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

Faculté des Sciences Exactes et d'Informatique
Département de Mathématiques et d'Informatique
Filière Informatique

Deuxième Année Master informatique
Spécialité: **Systèmes d'Information Géographiques**

Rapport de Mini-Projet

Titre

Conception d'un entrepôt de données spatiales sécurisé

Présentées par :
Ouinas Nassima
Seydou Ousseina

Encadrés par:
Mr. Midoun Mohamed
Mr. Tbahriti Salah Eddine

Année Universitaire 2014/ 2015

Sommaire

Liste des figures et tableaux

Résumé

Intitulé du projet : Conception d'un entrepôt de données spatiales sécurisé.

Résumé

Face à la croissance des données géo référencées, les outils d'analyse spatiale traditionnels sont loin d'être suffisants pour répondre aux besoins de manipulation de gros volumes de données.

Les entrepôts de données spatiaux se positionnent comme une bonne solution pour le stockage des bases de données géographiques volumineuses. D'autre part, Le Spatial-OLAP ou SOLAP (Spatial online analytical processing) est un prolongement de l'OLAP qui tient compte des interactions dans l'espace. Il est considéré comme une direction importante dans le développement d'une nouvelle génération d'outils d'analyse spatiale.

A l'instar, des bases de données volumineuses traditionnelles, la sécurité des entrepôts de données spatiaux s'impose et notamment pour les requêtes multidimensionnel d'un OLAP Spatial.

L'objectif de ce projet s'articule autour de trois axes :

- L'étude bibliographique concernant les mécanismes de sécurité des données spatiales dans un entrepôt de données spatiales.
- La conception d'un mécanisme de sécurité à base d'un algorithme de cryptage et décryptage de données spatiales
- Le développement d'un prototype pour la création, l'alimentation et l'interrogation d'un entrepôt de données spatiale intégrant aussi l'algorithme développé.

Mots clés : Sécurité de données, entrepôts de données spatiaux, information spatiales

I. Introduction

De nos jours, les volumes de données à traiter sont de plus en plus importants. Apparus pour gérer de tels volumes de données issues de sources hétérogènes, les entrepôts de données constituent l'outil essentiel de collecte et de stockage des données en vue de leur analyse interactive, rapide et dynamique.

Ainsi plus de 80% de ces données ont une composante spatiale qui est souvent inexploitée donc il y'a un besoin de nouveaux outils d'analyse spatio-temporelle pour exploiter cette composante. Il est bien connu que les SIG seuls ne présentent pas l'efficacité requise pour les applications analytiques (langages d'interrogation, interfaces complexes, temps de traitement longs) L'intérêt d'OLAP pour l'analyse spatio-temporelle a été démontré .Cependant, sans volet cartographique, il est impossible de visualiser la composante géométrique des données. Une solution consiste à combiner des technologies spatiales et non-spatiales : SIG et OLAP d'où SOLAP.

II. Concepts fondamentaux des entrepôts de données

II.1. Définition d'un entrepôt de données (ou DataWarehouse)

Bill Inmon définit l'entrepôt de données, dans son livre considéré comme étant la référence dans le domaine "Building the DataWarehouse" **[1]** comme suit:

« L'entrepôt de données est une collection de données orientées sujet, intégrées, non volatiles et évolutives dans le temps, organisées pour le support d'un processus d'aide à la décision. »

Les paragraphes suivants illustrent les caractéristiques citées dans la définition d'Inmon.

Orienté sujet : L'entrepôt de données est organisé selon le thème c'est à dire autour des sujets majeurs de l'entreprise tels que clientèle, ventes, produits…. et non suivant les processus fonctionnels tels que cartes bancaires, clients… . Le sujet est transversal aux structures fonctionnelles et organisationnelles de l'entreprise. On peut accéder aux données utiles sur un sujet. L'intégration des différents sujets se fait dans une structure unique. Ainsi, Il n'y a pas de duplication des informations communes à plusieurs sujets.

Intégrée : L'entrepôt de données intègre des données qui proviennent de différentes sources. Il intègre les données afin de les homogénéiser et de leur donner un sens unique, compréhensible par tous les utilisateurs c'est à dire que les données intégrées doivent subir une mise en cohérence.

Evolutives dans le temps : La prise en compte de l'évolution des données est essentielle pour la prise de décision qui par exemple utilise des techniques de prédiction en s'appuyant sur les évolutions passées pour prévoir les évolutions futures**.** Dans un entrepôt de données chaque valeur est associée à un moment.

« Every key structure in the data warehouse contains - implicitly or explicitly -an element oftime » **[2].** Les données de l'entrepôt ne sont précises et valables qu'à un certain moment ou pendant un intervalle de temps donné.

Non volatiles : c'est ce qui est, en quelque sorte la conséquence de l'historisation décrite précédemment. Une donnée dans un environnement opérationnel peut être mise à jour ou supprimée, de telles opérations n'existent pas dans un environnement d'entrepôt de données. Les données de l'entrepôt sont essentiellement utilisées en mode de consultation. Elles ne sont pas modifiées par les utilisateurs.

Organisées pour le support d'un processus d'aide à la décision : Les données de l'entrepôt sont organisées de manière à permettre l'exécution des processus d'aide à la décision. Elles permettent non seulement d'appréhender rapidement une situation mais aussi de connaître les facteurs explicatifs.

II.2. Objectifs des entrepôts de données

Un entrepôt de données :

- permet le développement d'applications décisionnelles et de pilotage de l'entreprise et de ses processus.
- joue un rôle de référentiel pour l'entreprise puisqu' 'il permet de fédérer des données souvent éparpillées dans différentes bases de données.
- offre une vision globale et orientée sur métiers de toutes les données que manipule l'entreprise.
- permet de faire face aux changements du marché et de l'entreprise.
- offre une information compréhensible, utile et rapide

II.3. Les éléments d'un système décisionnel

L'environnement de l'entrepôt de données est constitué essentiellement de quatre composantes : les applications opérationnelles, la zone de préparation des données, la présentation des données et les outils d'accès aux données.

- **Les applications opérationnelles :** ce sont les applications du système opérationnel de l'entreprise et dont la priorité est d'assurer le fonctionnement de ce dernier et sa performance. Ces applications sont extérieures à l'entrepôt de données.

- **Préparation des données :** la préparation englobe tout ce qu'il y a entre les applications opérationnelles et la présentation des données. Elle est constituée d'un ensemble de processus appelé ETL, « Extract, transform and Load », les données sont extraites et stockées pour subir les transformations nécessaires avant leur chargement. « Un point très important, dans l'aménagement d'un entrepôt de données, est d'interdire aux utilisateurs l'accès à la zone de préparation des données, qui ne fournit aucun service de requête ou de présentation » **[3]**.

- **Zone de stockage :** c'est l'entrepôt où les données sont organisées et stockées. Si les données de la zone de préparation sont interdites aux utilisateurs, la zone de présentation est tout ce que l'utilisateur voit et touche par le biais des outils d'accès.

