L'analyse des risques met également en évidence les mesures susceptibles de ramener chaque risque à un niveau acceptable.

Cette analyse des risques s'appuie sur un ensemble de scénarios précis et peut servir à :

- définir les mesures de sécurité, les mieux adaptées au contexte et aux enjeux dans une démarche de management de la sécurité de l'information (SMSI), par exemple dans une démarche ISO 27001.
- mettre en place un management des risques et garantir que toutes les situations de risques critiques ont été identifiées, prises en compte et un plan d'action défini.

IV.2.4. Structure de la méthode MEHARI :

Les modules de MEHARI peuvent être combinés, en fonction de choix d'orientation ou de politiques d'entreprise, pour bâtir des plans d'action ou, tout simplement, pour aider la prise de décision concernant la sécurité de l'information.

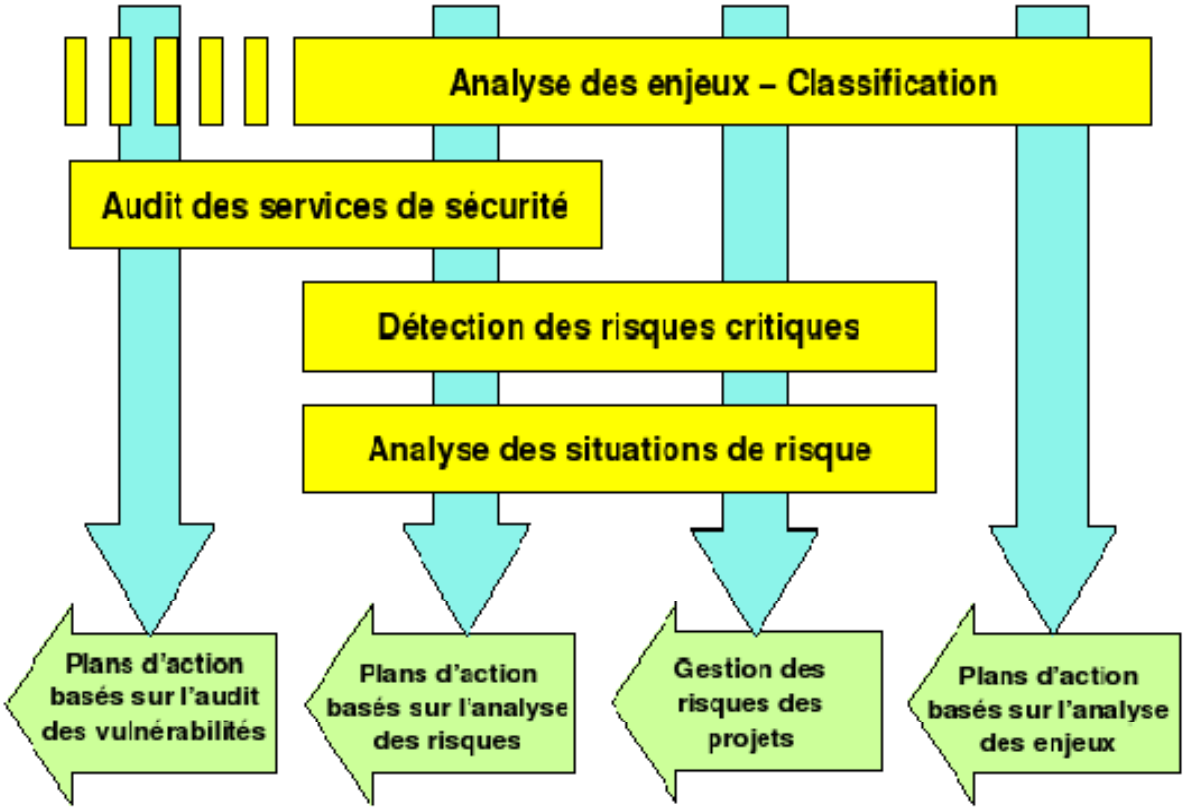


Figure IV.1 : La structure de la méthode MEHARI.

IV.3. Environnement de développement et d'implémentation :

Dans ce qui suit, nous allons décrire l'environnement utilisé pour le développement et l'implémentation de notre application, puisque notre application est une plateforme, nous allons développer des pages web dynamiques connectées à une base de données.

IV.3.1. Le serveur Web:

Un serveur Web est un logiciel permettant à des clients d'accéder à des pages Web, c'est-à-dire des fichiers au format HTML à partir d'un navigateur (aussi appelé browser) installé sur leur ordinateur distant.

Un serveur Web est donc un logiciel capable d'interpréter les requêtes HTTP arrivant sur le port associé au protocole HTTP, et de fournir une réponse avec ce même protocole. Les principaux serveurs Web sont : Apache, Microsoft IIS (Internet Information Server), Microsoft PWS (Personal Web Server).

Afin d'exécuter et de tester notre application durant la partie réalisation, nous avons opté pour l'utilisation d'Apache Web Server.

L'ancêtre Apache est le serveur libre développé par le NCSA (National Centre for Super computing Application) de l'université de l'Illinois. L'évolution de ce serveur s'est arrêtée lorsque le responsable a quitté le NCSA en 1994, les utilisateurs ont continué à corriger les bugs et à créer des extensions qu'ils distribuaient sous forme de "patch"(bouts de programmes ajoutés par les utilisateurs des NCSA pour étendre les fonctionnalités d'Apache) d'où le nom "a patchee Server" ou encore " un serveur rafistolé" la version 1.0 de Apache a été disponible le 1 Décembre 1995.

Notre choix d'utiliser le serveur Apache se justifie par plusieurs raisons :

- Il est ouvert et portable (il tourne sur la plupart des systèmes Unix et Windows), contrairement au serveur Microsoft IIS (Internet Information Server).
- De plus, il est considéré comme stable et sécurisé.
- Apache est aujourd'hui le serveur le plus répandu sur Internet ;
- Un niveau élevé de performance des exigences matérielles modestes ;
- C'est un serveur gratuit (peut être téléchargé à partir du site du groupe Apache à l'adresse "http : //www.apache.org") ;
- Il est extensible, modulaire et configurable ;
- Il est en outre associé au langage de scripte PHP que nous utiliserons pour l'implémentation de notre plate-forme.

IV.3.2. Serveur de base de données :

IV.3.2.1. Serveur MySQL : [22]

MYSQL est un véritable serveur de base de données SQL (Structured Query Language) multiutilisateurs et multitraitements qui est un langage de requêtes vers les bases de données exploitant le modèle relationnel. Il en reprend la syntaxe mais n'en conserve pas toute la puissance puisque de nombreuses fonctionnalités de SQL n'apparaissant pas dans MYSQL (sélections imbriquées, clés étrangères…).

MYSQL est une configuration client/serveur qui est souvent utilisée avec le langage de création de pages Web dynamiques PHP comme le montre la figure suivante :

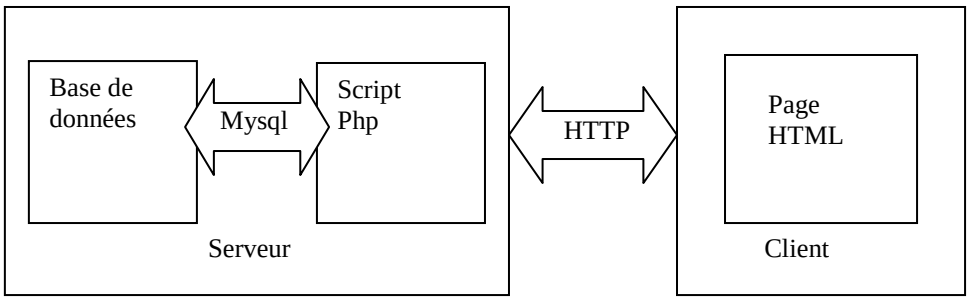


Figure IV.2: Serveur MYSQL.