L'entrepôt de données est constitué d'un ensemble de Data Mart. Ce dernier est défini comme étant une miniaturisation d'un entrepôt de données, construit autour d'un sujet précis d'analyse ou consacré à un niveau départemental **[4].** Le Data-Mart est donc un mini entrepôt de données lié à un métier particulier de l'entreprise (finance, commercial, …).

- **Zone de présentation :** La zone de présentation donne accès aux données contenues dans l'entrepôt de données. Elle peut contenir des outils d'analyse programmés (rapports, requêtes, …).

Après avoir défini chacun des éléments constituant l'environnement d'un entrepôt de données**,** il serait intéressant de connaitre le positionnement de ces éléments dans une architecture globale d'un système décisionnel**.**

II.4. Architecture d'un système décisionnel

La figure **I.1** illustre l'architecture globale d'un système décisionnel **[Web.1].**

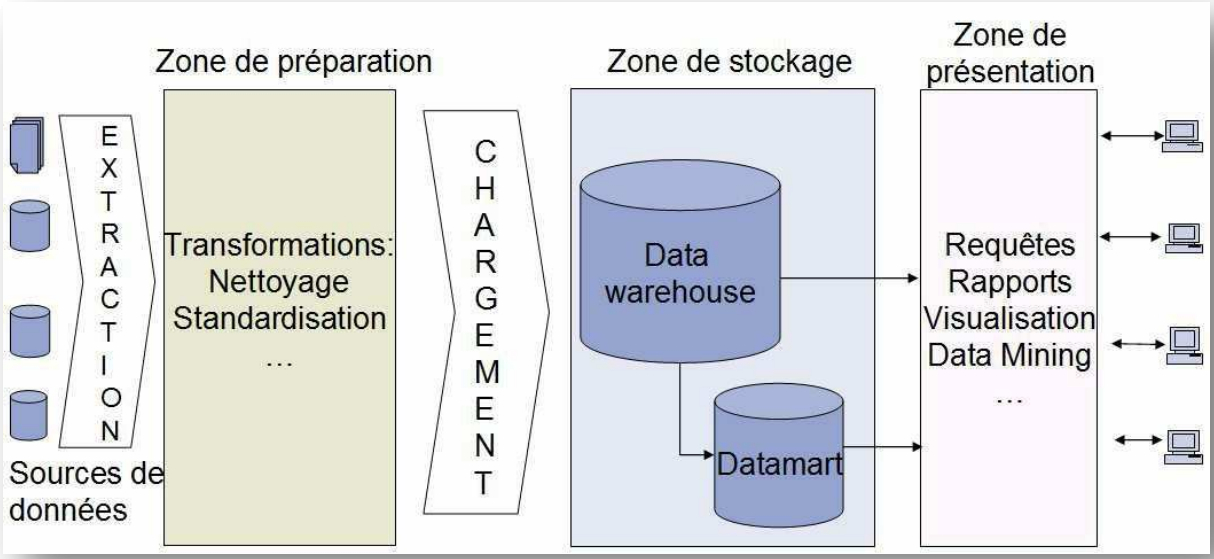


Figure I.1 : Architecture générale d'un système décisionnel.

II.5. Modélisation de l'entrepôt de données

II.5.1. La modélisation dimensionnelle et ses concepts

Les entrepôts de données ont introduit une nouvelle méthode de conception autour des concepts métiers c'est à dire qu'ils sont destinés à la mise en place de systèmes décisionnels. On ne parle plus de normalisation au sens relationnel du terme. Elle consiste à considérer un sujet d'analyse comme un cube à plusieurs dimensions, offrant des vues en tranches ou des analyses selon différents axes. Les données sont organisées de manière à mettre en évidence le sujet analysé et les différentes perspectives de l'analyse.
Cette modélisation a donné naissance aux concepts de fait et de dimension **[5].**

- **Concept de fait**

La table de fait modélise le sujet de l'analyse. Une table de faits est la table centrale d'un modèle dimensionnel, où les mesures de performances sont stockées. Une ligne d'une table de faits correspond à une mesure. Ces mesures sont numériques et généralement valorisées de manière continue.

Les mesures sont numériques pour permettre de résumer un grand nombre d'enregistrements en quelques opérations (on peut les additionner, les dénombrer ou bien calculer le minimum, le maximum ou la moyenne).

Les mesures sont valorisées de façon continue car il est important de ne pas valoriser le fait avec des valeurs nulles. Elles sont aussi souvent additives ou semi-additives afin de pouvoir les combiner au moyen d'opérateurs arithmétiques.

La figure **I.2** illustre l'exemple d'une table de fait.

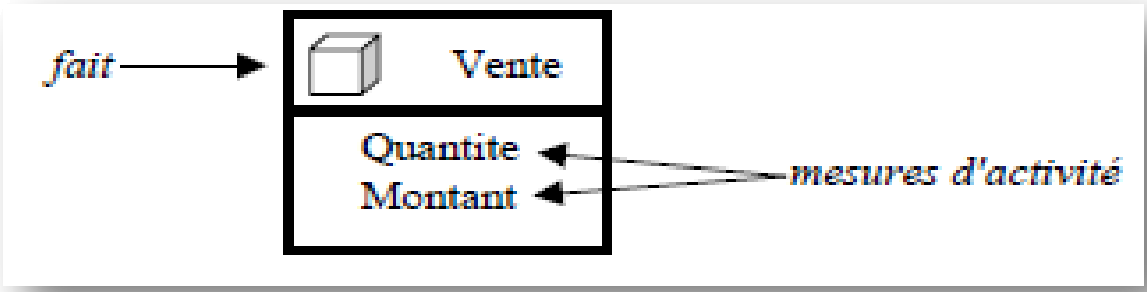


Figure I.2 : Exemple de table de fait

- **Concept de Dimension**

Le sujet analysé, c'est à dire le fait, est analysé suivant différentes perspectives. Ces perspectives correspondent à une catégorie utilisée pour caractériser les mesures d'activité analysées **[6]** ; on parle de dimensions.

Une table de dimension modélise une perspective de l'analyse. Elle se compose de paramètres correspondant aux informations faisant varier les mesures de l'activité.

Les dimensions servent à enregistrer les valeurs pour lesquelles sont analysées les mesures de l'activité. Les tables de dimension sont les tables qui raccompagnent une table de faits, elles contiennent les descriptions textuelles de l'activité.

La figure **I.3** illustre l'exemple de tables de dimensions.

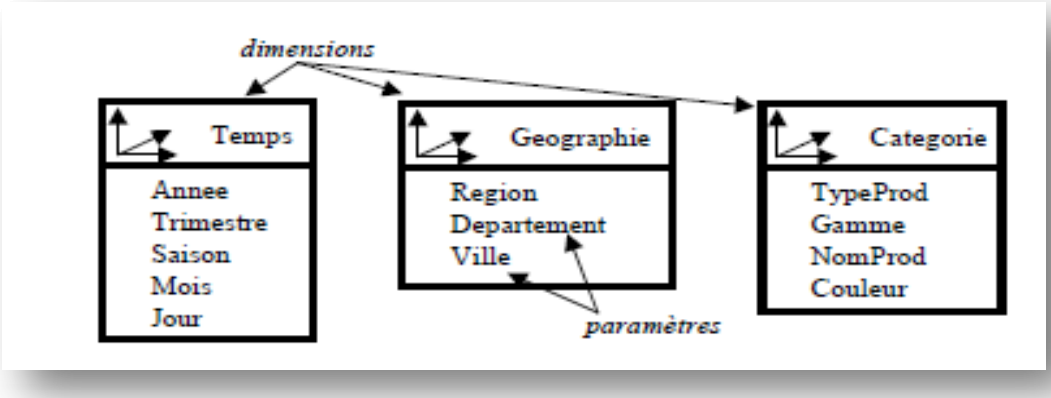


Figure I.3 : Exemple de tables de dimensions

II.5.2. Différents modèles de la modélisation dimensionnelle

Le modèle en étoile et le modèle en flocon sont les deux modèles les plus utilisés pour modéliser un entrepôt de données.

- **Modèle en étoile**

Cette structure est constituée du fait central et des dimensions. Ce modèle représente visuellement une étoile, on parle de modèle en étoile **[5].**
La figure **I.4** illustre la modélisation en étoile.

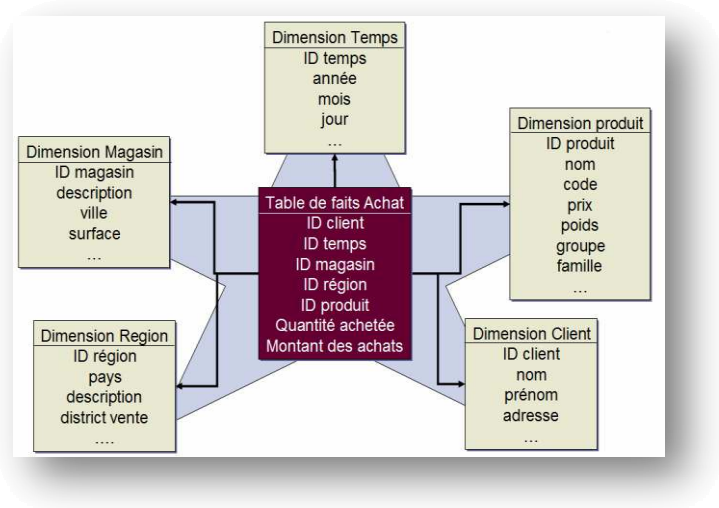


Figure I.4 : Modélisation en étoile

- **Modèle en flocon**

Une modélisation en flocon consiste à décomposer les dimensions du modèle en étoile en sous hiérarchies **[5]**. La modélisation en flocon est donc une émanation de la modélisation en étoile ; le fait est conservé et les dimensions sont éclatées conformément à sa hiérarchie des paramètres.
La figure **I.5** illustre la modélisation en flocon dérivant du modèle en étoile de la figure **I.4 [5].**

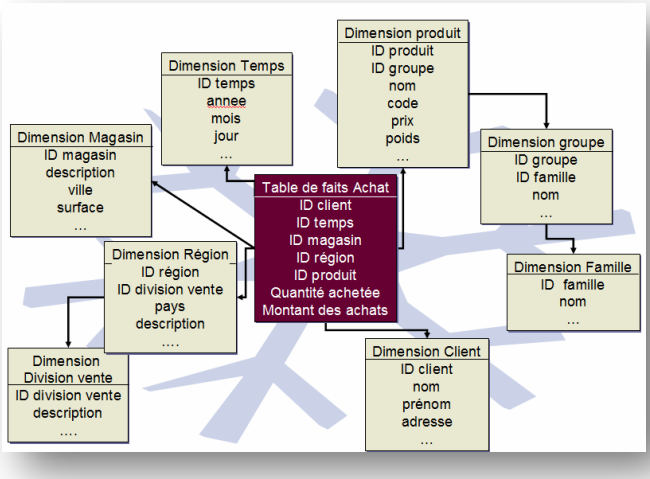


Figure I.5 : Modélisation en flocon

II.5.3. Comparaison entre le modèle en étoile et le modèle en flocon

Le tableau **I.1** montre la différence entre le modèle en étoile et le modèle en flocon en donnant quelques avantages et inconvénients **[6]**.

	Avantages	Inconvénients
Modèle en étoile	– Facilité de navigation – Nombre restreint de jointures.	– Redondance des dimensions – toutes les dimensions ne concernent pas les mesures
Modèle en flocon	– Normalisation des dimensions – Economie d'espace disque	– plus complexe – plusieurs jointures dans le traitement des requêtes.

Tableau I.2 : Comparaison entre Modèle en étoile et le modèle en flocon

III. OLAP

Le but de l'OLAP (*On-Line AnalyticalProcessing*) est de permettre une analyse multidimensionnelle sur des bases de données volumineuses afin de mettre en évidence une analyse particulière des données (il est l'objet d'un questionnement particulier).

III.1. Définition de l'OLAP

R. Kimball définit le concept « OLAP » comme «Activité globale de requêtage et de présentation de données textuelles et numériques contenues dans l'entrepôt de données ; Style d'interrogation spécifiquement dimensionnel » **[7].** Elle permet une analyse et une visualisation des données plus fine, pouvant utiliser plusieurs niveaux de granularité.

Grâce à l'OLAP, les utilisateurs peuvent créer des représentations multidimensionnelles (appelées « *hypercube »s* ou « *cubes OLAP* ») selon les critères qu'ils définissent afin de simuler des situations.

III.2. Architecture OLAP

Une architecture OLAP générale comprend trois composantes :

- **Base de données :**

– Doit supporter les données agrégées ou résumées

– Peut provenir d'un entrepôt ou d'un marché de données

– Doit posséder une structure multidimensionnelle (SGDB multidimensionnel ou relationnel)

- **Serveur OLAP :**

– Gère la structure multidimensionnelle dans le SGBD

– Gère l'accès aux données de la part des usagers

- **Module client :**

– Permet aux usagers de manipuler et d'explorer les données

– Affiche les données sous forme de graphiques statistiques et de tableaux

La figure **I.6** montre les composants de l'architecture OLAP.

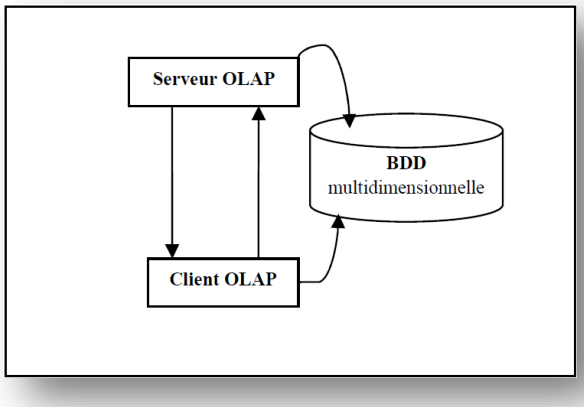


Figure I.6 : Composants de l'architecture OLAP

Les trois composantes peuvent se combiner en plusieurs configurations, selon le type de la base de données accédée : relationnelle, multidimensionnelle, ou hybride. Ce qui va donner les différents types de l'OLAP.