IV.3.2.2. Fonctionnalités de MySQL : [23]

La liste suivante décrit quelques fonctionnalités importantes de MySQL :

- ***Multitraitements* :** MySQL est multitraitement en utilisant les threads du noyau. Il peut utiliser plusieurs CPU (Central Processing Unit).
- ***Langues* :** le serveur peut fournir au client les messages d'erreurs en plusieurs langues.
- ***Langages (API : Application Programming Interface) :*** les applications de bases de données MySQL peuvent être écrites en C, C++, Eiffel, JAVA, PERL, PHP, PYTHON et TCL.
- ***Multi plateformes* :** prise en charge de plus de 20 plates-formes de système d'exploitation Windows, UNIX et LINUX.
- ***Table* :** MySQL stocke chaque table sous forme de fichier distinct dans le répertoire de bases de données. La taille maximale d'une table comprise entre 4Go et la taille maximale de fichier acceptée par le système d'exploitation. Le mélange des tables de différentes bases est supporté dans une même requête.
- ***Système de droits flexible et sécurisé :*** Système de droits flexible et sécurisé de mots de passe, et qui autorise une vérification faite sur l'hôte : le serveur détermine

l'identité du client grâce à l'hôte depuis lequel il se connecte et le nom d'utilisateur qu'il spécifie. Puis, l'associer avec les droits d'utilisation des commandes : Select, Insert, Update et Delete sur cette base (le serveur vérifie chaque requête émise pour voir si elle est autorisée).

IV.3.3. Les langages utilisés : [Web 07]

IV.3.3.1. Le langage PHP : (Prsonnal Home Page) :

PHP est un langage de script coté serveur, incorporé au document HTML, mais exécuté par le serveur Web et non par le client. Conçu pour réaliser des pages dynamiques, le résultat du script est un document HTML standard, sans trace du script exécuté préalablement garantissant ainsi une compatibilité avec tous les navigateurs disponibles. Les raisons qui nous ont amenées à choisir le langage PHP (parmi d'autres langages tel qu'ASP : Active Server Page) sont nombreuses. Nous citons les suivantes :

- ***Le PHP est rapide*** **:** Compilé en tant que module Apache, les temps d'exécution sont plus courts que les temps d'exécution de ASP, surtout sous Unix. Les scripts PHP sont donc exécutés par le serveur Web, sans ressources supplémentaires.
- ***Simplicité d'écriture de scripts ;***
- ***Le PHP est multi plates formes*** **:** il fonctionne sous Windows, Unix…. ce qui n'est pas le cas de ASP (propriété de Microsoft) ;
- ***Le PHP gère très bien les requêtes SQL*** **:** Nous pouvons facilement écrire des programmes qui affichent des données extraites de bases SQL, ou qui stockent des données postées par un formulaire dans une table SQL. Le PHP sait communiquer avec presque tous les SGBD (Oracle, MySQL, DB2, Informix, Ingres, Postgresql, SQL Server, Access ….) ;
- ***Le PHP fournit une multitude de fonctions*** **:** couvrant presque tous les besoins pour un développeur de sites Internet : prise en charge de XML, génération de PDF (Portables Document Format), création d'images, compression/décompression, statistiques, cryptologie, génération d'email… ;
- ***Le PHP est ouvert (gratuit)*** **:** contrairement à ASP qui a un noyau gratuit mais des composants complémentaires payants ;
- ***Intégration au sein de nombreux serveur Web (Apache, Microsoft IIS,..)*** ;
- ***Simplicités d'interfaçage*** avec des bases de données (de nombreux SGBD sont supportés, mais le plus utilisé avec ce langage est MySQL, un SGBD (Système de Gestion de Base de Données) gratuit disponible sur les plates formes Unix, Linux et Windows).

- ***Fonctionnement de PHP :***

Le serveur Web reconnait de l'extension des fichiers, différente de celle des pages HTML, si le document appelé par le client comporte du code PHP.

1. Le serveur Web lance l'interpréteur PHP ;
2. L'interpréteur PHP traduit le document demandé et exécute le code source de la page ;
3. Les commandes figurant dans la page interprétées et le résultat prend la forme d'une page HTML publiée à la place du code source dans le même document ;
4. La page modifiée est envoyée au client pour y être affichée par le navigateur ;

De cette façon, la page Web est crée dynamiquement, c'est-à-dire au moment même où le client est en dialogue avec le serveur.

IV.3.3.2. Le langage HTML (Hyper Text Markup Language) :

HTML est un langage de description de document (et non pas un langage de programmation), il utilise des marques explicites (appelés tags ou balises qui précisent la structure et la mise en forme du contenu du document. Ces marqueurs seront reconnus par les navigateurs, et interprétés comme des directives, afin de réaliser la présentation attendue sur le poste client. Il permet d'inclure des informations variées (textes, images, sons, animations….) et d'établir des relations cohérentes entre ces informations grâce aux liens hypertextes.

Exemple d'un fichier HTML :

```
<HTML>
<HEAD>
<TITLE>EXEMPLE</TITLE>
</HEAD>
<BODY>
BONJOUR MONSIEUR
</BODY>
</HTML>
```

Les balises <HTML> et </HTML> stipulent que ce fichier texte est formaté selon le langage HTML et délimitent le contenu à interpréter.

Les balises <HEAD> et </HEAD> viennent du mot HEADER (entête) et délimitent l'entête du document contenant son titre et des informations sur son contenu.

Les balises <BODY> et </BODY> délimitent le corps du document contenant le texte, son formatage, les objets et les liens qu'il inclut.

IV.3.3.3. Le langage JavaScript:

Le JavaScript est le langage favori des créateurs de sites web. Il permet en quelques lignes de code de dynamiser une page. C'est un langage interprété par les navigateurs qui n'exige aucune configuration spéciale des serveurs web. Les avantages qu'offre ce langage sont nombreux, nous pouvons en citer les suivants :

1. Il est indépendant de la plate-forme.
2. Il est facile à débugger.
3. Il est facile à apprendre (surtout pour des personnes ayant des notions en C).

Les balises annonçant un code JavaScript sont les suivantes :

<SCRIPT langage= JavaScript > Placez ici votre code </SCRIPT>

IV.3.4. Les outils de développement : [24]

IV.3.4.1 EasyPHP:

EasyPHP est un package qui installe et configure automatiquement un environnement de travail complet sous Windows, permettant de mettre en œuvre toute la puissance et la souplesse qu'offre le langage dynamique PHP et son support efficace des bases de données. EasyPHP regroupe un serveur Web apache, une base de données MYSQL, le langage PHP ainsi que des outils facilitant le développement des sites ou des applications.

Nous avons développé notre application, on utilisant la version EasyPHP 5.3.3.1.

IV.3.4.1.1 Installer EasyPHP :

- Télécharger EasyPHP sur le site *www.easyphp.org*.
- Double cliquer sur l'exécutable téléchargé.
- Sélectionner le répertoire d'installation et suivre la procédure.

IV.3.4.1.2 Lancer EasyPHP :

Nous ne pouvons pas à proprement parler du lancement d'EasyPHP, il s'agit en fait de la mise en route du serveur Apache et de MySQL. A l'installation, un raccourci vers EasyPHP est créé dans le répertoire "Démarrer/Programmes/EasyPHP".

Une fois EasyPHP lancé, une icône se place dans la barre de taches.

Un clic droit permet d'accéder à différents menus :

- Aide : aide d'EasyPHP ;

- Fichiers Log : renvoie les erreurs générées par Apache, MySQL et EasyPHP ;
- Configuration : donne accès aux différents outils de configuration ;
- Explorer : ouvre le répertoire "www" via l'explorateur Windows ;
- Administration : ouvre la page d'administration ;
- Web local : ouvre le web local ;
- Redémarrer: redémarre Apache et MySQL ;
- Démarrer/Arrêter : démarre/arrête Apache et MySQL ;
- Quitter : ferme EasyPHP.