III.3.Types d'OLAP

III.3.1.MOLAP

Ces systèmes MOLAP « Multidimentional On-line Analytical Processing » sont conçus exceptionnellement pour l'analyse multidimensionnelle.

R. Kimball définit ces systèmes comme étant un « Ensemble d'interfaces utilisateur, d'applications et de technologies de bases de données propriétaire dont l'aspect dimensionnel est prépondérant » **[7].** MOLAP offre des temps d'accès optimisés et cela en prédéfinissant les opérations de manipulation et de chemin d'accès prédéfinis.

Autre caractéristique du MOLAP c'est qu'il agrège tout par défaut, pénalisant du coup le système lorsque la quantité de données à traiter augmente.

III.3.2. ROLAP (OLAP Relationnel)

« Ensemble d'interfaces utilisateurs et d'applications qui donnent une vision dimensionnelle à des bases de données relationnelles » **[7].**Les systèmes ROLAP « **R**elationnel **O**n-line **A**nalytical **P**rocessing » sont en mesure de simuler le comportement d'une SGBD multidimensionnel en exploitant un SGBD relationnel. L'utilisateur aura ainsi l'impression d'interroger un cube multidimensionnel alors qu'en réalité il ne fait qu'adresser des requêtes sur une base de données relationnelles.

III.3.3. HOLAP (OLAP Hybride)

HOLAP « **H**ybride **O**n-line **A**nalytical **P**rocessing » consiste a un croisement des systèmes MOLAP et ROLAP. Cette combinaison donne à ce type de système les avantages du ROLAP et du MOLAP en utilisant tour à tour l'un ou l'autre selon le type de données.

III.4. Les opérateurs OLAP

Les outils OLAP utilisent des opérateurs particuliers afin de « naviguer » dans les cubes multidimensionnels **[Web.2]**. Les opérateurs OLAP permettent d'explorer les données multidimensionnelles en utilisant les différents concepts de dimensions et hiérarchies.

Le cube de données est exploré à l'aide de nombreuses opérations qui permettent sa manipulation. Les opérateurs OLAP proposés dans la littérature les plus communs sont :

- **Les opérateurs de forage**
  - **Forer (drill-down) :** Permet de descendre dans la hiérarchie de la dimension. Par exemple, visualiser le nombre d'accidents par mois au lieu de par année.
  - **Remonter (drill-up, roll-up) :** Permet de remonter dans la hiérarchie de la dimension. Par exemple, visualiser le nombre d'accidents par année au lieu de par mois.
- **Les opérateurs de coupe**
- **Slice :** utilise un prédicat défini sur les membres des dimensions pour couper une partie de l'hyper cube limitant le champ d'analyse et permettant à l'utilisateur de se concentrer sur des aspects particuliers du phénomène. En utilisant la terminologie de l'algèbre relationnelle, l'opération de slice est l'équivalent de la sélection.
- **Dice :** réduit la dimensionnalité de l'hyper cube en éliminant une dimension. Cette opération est équivalente à la projection de l'algèbre relationnelle.

- **Pivoter (pivot, swap) :** Permet d'inter changer deux dimensions. Par exemple, visualiser le nombre d'accident par mois ensuite par région.

➢ **Les opérateurs inter-cubent**

- **Forer latéralement (drill-across)** : Permet de passer d'une mesure à l'autre. Par exemple, visualiser le coût des travaux au lieu du nombre d'accidents.

III.5. Les requêtes multidimensionnelles

Le MDX (de l'anglais Multidimensional Expressions, « expressions multidimensionnelles ») est un langage de requête pour les bases de données OLAP, analogue au rôle de SQL pour les bases de données relationnelles. C'est aussi un langage de calcul avec une syntaxe similaire à celle des tableurs. MDX est fait pour naviguer dans les bases multidimensionnelles et pour définir des requêtes sur tous les objets (dimensions, hiérarchies, niveaux, membres et cellules) afin d'obtenir (simplement) une représentation sous forme de tableaux croisés **[Web.3].**

III.5.1. Les types de données MDX

Il existe six types de données primaires dans MDX :

- **Scalaire :** Scalaire est un nombre ou une chaîne. Il peut être spécifié comme un littéral, par exemple Numéro 5 ou chaîne "OLAP" ou il peut être retourné par une fonction MDX Etc.
- **Dimension / Hiérarchie :** La dimension est une dimension d'un cube. Une dimension est un organisateur de mesure principale et d'information d'attribut dans un cube. MDX ne connaît pas, ni ne assume aucune, des dépendances entre les dimensions qui sont supposés être indépendants les uns des autres. Une dimension contiendra certains membres organisés dans certains niveaux de la hiérarchie.
  Il peut être spécifié par son nom unique, par exemple comme il peut être renvoyé par une fonction MDX. La hiérarchie est une hiérarchie de dimension d'un cube. Il peut être spécifié par son nom unique, par exemple ou il peut être renvoyé par une fonction MDX. Les hiérarchies sont contenues dans les dimensions.

- **Niveau :** Le niveau est un niveau dans une hiérarchie de dimension. Il peut être spécifié par son nom unique, par exemple ou il peut être renvoyé par une fonction MDX.

- **Membres :** Membres est un membre dans une hiérarchie de dimension. Il peut être spécifié par son nom unique. Par nom qualifié, par exemple ou retourné par une fonction MDX Etc. Notons que tous les membres sont spécifiques à une hiérarchie. Si l'auto même produit est membre de deux hiérarchies différentes, il y aura deux membres différents visibles qui peuvent être coordonnés dans les ensembles et tuples.

- **Tuple :** Tuple est une collection ordonnée d'un ou plusieurs membres de différentes dimensions. Tuples peuvent être spécifiées en énumérant les membres, ou retourné par une fonction MDX.

- **Set :** Set est une collection ordonnée de tuples avec la même dimension, ou hiérarchisé dans le cas de la mise en œuvre de Microsoft. Il peut être spécifié énumérant les tuples, par exemple ou renvoyé par fonction ou un opérateur MDX Etc.

III.5.2. Structure générale d'une requête MDX

Un prototype de requête MDX est donné par la syntaxe suivante :
SELECT [<axis_specification>
[, <spécification_des_axes>...]]
FROM [<spécification_d_un_cube>]
[**WHERE** [<spécification_de_filtres>]]

IV. SOLAP

IV.1. Concepts principaux de l'OLAP Spatial

IV.1.1. Définition de l'OLAP Spatial

L'OLAP Spatial (SOLAP) a été défini par Yvan Bédard comme « une plateforme visuelle conçue spécialement pour supporter une analyse spatio-temporelle rapide et efficace à travers une approche multidimensionnelle qui comprend des niveaux d'agrégation cartographiques, graphiques et tabulaires » **[8].**

IV.1.2. Les avantages de l'OLAP Spatial

La visualisation des mesures sur une carte permet de comprendre la distribution géographique d'un phénomène qui, souvent, peut être différente de l'espace géographique identifié par la structure hiérarchique définie par la dimension géographique.
De plus, l'affichage cartographique révèle des informations spatiales (relations spatiales et informations métriques) qu'une simple étiquette textuelle ou un affichage graphique n'aurait jamais montrées.
La composante cartographique dans l'OLAP représente un instrument de visualisation et surtout d'analyse, qui permet à l'utilisateur de voir et comprendre les données spatio-multidimensionnelles, et elle constitue une interface vers l'entrepôt de données spatiale **[9]**.

IV.1.3. Entrepôt de données spatiales

Un entrepôt de données spatiales est une collection de données spatiales et thématiques, intégrées, non volatiles et historiées pour la prise de décisions spatiales **[10]**. Un entrepôt de données spatiales est comme un entrepôt conventionnel mais sauf que les données sont de nature spatiale. Il contient en même temps des données spatiales et alphanumériques et il reformule les concepts classiques de dimension et de mesure pour prendre en compte la composante spatiale de l'information géographique en définissant les dimensions et les mesures spatiales.

IV.1.4. L'information géographique

L'information géographique se caractérise par une composante de localisation spatiale. Cette localisation s'inscrit sur la surface terrestre.

En outre, on capture la morphologie des objets qui se traduit, entre autres, par la dimension de l'objet représenté, à savoir des points, des lignes ou des surfaces **[Web.4].**

IV.1.5. Base de données spatiale

Une base de données géographique est définie par un ensemble d'objets géographiques organisé de manière à pouvoir être manipulé dans un SIG. C'est une base de données qui regroupe des données spatiales dont la position de chaque objet est conforme à la précision géométrique, y compris des points, les lignes et des polygones **[Web.5].**

La figure **I.7** résume la structure d'une base de données spatiale.

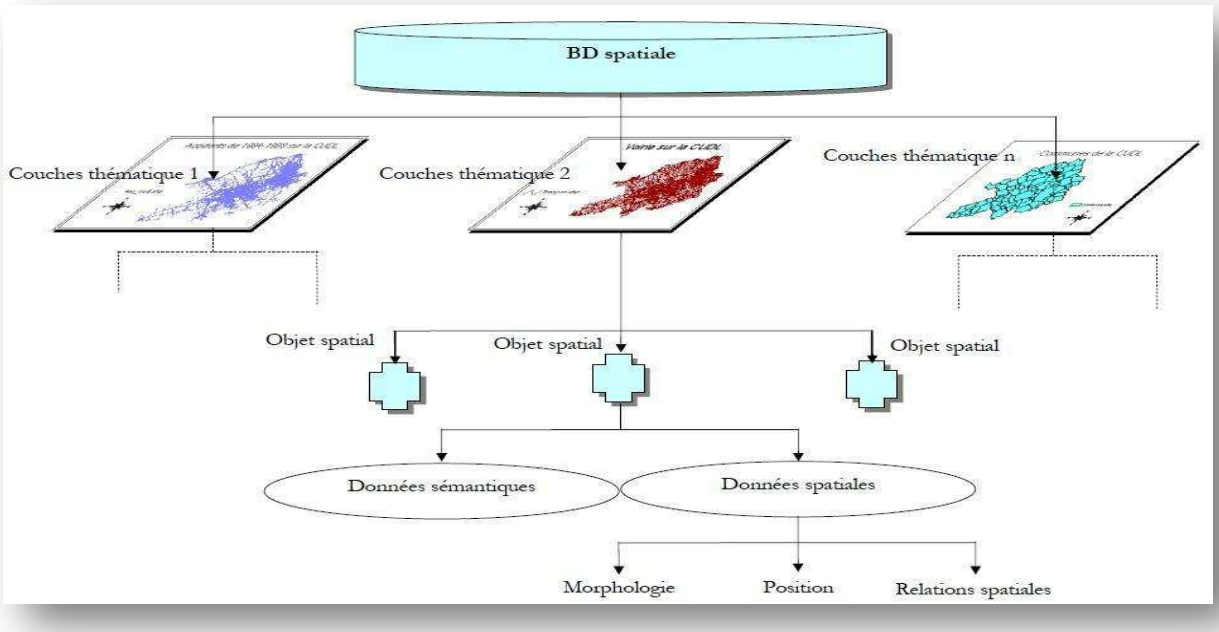


Figure I.7 : Structure d'une base de données spatiale

IV.1.6. L'objet spatial

Un objet spatial est une entité du monde réel (par exemple, une ville, un pays, une route, un lac, un arbre,…) représenté dans une base de données spatiales par une structure. Cette structure contient à la fois des données sémantiques et des données spatiales **[Web.6].**

Les données sémantiques, appelées aussi les données non-spatiales ou alphanumériques, décrivent qualitativement ou quantitativement les propriétés de l'objet (Ex : le nom d'une commune, la hauteur d'un bâtiment, …)**.** Les données spatiales décrivent la géométrie de l'objet spatial, sa localisation dans l'espace et les relations spatiales qui le relient aux autres objets. Le terme géométrie désigne la forme ou la morphologie d'un objet (par exemple : point, ligne, polygone, cercle, …). La localisation est la position géographique de l'objet. Elle est repérée, selon un système de projection donné, par la latitude, la longitude et éventuellement l'altitude de l'objet. Les relations spatiales désignent les liens de voisinage entre les objets.

IV.1.7. Relations spatiales

Les relations spatiales jouent un rôle important en géographie car elles mettent en évidence l'influence du voisinage qui est la principale spécificité des données géographiques. Ces relations peuvent être métriques (basées sur la distance), topologiques (par exemple : intersection, au bord de, inclusion, union, etc.) ou directionnelles (par exemple : nord, ouest). Les relations spatiales sont des informations qui traduisent des propriétés essentielles dans le monde géographique.

Tout géographe s'accorde à dire que tout phénomène en un endroit est lié à l'influence du voisinage et cette influence décroît avec l'éloignement (1ère loi en géographie **[11]).** De nombreuses études ont été faites pour classifier les relations spatiales pouvant exister. Le tableau **I.2** illustre les prédicats spatiaux les plus courants **[12].**

Prédicats binaires	Région	Ligne
Région	Adjacent, inclusion chevauchement	Borde chevauchement
Ligne	Gauche, droite, inclusion chevauchement	Connecte, inclusion chevauchement
Point	Inclusion	Extrémité, inclusion

Tableau I.1: Exemple de relations spatiales.

IV.2. Les outils OLAP spatial

Un outil SOLAP repose sur l'intégration des fonctionnalités SIG et OLAP **[13] et [14]**. La composante cartographique est utilisée pour visualiser les membres de dimensions et/ou les mesures avec une composante spatiale, pour représenter les mesures alphanumériques, grâce à des cartes thématiques, et pour accéder aux opérations de navigation multidimensionnelle. Différents systèmes SOLAP, pouvant être classifiés en trois différentes typologies, ont été développés.

IV.2.1. Typologies

En **[15]** et **[9]** les solutions SOLAP sont regroupées en trois grandes classes: Olap dominant, SIG dominant et OLAP-SIG intégrée.