IV.3.4.1.3 Utiliser le répertoire WWW ou des alias :

Pour que les pages PHP soient interprétées, il est impératif de placer les fichiers dans le répertoire "www" ou dans un alias créé. Pour visualiser les pages il suffit alors d'ouvrir le "***Web local***" ou d'accéder aux alias via la page d' "Administration".

Un alias

IV.3.4.1.4 PhpMyAdmin :

PhpMyAdmin est un utilitaire rendant plus conviviale l'administration de base de données MySQL. Il consiste en un ensemble de scripts PHP permettant d'administrer des bases de données MySQL en passant par un navigateur Web.

- ***Les fonctions principales de PhpMyAdmin:***
  - Création de nouvelles bases de données ;
  - Création/suppression/modification des tables ;
  - L'édition, l'ajout et la suppression de champs ;
  - L'exécution de commandes SQL et de requêtes ;
  - Chargement de fichier dans des tables ;

- Gérer les privilèges des utilisateurs.

➢ Utilisation de PhpMyAdmin :

Pour accéder à PhpMyAdmin, il faut d'abord vérifier qu'Easyphp.exe est lancé et que le serveur fonctionne, après nous pouvons accéder à partir de " l'administrateur ". Pour ouvrir l'administrateur il suffit de faire un clic droit sur l'icône et sélectionner "administration". Une page Web apparait, au milieu de celle-ci il y a un bouton PhpMyAdmin avec un simple clique là-dessus, la page d'accueil de PhpMyAdmin s'affiche dans la fenêtre du navigateur, accompagnée d'un champ de sélection de bases de données présentes sur l'hôte MySQL par défaut, comme l'illustre la figure suivante :

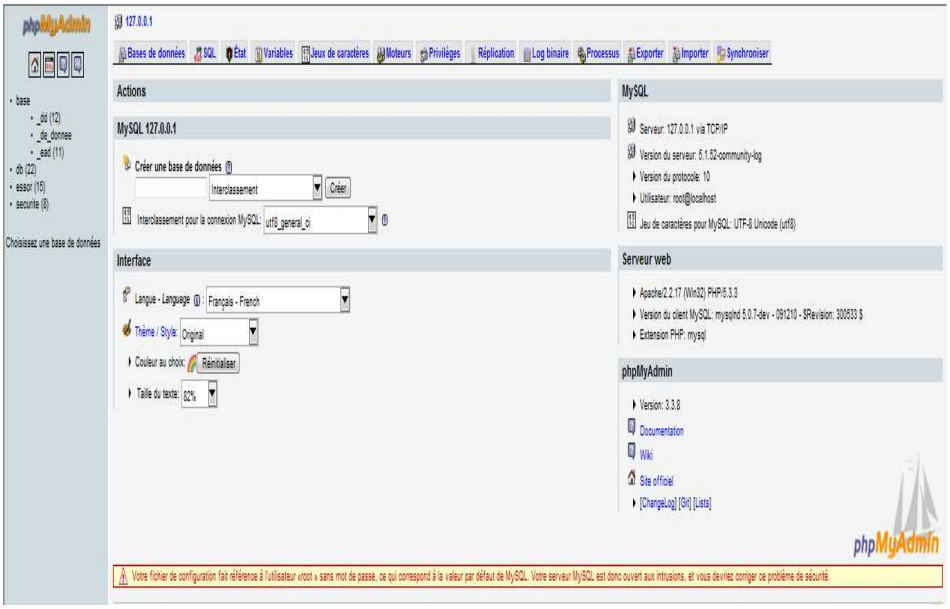


Figure IV.3 : Administration de MySQL à partir de PhpMyAdmin.

Pour afficher le contenu de la base personnelle par exemple, il faut cliquer sur la ligne correspondante à la base de données personnelle dans la partie gauche de la fenêtre du navigateur. Toutes les tables de cette base de données seront affichées :

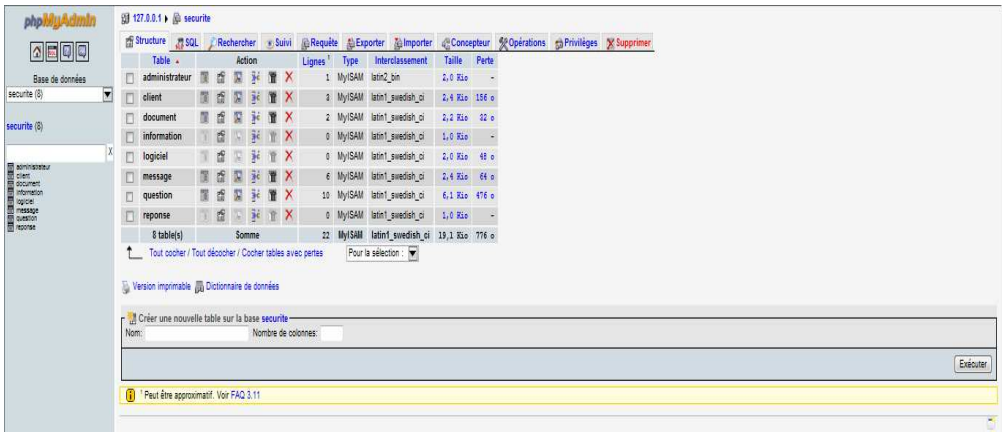


Figure IV.4 Accès à notre base de données à partir de PhpMyAdmin.

IV.3.4.2. Dreamweaver : [25]

Macromedia Dreamweaver8 est un éditeur HTML professionnel destiné à la conception, au codage et au développement des sites, de pages et d'applications Web. Sous Windows, Dreamweaver propose une présentation en une seule fenêtre. Dans l'espace de travail intégré, toutes les fenêtres et tous les panneaux sont rassemblés dans une grande fenêtre d'application. C'est un éditeur de page HTML, convivial et simple à utiliser.

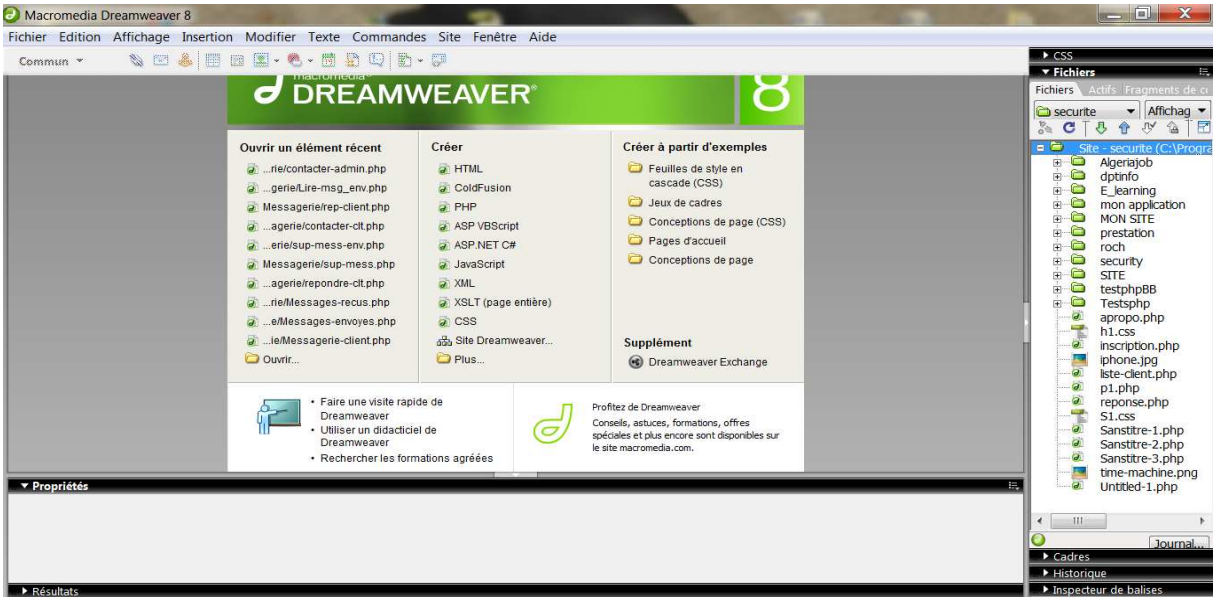


Figure IV.5: Espace de travail de Dreamweaver.