- **SIG dominant**

Dans les solutions SIG dominantes comme **[16]**, le serveur OLAP est simulé grâce à une base de données relationnelle modélisée sous forme d'étoile.

Les solutions SIG dominantes, comme décrit par **[12],** offrent toutes les fonctionnalités d'un outil SIG : stockage, analyse et visualisation des données spatiales.

Par contre, elles doivent inclure, dans la base de données, des éléments permettant d'implémenter les opérations OLAP de forage et de coupe, puisqu'il n'existe pas de serveur OLAP pour gérer ces opérations. De plus, toutes les fonctionnalités avancées OLAP comme l'utilisation de mesures dérivées, ne sont pas présentes dans ce type d'outil, ce qui limite ses capacités d'analyse multidimensionnelles.

- **OLAP dominants**

Les outils OLAP dominants comme **[17]** utilisent un système OLAP et offrent toutes les fonctionnalités classiques pour l'analyse multidimensionnelle.
Par contre, les fonctionnalités SIG sont limitées à une simple représentation cartographique des mesures et des dimensions spatiales, à la navigation cartographique (c'est à dire déplacement et changement de couche) et à la sélection d'objets géographiques **[9]**.
Ces solutions ne présentent aucun instrument pour l'analyse spatiale ou d'autres fonctionnalités avancées SIG.
Ceux-ci, comme montré par plusieurs travaux **[16], [9]** sont nécessaires et complémentaires à l'analyse spatio-multidimensionnelle.
De plus, dans ces solutions les opérateurs de forage sur la dimension spatiale sont inexistants ou limités. Il n'est pas possible par exemple, d'obtenir une carte avec des membres spatiaux de différents niveaux, grâce à une simple opération de forage sur un seul membre spatial **[9]**.

- **OLAP-SIG intégrée**

Les solutions OLAP-SIG intégrées comme JMap fusionnent toutes les fonctionnalités des deux différents systèmes dans un seul environnent. Comme montré dans [**16]** les environnements SIG d'analyse et de visualisation sont nécessaires pour l'analyse spatio-multidimensionnelle et elles complètent les fonctionnalités purement OLAP. Les solutions OLAP-SIG intégrées sont alors les plus adaptées pour une analyse spatio-multidimensionnelle réelle et efficace. Cette intégration peut être vue comme une reformulation des trois niveaux d'une architecture OLAP classique, en utilisant et/ou en ajoutant des fonctionnalités SIG.
Le premier niveau est un entrepôt de données spatiales, qui doit permettre de modéliser les complexes structures de données associées aux dimensions et aux mesures spatiales. Le deuxième niveau est un serveur OLAP capable de gérer des requêtes spatio-multidimensionnelles.

IV.3. Modèle des données multidimensionnelles

La composante sémantique de l'information géographique influe sur la modélisation des dimensions et des mesures spatiales.

IV.3.1. Dimension spatiale

Dans **[18],** les auteurs introduisent le concept de dimension spatiale comme un ensemble de hiérarchies spatiales.
La dimension spatiale désigne l'introduction de l'information spatiale dans une application décisionnelle en tant qu'axe d'analyse. Une hiérarchie est spatiale s'il y a au moins un niveau qui contient la composante spatiale. De plus, entre les membres de deux niveaux spatiaux doit exister une relation topologique d'inclusion ou d'intersection.

Une hiérarchie spatiale peut être totalement spatiale si tous les niveaux sont spatiaux, partiellement spatiale s'il y a au moins un niveau non spatial.
La figure **I.8** illustre le schéma de la hiérarchie.

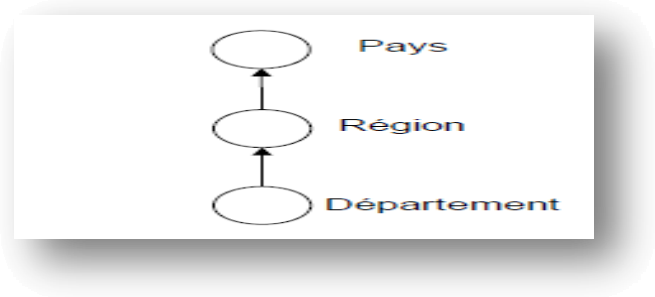


Figure I.8 : Dimension spatiale géométrique

IV.3.2. Mesure spatiale

(Rivest et al)**[19],** (Malinowsky et Zimányi) **[20]et** (Sampio et al)**[21]**définissent une mesure spatiale comme un objet géométrique qui est un attribut spatial du fait, et qui, contrairement aux modèles de (Fidalgo et al)**[22],** Stéfanovic et al **[10]** et (Marchand et al)**[23]**, peut ne pas être répliqué dans une dimension spatiale.
La composante spatiale et la composante descriptive des objets géographiques, sont identifiées par l'ensemble des attributs alphanumériques, elles doivent pouvoir être utilisées comme mesures. La composante descriptive peut être utile au processus décisionnel, pour expliquer un phénomène ou caractériser un ensemble des faits.

V. Conclusion

Le concept entrepôt de données est apparu comme une réponse à des besoins grandissants dans le domaine décisionnel. Sa capacité de fournir les données nécessaires à une bonne analyse, ont fait de lui un atout majeur et incontournable pour toute entreprise soucieuse du suivi de ses performances.

L'introduction de l'information spatiale dans l'analyse multidimensionnelle implique une reformulation des concepts des entrepôts de données spatiales et de l'OLAP spatial.

Dans la section suivante nous parlerons des étapes à suivre pour la sécurité des données spatiales. Ainsi, nous essayerons d'appliquer cette démarche pour pouvoir sécuriser notre entrepôt de données spatiales plus précisément les requêtes.

I. Introduction

L'évolution de l'utilisation d'internet, oblige beaucoup d'organisations à mettre en place un système d'information très développé et fiable. Ces systèmes d'information contiennent des données très importantes pour le déroulement des activités organisationnelles. Mais, ces données sont quotidiennement exposées à des risques suite à de mauvaises manipulation ; un vol, ou attaque de virus. Ceci peut nous conduire alors à perdre ces données. Il est donc nécessaire de les protéger contre les intrusions et les accès non autorisés. C'est pourquoi il est essentiel de mettre en place des moyens préventifs pour sécuriser nos données. Ainsi, la sécurité des données devient alors un facteur indispensable pour le bon fonctionnement des organisations.

II. Définition de la sécurité des données

La sécurité des données est l'ensemble des mesures adoptées pour empêcher l'utilisation (ajout, suppression, modification…), non autorisée d'un ensemble de données **[24]**. Elles désignent donc les mesures préventives que nous mettons en place pour préserver nos données. Elles visent à protéger les données contre tout accès et utilisation non autorisé. Elle est composée entre autre de trois notions élémentaires : la confidentialité, l'intégrité, et l'authentification.

II.1. Notion de base de la sécurité de données

II.1.1. Confidentialité

La confidentialité de données a été définie par l'Organisation internationale de normalisation (ISO) comme « le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé **[Web.7].**

Elle permet d'empêcher la divulgation non autorisée des données. Cela consiste à protéger les données sensibles contre les accès des utilisateurs non autorisés.

II.1.2. L'intégrité

L'intégrité de données est l'action qui permet de garantir la non modification des données c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Elle permet d'empêcher toute modification (suppression, ajout, mise à jour) non autorisée des données. Elle garantit que cet objet n'a pas été modifié par une autre personne que son auteur **[Web.8].**

II.1.3. L'authentification

L'authentification de données permet d'empêcher l'utilisation non autorisée des données. Lorsque qu'une donnée est échangée, l'authentification garantit son origine et sa destination. L'authentification de données consiste à assurer que seules les personnes autorisées aient accès a ces données **[Web.9].**

Ces notions sont appliquées à travers un ensemble d'outils qui s'appliquent dans le cadre d'une politique de sécurité.

III. Politique de sécurité

Les ITSEC (**Information Technology Security Evaluation Criteria**) définissent la politique de sécurité comme l'ensemble des lois, règles ou pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système d'information(données, utilisateurs ,machines, etc.)**[25]**. Elles spécifient les autorisations, interdictions et obligations des sujets qui peuvent accéder aux données du système.

A partir de cette définition nous dégageons trois concepts fondamentaux d'une politique de sécurité qui sont :

- **Sujet**: entité active qui accède aux données du système. Le sujet peut être un utilisateur, une application, une adresse IP …
- **Objet**: entité passive qui représente les données à protéger. L'objet peut être, par exemple, un fichier, une table relationnelle, une classe …
- **Action** : permet aux sujets de manipuler les objets. L'action peut être lire, écrire, exécuter …
- Les sujets ont des **permissions** de réaliser des actions sur des objets.

La figure **II.1** illustre le principe de la politique de sécurité.

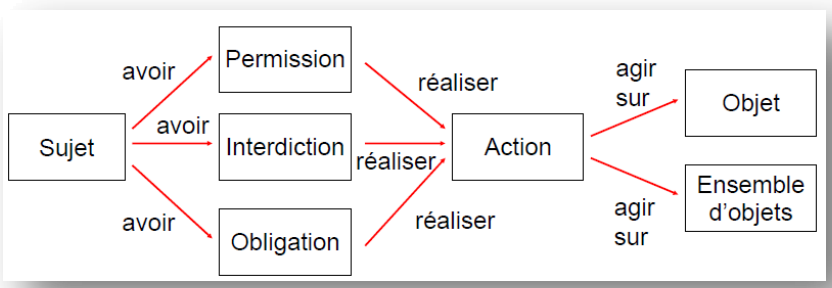


Figure II.1:Principe de la politique de sécurité.

Cette politique de sécurité peut être représentée de façon claire et simple par des modèles de contrôle d'accès.

III.1. Modèles de contrôle d'accès

C'est le modèle qui met en œuvre la politique de sécurité. Il décrit une représentation formelle des politiques de sécurité et de leur fonctionnement afin d'assurer la protection des données contre tout accès (lecture, écriture, modification, divulgation,.....) non autorisé et en gérant le contrôle d'accès aux données par des modèles de contrôle d'accès qui ont été définie dans la littérature dont le but est de garantir la confidentialité des données **[26].**

Dans la littérature il existe plusieurs modèles de contrôle d'accès dont les plus connus sont le DAC, MAC et le RBAC.

III.1.1. Contrôle d'accès discrétionnaire (Discretionary Access Control : DAC)

Ce modèle a été défini par TCSEC (Trusted Computer System Evaluation Criteria) comme" Un moyen de restriction d'accès aux objets basé sur l'identité des sujets et/ou du groupe auquel ils appartiennent. Les contrôles sont discrétionnaires dans le sens où le sujet est capable de transférer les permissions d'accès à d'autres sujets" **[27].**L'administration des droits dans le modèle DAC repose sur la notion de propriétaire : chaque objet a un propriétaire qui décide quels sont les autres sujets qui peuvent avoir accès à cet objet, étant donné que l'attribution des droits est faite par les utilisateurs et non pas par les administrateurs.
Voici les principes d'accès qui s'appliquent au modèle "discrétionnaire" :

- ✓ Un sujet dispose du plein contrôle des objets dont il est propriétaire.
- ✓ Le propriétaire est souvent le créateur des objets.
- ✓ Le propriétaire détermine les permissions et droits d'accès aux ressources sous son contrôle.

Dans ce modèle l'état du système est représenté par le triplet (S, O, M), d'où S signifie l'ensemble des sujets, O l'ensemble des objets, et M[S, O] la matrice de contrôle d'accès, d'où les lignes représentent les sujets et les colonnes représentent les objets. Les actions de (s) sur (o) (lecture, écriture,....) sont modélisées par une entrée M[S, O] **[28].**

- **Modèle de Lampson**

Ce modèle a été créé par Lampson en 1971**[29].** Il a pour but le contrôle d'accès aux données, en représentant les autorisations par la matrice de contrôle d'accès. On peut représenter ce modèle par le triplet (S, O, M) ou S signifie les sujets, O les objets, M la matrice de contrôle d'accès qui affecte à chaque couple (S, O) un ensemble de droits d'accès.
Le tableau **II.1** illustre la matrice de contrôle d'accès.

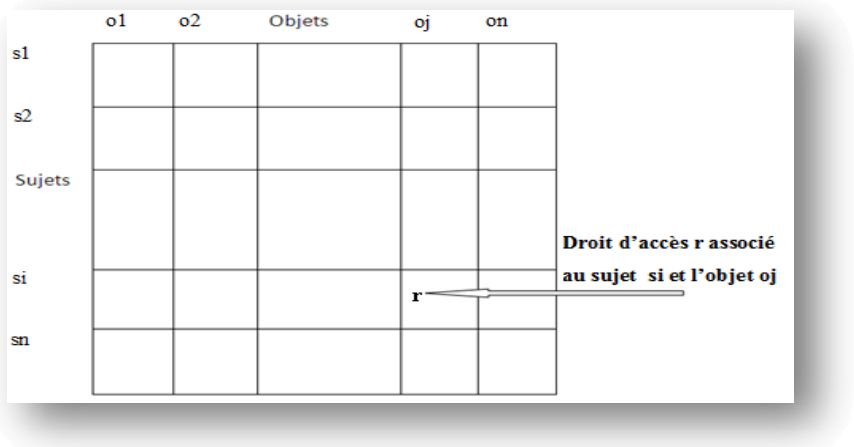


Tableau II.1:Matrice de contrôle d'accès

La matrice modélisée par le tableau **II.1** montre l'affectation des droits d'accès **r** à l'objet **oj** par le sujet **si**. Les interdictions des droits d'accès sont exprimées indirectement par la matrice de contrôle d'accès.

III.1.2. Contrôle d'accès obligatoire (Mandatory Access Control : MAC)

Ce modèle a été défini dont le but d'assurer le contrôle d'accès aux données, en définissant des règles rigides et incontournables afin de remédier à tout accès aux données non autorisé (lecture, modification, divulgation, destruction).