IV.3.4.3. Macromedia Flash 8:

C'est un logiciel qui permet d'apporter des solutions et développer des contenus et des applications Internet et les rendre riches. Que se soit pour créer des graphiques animés ou des applications de données, les solutions Flash mettent à la disposition de ses utilisateurs tous les outils nécessaires pour permettre d'obtenir les meilleurs résultats.

Figure IV.6: Espace de travail de Macromedia Flash 8.

IV.3.4.4. Navigateurs:

Un navigateur Web est un logiciel conçu pour consulter le World Wide Web. Techniquement, c'est au minimum un client HTTP. Le terme *navigateur web (ou navigateur Internet)* est inspiré de Netscape Navigator. D'autres termes sont utilisés notamment *browser*, en anglais.

Parmi les navigateurs les plus confrontés :

- ***Internet explorer :***

Windows Internet Explorer, ou plus simplement Internet Explorer, est le navigateur Web de Microsoft, installé par défaut avec Windows.

- ***Mozilla Firefox :***

Mozilla Firefox est un navigateur Web gratuit, développé et distribué par Mozilla Foundation aidée de centaines de bénévoles grâce aux méthodes de développement du logiciel libre/Open Source et à la liberté du code source.

IV.4. Présentation de quelques interfaces de notre plate-forme :

Dans ce qui suit, nous présenterons les principales interfaces de notre plate-forme:

IV.4.1. L'espace visiteur

1. La page d'accueil :

C'est la première page qui apparaît dans le navigateur lors de la connexion à la plateforme. La page d'accueil de notre plate-forme résume le fonctionnement du système, nous y trouvons une explication des fonctionnalités de l'environnement, avec des liens actifs vers d'autres pages donnant plus d'explication.

Nous trouvons la barre de navigation qui contient les liens suivants :

- En haut de la page les liens permettent aux visiteurs d'accéder aux différentes pages contenants différentes informations.
- La partie droite de la page est réservée aux clients pour s'identifier et accéder à leurs espaces.
- Au centre de la page nous trouvons une description totale de notre plateforme.

Figure IV.7 : Page d'accueil de notre plateforme

2. *La page d'inscription :*

Cette page contient un formulaire contenant toutes les informations relatives aux clients, un visiteur voulant s'inscrire doit remplir le formulaire pour qu'il puisse faire l'inscription, certain champs sont obligatoires et d'autres non.

Figure IV.8 : Page d'inscription du client

IV.4.2. L'espace client :

1. Page d'accueil de client :

Cette page est affichée après identification d'un client. Elle permet aux clients de s'informer, de télécharger des logiciels, de consulter la messagerie, et de passer le test d'évaluation de la sécurité de leur entreprise.

Figure IV.9 : Page d'accueil client

2. Page de téléchargement:

Cette page permet aux clients de télécharger des logiciels.

Figure IV.10 : Page de téléchargement

3. Page Test :

Cette page permet aux clients de passer le test d'évaluation en répondant aux questions proposées.

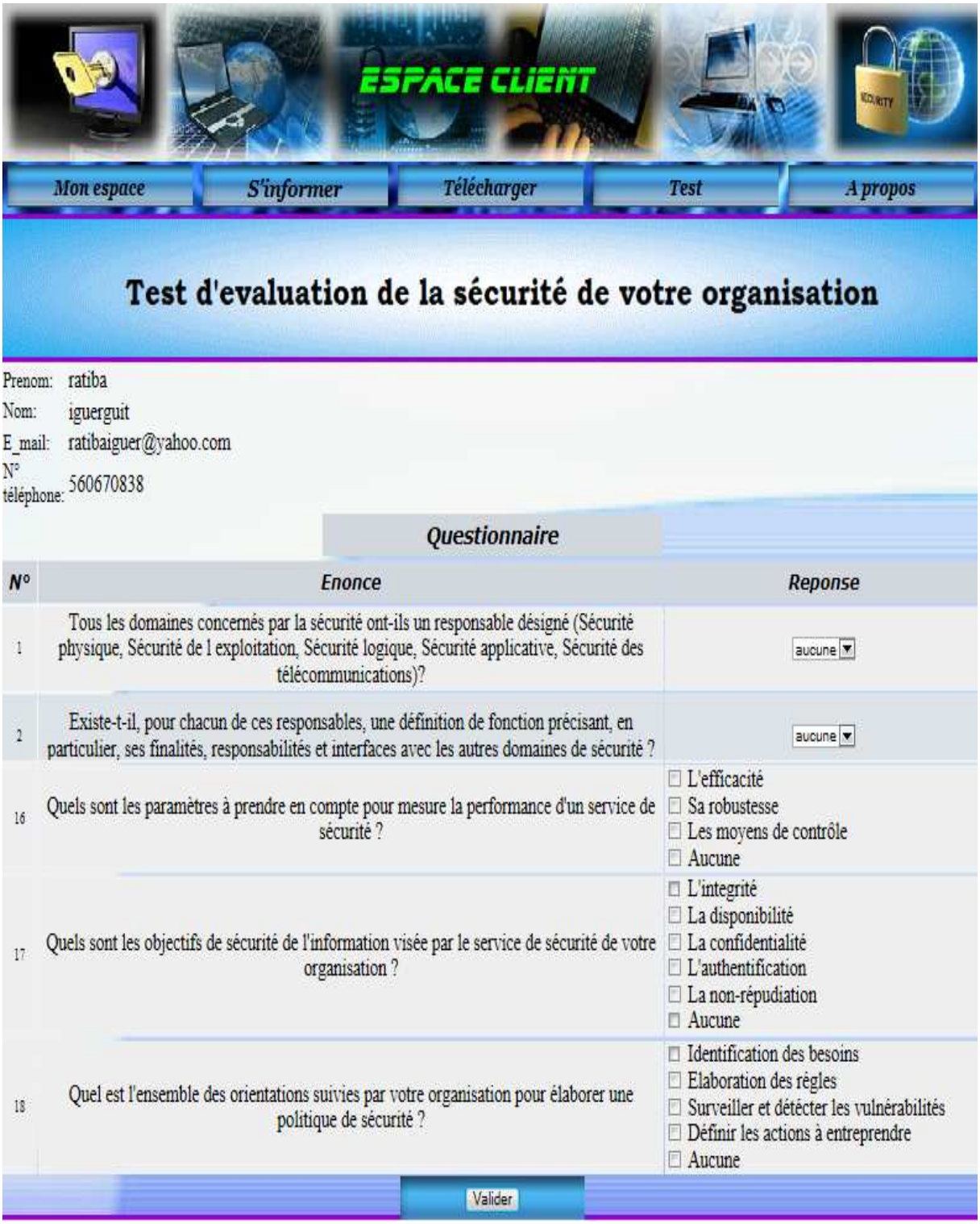
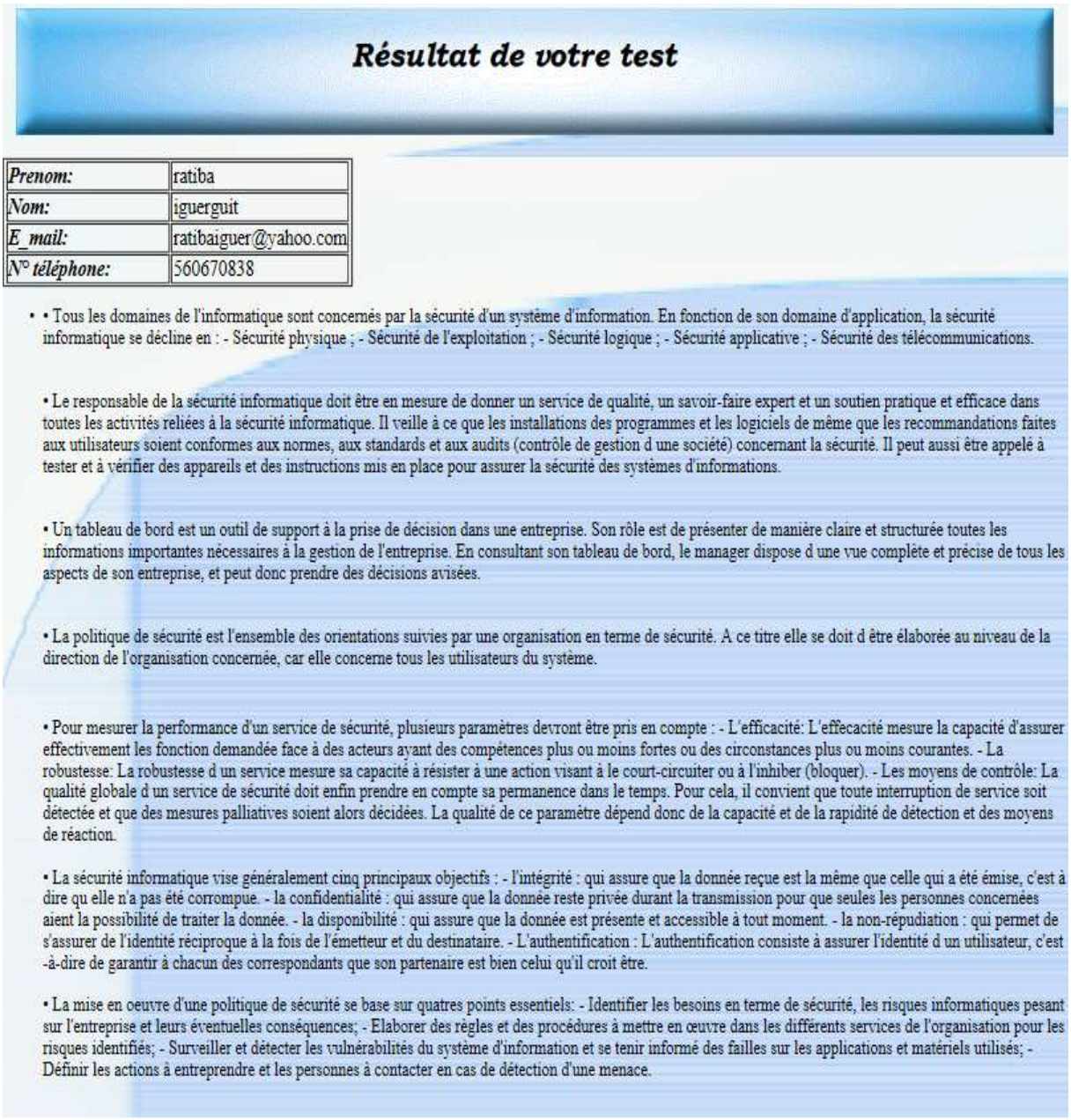


Figure IV.11 : Page Test.

4. Page résultat du test :

Permet au client de voir le résultat de son test avec un rapport qui décrit les fonctions et procédures à prendre en compte pour bien suivre la sécurité de son organisation.



Résultat de votre test

Prenom:	ratiba
Nom:	iguerguit
E_mail:	ratibaiguer@yahoo.com
N° téléphone:	560670838

• • Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique se décline en : - Sécurité physique ; - Sécurité de l'exploitation ; - Sécurité logique ; - Sécurité applicative ; - Sécurité des télécommunications.

• Le responsable de la sécurité informatique doit être en mesure de donner un service de qualité, un savoir-faire expert et un soutien pratique et efficace dans toutes les activités reliées à la sécurité informatique. Il veille à ce que les installations des programmes et les logiciels de même que les recommandations faites aux utilisateurs soient conformes aux normes, aux standards et aux audits (contrôle de gestion d une société) concernant la sécurité. Il peut aussi être appelé à tester et à vérifier des appareils et des instructions mis en place pour assurer la sécurité des systèmes d'informations.

• Un tableau de bord est un outil de support à la prise de décision dans une entreprise. Son rôle est de présenter de manière claire et structurée toutes les informations importantes nécessaires à la gestion de l'entreprise. En consultant son tableau de bord, le manager dispose d une vue complète et précise de tous les aspects de son entreprise, et peut donc prendre des décisions avisées.

• La politique de sécurité est l'ensemble des orientations suivies par une organisation en terme de sécurité. A ce titre elle se doit d être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

• Pour mesurer la performance d'un service de sécurité, plusieurs paramètres devront être pris en compte : - L'efficacité: L'effecacité mesure la capacité d'assurer effectivement les fonction demandée face à des acteurs ayant des compétences plus ou moins fortes ou des circonstances plus ou moins courantes. - La robustesse: La robustesse d un service mesure sa capacité à résister à une action visant à le court-circuiter ou à l'inhiber (bloquer). - Les moyens de contrôle: La qualité globale d un service de sécurité doit enfin prendre en compte sa permanence dans le temps. Pour cela, il convient que toute interruption de service soit détectée et que des mesures palliatives soient alors décidées. La qualité de ce paramètre dépend donc de la capacité et de la rapidité de détection et des moyens de réaction.

• La sécurité informatique vise généralement cinq principaux objectifs : - l'intégrité : qui assure que la donnée reçue est la même que celle qui a été émise, c'est à dire qu elle n'a pas été corrompue. - la confidentialité : qui assure que la donnée reste privée durant la transmission pour que seules les personnes concernées aient la possibilité de traiter la donnée. - la disponibilité : qui assure que la donnée est présente et accessible à tout moment. - la non-répudiation : qui permet de s'assurer de l'identité réciproque à la fois de l'émetteur et du destinataire. - L'authentification : L'authentification consiste à assurer l'identité d un utilisateur, c'est -à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

• La mise en oeuvre d'une politique de sécurité se base sur quatres points essentiels: - Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences; - Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés; - Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés; - Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

Figure IV.12 : Page résultat du test.

5. Page information:

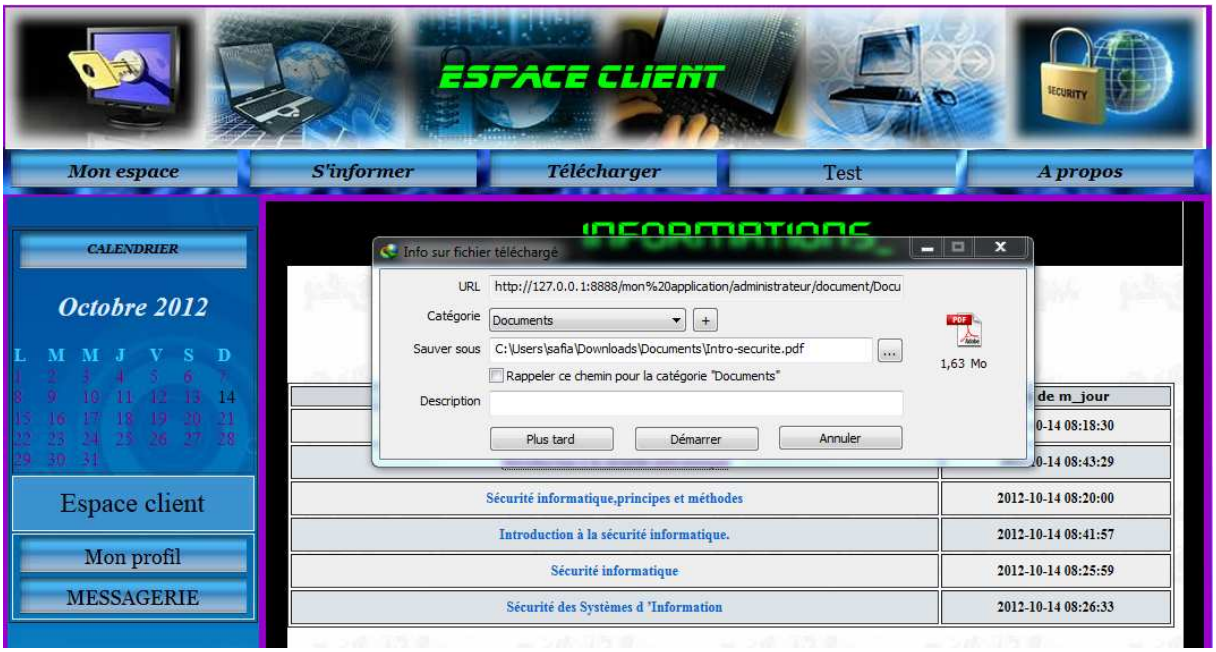


Figure IV.13 : Page information.

IV.4.3.L'espace administrateur :

1. La page d'accueil de l'administrateur :

Cet espace permet à l'administrateur de : Gérer les clients, Gérer les outils, Gérer les documents, Gérer le questionnaire et de consulter la messagerie.

Figure IV.14 : Page d'accueil administrateur.

2. *La page ajouter question :*

Cet espace permet à l'administrateur d'ajouter des questions.

Figure IV.15 : Page ajouter question.

IV.5.Conclusion :

Au niveau de ce chapitre, nous avons présenté l'environnement d'implémentation et de développement de notre application, en se focalisant sur les techniques de programmation utilisées pour implémenter les pages et nous avons décrit quelques interfaces d'utilisation de notre plateforme.

Conclusion générale

Conclusion générale

La sécurité à 100% reste un idéal à atteindre, surtout devant le large éventail des menaces qui mettent en danger l'exploitation d'un système d'information. Ainsi il est important de bien formaliser une politique de sécurité en prenant en compte les risques réelles qu'encourt un système informatique et en évaluant les coûts que peuvent engendrer les problèmes résultants de ces risques par rapport au coût nécessaire à la mise en place des solutions à ces problèmes.

Notre travail a été développé dans le contexte de réaliser et concevoir une plate forme pour la gestion de la sécurité informatique des entreprises, à l'aide d'un test d'évaluation qui permet aux responsables des services de sécurité de bien gérer ces derniers en prenant en compte le résultat de ce test. Pour réaliser ce test nous avons extrait quelques questions de la méthode de MEHARI.

Sa réalisation nous a permis d'acquérir des connaissances dans le nouveau monde des technologies du web et de l'information, et les notions de base de la sécurité informatique des entreprises, et les outils de programmation : HTML, PHP, JavaScript et MySQL pour l'interrogation des bases de données. Ainsi que consolider nos connaissances dans les méthodes d'analyse et de conception à savoir le langage de modélisation UML et son extension pour le web.

Toutefois, bien que notre application présente plusieurs fonctionnalités, elle reste toujours sujette à des améliorations et compléments pour en tirer un maximum d'avantages.

Nous espérons que ce modeste travail sera de grand intérêt pour les responsables des entreprises qui souhaitent protéger leur système face aux risques et menaces informatique qui les entourent.

Annexe

I. Introduction :

Les éléments standards d'UML ne sont pas suffisants pour exprimer les subtilités indispensables aux pages web comportant des scripts dans un diagramme de classe. Comme elles accomplissent des opérations métiers non négligeables et qu'elles se comportent comme de vrais objets du système, il est nécessaire qu'elles coexistent avec les classes et les objets du système, la seule solution pour rendre cela possible et de modifier UML.

La conception d'application web se distingue de la conception d'autres systèmes par deux activités majeurs : La répartition des objets sur le client ou le serveur et La définition de l'interface sous forme de pages web.

II. Présentation de l'UML : [25]

II.1. Définition de l'UML (Unified Modeling Language) :

UML est un langage ou formalisme de modélisation orienté objet qui représente un moyen de spécifier et représenter les composantes d'un système informatique. Il permet notamment la spécification de toutes les décisions importantes en matière d'analyse, de conception et d'implémentation, décisions qui doivent être prises lors du développement d'un système à forte composante logicielle.

II.2.La modélisation UML :

UML fournit des outils permettant de représenter l'ensemble des éléments du monde réel (classes, objets,…..etc) ainsi les liens qui les relient, il s'articule autour de plusieurs types de diagrammes tel que :

- ***Les diagrammes de cas d'utilisation :***

Ils décrivent, sous la forme d'actions et de réactions, le comportement d'un système du point de vue utilisateur. Ils permettent de définir les limites du système et les relations entre un système et son environnement. Nous utilisons les diagrammes de cas d'utilisation pour répondre à la question « comment les acteurs d'un système interagissent avec lui ?».

- ***Les diagrammes de séquence* :**

Ils peuvent servir à illustrer un cas d'utilisation, ils sont des diagrammes d'interaction UML. Ils représentent les échanges de messages entre objets dans le cadre d'un fonctionnement particulier du système. Le diagramme de séquence sert à développer les scenarios du système.

- ***Les diagrammes de classe :***

Ils constituent le cœur du langage UML. Ils offrent une vue statique du système, en représentant les classes et les relations entre elles.

- ***Les diagrammes d'activités :***

Variante du diagramme états-transitions, il permet de représenter le déclenchement d'événements en fonction des états du système et de modéliser des comportements multiprocessus.

II.3. Extension de l'UML pour le web :

Une extension d'UML définit un ensemble de stéréotype et de contraintes, qui rend possible la modélisation d'application web.

- ***Un stéréotype :***

C'est une extension du vocabulaire d'UML, il permet d'associer une nouvelle signification à un élément du modèle. Les stéréotypes peuvent être appliqués à presque tous les éléments du modèle et sont habituellement représentés par une chaine de caractères entre guillemets (« »).

- **Une étiquette :**

C'est une extension des propriétés d'un élément. Elle permet la description d'une nouvelle propriété d'un modèle. Elle est représentée dans un diagramme par une chaine de caractères entre chevrons (< >).

- **Une contrainte :**

C'est une extension de la sémantique d'UML. Elle prescrit la règle que le modèle doit vérifier pour être qualifie. Elle est représentée par une chaine de caractères entre accolades ({ }).

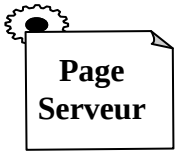
Le principal élément spécifique des applications web étant la page web, plusieurs stéréotypes lui sont destinés.

II.3.1.Stéréotype :

II.3.1.1.Classe :

*II.3.1.1.1.***Page serveur « Server page » :**

- ***Icône* :**



- ***Description* :**

Représente une page Web possédant des scripts qui interagissent avec des ressources serveur telles que les bases de données, ces scripts sont exécutés par le serveur.

- ***Contraintes*** **:**

  Les pages serveur ne peuvent avoir de relation qu'avec des objets sur le serveur.

- ***Étiquette*** **:**

  Moteur de script qui peut être un langage ou le moteur qui doit être utilisé pour exécuter ou interpréter cette page.

II.3.1.1.2. Page client « client page » :

- ***Icône :***

- ***Description :***

  Une instance d'une page client est une page Web formatée en HTML. Les pages clients peuvent contenir des scripts interprétés par les navigateurs lorsque celles-ci sont restituées par ces derniers. Les fonctions des pages clients correspondent aux fonctions des scripts de la page web.

- ***Contraintes :***

  Aucune.

- ***Etiquette :***

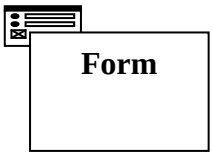
  -Titre de page : tel qu'il est affiché par le navigateur**.**

  -Base : URL de base pour référencer l'URL relatives.

  -Corps : ensemble des attributs de la balise <body> qui définit des caractéristiques par défaut du texte et de l'arrière plan.

II.3.1.1.3.Les formulaire « Form » :

- ***Icône :***



- ***Description :***

  Un stéréotype « Form » est un ensemble de champs de saisie faisant partie d'une page client. A une classe formulaire correspond une balise « Form » en HTML. Les attributs de cette classe correspondent aux éléments de saisie d'un formulaire HTML (zone de saisie, zone de texte, boutons d'option, etc.).

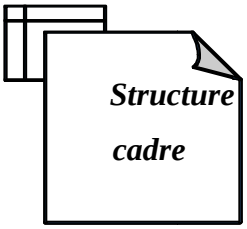
- ***Contrainte :***

  Aucune.

- ***Etiquette :***

Méthode GET ou POST utilisé pour soumettre les données à l'URL de l'attribut action de la balise HTML <Form>.

II.3.1.1.4. Structure de cadres « frameset » :

- ✓ **Icône :** 

- ✓ ***Description :***

  Une structure de cadres est un conteneur de plusieurs pages Web. La zone d'affichage rectangulaire est devisée en cadres rectangulaires inscrits. A chaque cadre peut être associé un nom unique de cible « Target ».

  Le contenu d'un cadre peut être une page Web ou une structure de cadre.

  Une classe stéréotypée « frameset » est directement associé à une structure de cadre de page Web par la balise HTML < frameset >.

  Une structure de cadre est une page client qui peut posséder des opérations et des attributs.

- ✓ **Contraintes :**

  Aucune.

- ✓ **Étiquette :**

  - Rangées (rows) : valeur de l'attribut rows de la balise HTML <framset>. C'est une chaine de pourcentages séparés par des virgules, définissant les hauteurs relatives des cadres.

  -Colonnes (cols) : valeur de l'attribut cols de la balise HTML <framset>. C'est une chaine de pourcentages séparés par des virgules, définissant les largeurs des cadres.

II.3.1.1.5. Cible « Target » :

- ✓ ***Icône :***

- ✓ ***Description :***

  Une cible est une zone nommée dans la fenêtre du navigateur dans laquelle des pages Web peuvent être affichées. Le nom de la classe stéréotypée est celui de la cible. Habituellement, une cible est le cadre d'une structure de cadre définie dans une fenêtre ; cependant, une cible peut être une toute nouvelle instance de navigateur : une fenêtre. Une association « targeted link » spécifie la cible où une page Web doit être affichée.

- ✓ **Contraintes :**

  Pour chaque client du système le nom de la cible doit être unique.

  Par conséquent sur un même client, il ne peut exister qu'une seule instance d'une même cible.

- ✓ **Étiquette :**

  Aucune.

II.3.1.1.6. Objet Java Script « JavaScript Object » :

- ✓ **Icône :**

  Aucune.

- ✓ ***Description :***

  Sur un navigateur compatible java script. De simuler des objets personnalisés à l'aide de fonctions java script. Les objets java script ne peuvent exister que dans le contexte de page client.

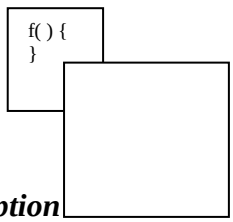
- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Etiquette :***

  Aucune.

II.3.1.1.7. Objet Script Client « Client Script Object » :

- ✓ ***Icône :*** 

- ✓ ***Description***

  Un objet script client est un ensemble qui regroupe des scripts client particuliers dans un fichier. Lequel est inclus dans une requête distincte du navigateur client. Ces objets regroupent des lots de fonctions couramment utilisés à travers d'une application ou d'une entreprise.

- ✓ ***Contraintes :***

  Aucune.

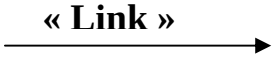
- ✓ ***Étiquette :***

  Aucune.

II.3.2. Les associations :

II.3.2.1. Lien « Link » :

- ✓ ***Icône :***



- ✓ ***Description :***

  Un lien est un pointeur d'une page client vers une autre page. Dans un diagramme de classes, un lien est une association entre une page client et une autre page client ou une page serveur. A un lien correspond une balise ancre HTML.

- ✓ **Contraintes :**

  Aucune.

- ✓ ***Étiquette :***

  Paramètres (paramètres) : liste de noms de paramètres qui doivent être passés avec la demande de la page liée.

II.3.2.2. Lien cible « targeted link »:

- ✓ ***Icône :***

- ✓ ***Description :***

  Similaire à une association lien. Un lien cible est un lien dont la page associée est affichée dans une cible. A un lien cible correspond une balise ancre HTML, dont l'attribut target prend la valeur de la cible.

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***

  -Paramètres (Paramètres) : liste de noms de paramètres qui doivent être passés avec la demande de la page liée.

  -Nom de la cible (target name) : nom de la cible ou la page vers laquelle pointe le lien qui doit être affichée.

II.3.2.3. Contenu de cadre « frame content » :

- ✓ ***Icône :***

  Aucune.

- ✓ ***Description :***

  Une association contenue de cadre est une association d'agrégation qui traduit l'appartenance d'une page ou d'une cible à un cadre.

  Une association contenue de cadre peut aussi pointer vers une structure de cadre, aboutissant dans ce cas, à des cadres imbriqués.

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***
  - Rangée (Row) : Entier qui indique la rangée du cadre dans la structure de cadre auquel appartient la page, ou la cible associée.
  - Colonne (col) : Entier qui indique la colonne du cadre dans la structure de cadre auquel appartient la page, ou la cible associée.

II.3.2.4. Soumet « submit » :

- ✓ **Icône :** **« Submit »** ⟶

- ✓ ***Description :***

  « submit » est une association qui se trouve toujours entre un formulaire et une page serveur. Les formulaires soumettent les valeurs de leurs champs au serveur, par l'intermédiaire de page serveur, pour qu'il les traite. Le serveur web traite la page serveur, qui accepte et utilise les informations du formulaire.

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***

  Une liste de noms de paramètres qui doivent passées par la demande de la page liée.

II.3.2.5. Construit « build » :

- ✓ ***Icône :***

  « Build » ⟶

- ✓ ***Description :***

  La relation « build » est une relation particulière qui fait le pont entre les pages client et les pages serveur. L'association « build » identifie quelle page serveur est responsable de la création d'une page client. C'est une relation orientée, puisque la page client n'à pas connaissance de la page qui est à l'origine de son existence. Une page serveur peut

construire plusieurs pages client, en revanche, une page client ne peut être construite que par une seule page serveur.

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***

  Aucune.

II.3.2.6. Rediriger « redirect » :

- ✓ ***Icône :***

- ✓ ***Description :***

  Une relation « redirect », est une association unidirectionnelle avec une autre page web, peut être dirigée à partir d'une page client ou serveur ou vers une page client ou serveur.

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***

  Délai (delay) : délai que doit observer une page client avant de rediriger vers la page destination. Cette valeur correspond à l'attribut content de la balise <META>

- ✓ ***Contraintes :***

  Aucune.

- ✓ ***Étiquette :***

  Aucune.

II.3.3. Attribut :

II.3.3.1. Elément de saisie « input element » :

- ✓ ***Icône :***

  Aucune.

- ✓ ***Description :***

  Un élément de saisie correspond à la balise <input>d'un formulaire HTML. Les étiquettes associées à cet attribut stéréotype, correspondant aux attributs de la balise <input>. Les attributs obligatoires de la balise HTML <input> sont renseignés de la manière suivante :

  -l'attribut « Name » prend la valeur du nom de l'élément de saisie et l'attribut « Value » prend celle de sa valeur initiale.

- ✓ ***Contraintes :***

Aucune.

- ✓ ***Étiquette :***

-Type (Type) : Le type de l'élément de saisie : texte, numérique, mot de passe, case à cocher, bouton d'option, bouton submit ou bouton reset.

-Taille(Size) : Définit la largeur visible allouée à l'écran en caractères.

-Longueur max (maxlength) : C'est le nombre maximal de caractères que peut saisir l'utilisateur.

II.3.3.2. Sélection d'éléments « select élément » :

- ✓ ***Icône :***

Aucune.

- ✓ **Description :**

Contrôle de saisie employé dans le formulaire, il permet à l'utilisateur de sélectionner une ou plusieurs valeurs dans une liste. La plupart des navigateurs restituent ce contrôle par une liste d'option ou une liste déroulante.

- ✓ ***Contrainte :***

Aucune.

- ✓ ***Étiquette :***

-Taille(Size) : définit le nombre d'élément qui doivent être affichés simultanément.

-Multiple (Multiple) : valeur booléenne qui indique que plusieurs éléments peuvent être sélectionnés conjointement.

II.3.3.3.Zone de texte « texte area element » :

- ✓ ***Icône :***

Aucune.

- ✓ ***Description :***

C'est un contrôle de saisie, employé dans les formulaires, qui permet l'écriture de plusieurs lignes de texte.

- ✓ ***Contraintes :***

Aucune.

- ✓ ***Étiquette :***

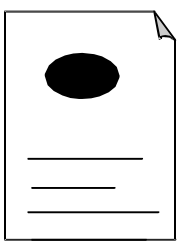
- Ligne (Rows) : Nombre de lignes de texte visibles.

-Colonne (cols) : Largeur visible du texte en largeur de caractères moyens.

II.3.4. Composant :

II.3.4.1. Page web « web page » :

- ✓ ***Icône :***



- ***Description :***

  Un composant page est une page web. Il peut être requis d'après son nom par un navigateur. Un composant page peut contenir des scripts client ou serveur. Le plus souvent, le composant page est un fichier texte accessible au serveur web, mais il peut être un module compilé, chargé et exécuté par le serveur web. Dans les deux cas, le serveur web produit, à partir du composant page, un document au format HTML, qui est renvoyé en réponse à la requête du navigateur.

- ***Contraintes :***

  Aucune.

- ***Étiquette :***

  Chemin (path) : Chemin requis pour spécifier la page web sur le serveur web. Cette valeur doit être relative au répertoire racine du site de l'application web.

II.4.Règles de cohérence sémantique :

II.4.1.Réalisation de composant :

En principe les composants pages web peuvent réaliser les classes stéréotypées « serveur page », « client page », « form », « JavaScript Object », « client script Object », « frameset » et « target ».

II.4.2. Généralisation :

Tous les éléments de modélisation impliqués dans une même généralisation doivent être du même stéréotype.

II.4.3. Association :

Une page client peut avoir au plus une relation « build » avec une page serveur, mais une page serveur peut avoir plusieurs relations « build » avec déférentes pages clients.

En plus de la combinaison standard d'UML, les combinaisons de stéréotypes présentées au tableau ci-dessous sont permises.

II.5. Les combinaisons valides d'associations de stéréotypes:

A / DE	« client page»	« Serveur page »	« Frameset»	« target »	« form »
« client page»	« Link » « redirect » « Targeted Link»	« Link » « redirect » « target link »	« Link » « redirect » « target Link »	«dépendance»	« agrégation»
« serveur page »	« build » « redirect »	« redirect »	« build » « redirect »		
« frameset »	« frame content »		« frame content»	«Frame conte »	
« form »	« aggregated by »	« submit »			

II.6. Conclusion :

Dans cette annexe nous avons présenté l'outil UML que nous avons utilisé pour modéliser notre application.

Bibliographie

Bibliographie

Les ouvrages

[01] : **Bruno Péan**, Support de cours sur les réseaux, Ecole Internationale des Sciences du Traitement de l'Information-EISTI », Edition 2001.

[02] : **Paola ZANELLA, Yves Ligier,** Architecture et technologie des ordinateurs, 4ème Edition, Edition DUNOD.

[03] : Architecture des réseaux, 1ère partie IDEC 2010,

[04] : Les réseaux : Matériels et normes, BTS IG 2ème année AMSI,

[05] : **Daniele DRONAD, Dominique SERET**, Architecture des réseaux, Pearson, France 2010.

[06] : **Pascal Nicolas,** Cours de réseaux, Maitrise d'informatique, 1999/2000.

[07] : Les Fiches thématiques Jur@tic, Réseau informatique, Usages et choix techniques.

[08] : Les réseaux : Généralité, Septembre 2009.

[09] : **Razak MEZARI et Mourad LAHDIR**, Mise en œuvre des réseaux locaux.

[10]:**François LAISSUS,** Cours d'introduction à TCP/IP, Version 2002.

[11] : **Jean-Claude Silvène TAJAN**, GroupWare et internet, Edition DUNOD ,1999.

[12]: **Université Nice Sophie ANTIPLIS**, Les réseaux informatiques.

[13]: **Robert ORGALLE, Dan HAKEY Jerry EDWARDS**, Client/serveur guide de service, Traduction en français, **LEROY et Jean-Pierre GOUT**.

[14] : **Guillaume EVANGELISTA**, La sécurité des réseaux, Edition CompusPress, 2001.

[15] : **Ayoub FIGUIGUI**, Introduction à la sécurité informatique, Menaces, 17/07/2010.

[16] : **Jean-Francois CARPENTIER**, La sécurité informatique dans la petite entreprise, Edition ENI, Avril 2009.

[17] : **Saci MEDILEH** : Les virus informatiques, Décembre 2005.

[18] : **MEHARITM V3**, Principes et mécanismes, Edition Octobre 2004. www.clusif.asso.fr

[19] : CHAMPAGNE & ARDENNE, Les principes de la sécurité, Université de REIMS, 2000.

[21] : **G. A. Leirier et R. Stoll,** Grand livre PHP 4 & MYSQL, Edition Micro Application, 2000.

[22] : **Gilles Hunault,** Un petit tuteur MYSQL, Angers, janvier 2000.

[23] : Manuel d'aide fourni avec le logiciel EASY PHP 2.0.

[24] : Manuel d'aide fourni avec le logiciel Macromedia DREAMWEAVER 8.

[25] **: Jim Conallen**, Mdélisation des applications Web avec UML Edition Eyrolles, 2000.

Les sites

[WEB 01]: www.commentcamarche.net

Introduction à la sécurité informatique.

[WEB 02] : www.matael.info

La sécurité des systèmes informatiques (théorie).

[WEB 03] : www.ai-psinfo

Share/définition-virus.

[WEB 04] : www.bestcours.com

Réseau informatique/Politique de sécurité.

[WEB 05] : www.awt.be

Web/sécurité/sécurité et aspect juridiques des TIC

[WEB 06] : www.commentcamarche.net

UML-cas d'utilisation.

[WEB07]: www.webmasterhub.com.

[WEB08]:www.liafa.jussieu.fr/~carton/Enseignement/InterfacesGraphiques/MasterInfo/Cours

/Swing/mvc.html.

Architecture Modèle/Vue/Contrôleur.

[WEB09] : WWW.clusif.asso.fr