Le MAC se base sur des politiques multi-niveaux qui classent les sujets et les objets selon une autorité centrale. Il ne permet pas à ces utilisateurs d'intervenir dans l'attribution des droits d'accès aux données **[30].**

- **Modèle multi-niveaux**

Ce modèle permet à un système de catégoriser ses entités (sujet, objet) selon un niveau d'habilitation et un niveau de classification. Habilitation c'est le niveau de sécurité d'un sujet et classification c'est le niveau de sécurité d'un objet. En introduisant la notion de classe d'accès **[31].** Pour chaque sujet et objet on affecte une classe d'accès. Une relation d'ordre partiel est définie sur l'ensemble des classes d'accès. C'est la relation de dominance symbolisée par ($\geq$). Une classe d'accès est formée de deux composants, Un niveau de sécurité et un ensemble de catégories. Le niveau de sécurité est un élément d'un ensemble totalement ordonné, par exemple top secret (TS), secret (S), confidentiel (C) et non classifié (N). L'ensemble des catégories décrit les divers domaines des systèmes en étude.

On a deux classes d'accès ac1 et ac2, la relation de dominance ($\geq$) peut être définit comme suite :

ac1 domine ac2 ou ac1 $\geq$ ac2 si :

- le niveau de sécurité de ac1 est plus grand ou égal à celui de ac2.
- les catégories de ac1 incluent celles de ac2.

La relation de dominance est définie formellement comme suite:

Soit L, l'ensemble des niveaux de sécurité, muni de la relation d'ordre partiel ($\geq$) et C, un ensemble de catégories, muni de la relation d'ordre partiel ($\supseteq$). Soit l1, l2 deux niveaux et c1,c2 deux catégories tels que l1 $\in$ L, l2$\in$ L, c1 $\in$ C et c2 $\in$ C.

$\forall$ ac1 = (l1,c1), ac2 = (l2,c2) : ac1 $\geq$ ac2 $\Leftrightarrow$ l1 $\geq$ l2 $\wedge$ c1 $\supseteq$ c2.on dit que deux classes d'accès ac1 et ac2 sont incomparable si on ne peut vérifier ni ac1 $\geq$ ac2 ,ni ac2 $\geq$ ac1.L'ensemble de classes qui possède une relation d'ordre ($\geq$) possède une borne inférieure et supérieure. Cet ensemble a une structure de forme d'un treillis **[32]**.

La figure **II.2** représente un exemple de treillis de sécurité pour le système militaire **[33].**

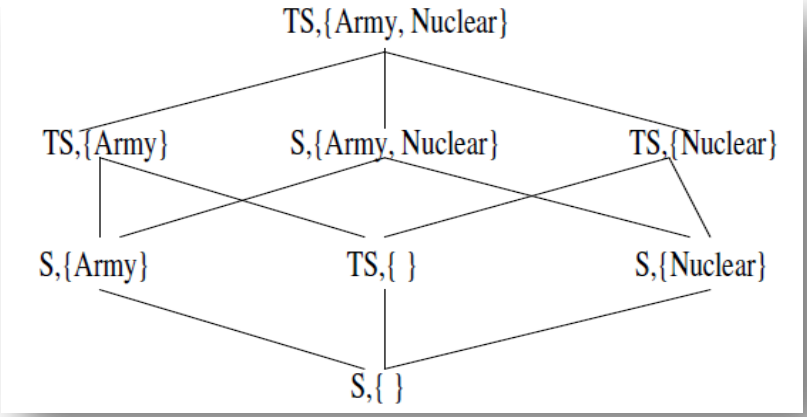


Figure II.2:Un exemple d'un treillis de sécurité

- **Modèle de Bell et LaPadula (BLP)**

Ce modèle a été proposé par David Elliott Bell et Len LaPadula en 1973**[34].** Il était destiné au département de la défense américaine, dont le but d'assurer la confidentialité des données militaires. Ce modèle a pour objectif la protection du secret des informations. Il est basé sur la classification des objets et des sujets par niveaux de secret.
L'ensemble des niveaux de secret est muni d'un ordre partiel (>).
Par exemple : Top secret (TS) > Secret (S) > Confidentiel (C) > Non classifié (NC).
Politique de sécurité : La politique de sécurité du modèle de Bell et LaPadula se résume dans les deux principes :
•**No Read Up Secrecy** : préserve de la lecture d'une information dans un objet par un sujet de niveau de secret inférieur.
•**No Write Down Secrecy** : préserve d'un transfert d'information d'un objet vers un autre objet de niveau de secret inférieur, par un utilisateur qui n'est pas de confiance. **[30].**

- **Modèle de Biba**

Ce modèle a été développé par Kenneth J. Biba en1977 **[26] [35].** Il a pour but d'assurer la sécurité à différents niveaux et l'intégrité des données **[36]**. Ila pour objectif la protection de l'intégrité des données. Il applique à la protection de l'intégrité une stratégie similaire à celle de la protection du secret par le modèle BLP : les sujets et les objets sont classés par niveaux d'intégrité.
L'ensemble des niveaux d'intégrité est muni d'un ordre partiel (>).
Par exemple : Crucial (TS) > Très important (TI) > Important (I) > Non classifié (NC)
Politique de sécurité : La politique de sécurité du modèle de Biba se résume dans les deux principes :
•**No Write Up Integrity :** préserve de l'écriture d'une information dans un objet par un sujet de niveau d'intégrité inférieur.

•**No Read Down Integrity :** préserve d'un transfert d'information d'un objet vers un autre objet de niveau d'intégrité supérieure par un utilisateur qui n'est pas de confiance. Ce modèle interdit le passage des données d'un bas niveau d'intégrité vers un niveau d'intégrité plus haut au moment de transfert des données **[37].**

- **Modèle de la muraille de Chine (Brewer & Nash)**

Ce modèle a été développé par (Brewer & Nash) en 1989 **[38].** Il a été créé dans le but d'assurer la confidentialité des données et réduire les conflits d'intérêts entre les différentes entreprises commerciales. Il se compose de trois ensembles: C'est l'ensemble des compagnies, S l'ensemble des sujets, et le O l'ensemble des objets (fichiers). Les données sont classées en trois niveaux hiérarchiques:

- Le niveau le plus bas contient des données concernant toutes les compagnies.
- Le niveau intermédiaire regroupe les objets concernant la même compagnie.
- Le niveau supérieur regroupe les données des compagnies en concurrence.
- ✓ La fonction X, tel que X (oi) désigne l'ensemble de compagnies en compétition avec l'objet (oi).
- ✓ La fonction Y, tel que Y (oj) désigne l'ensemble des données de compagnie de l'objet (oj).

On peut avoir des conflits d'intérêts en consultant les objets, et à travers les accès antérieurs. Pour historiés les actions en utilisant la matrice N définie par:
N(s,o)=1 si (s) a déjà accédé à (o) , N(s,o)=0 sinon. L'objectif est d'empêcher l'accès des utilisateurs à des ensembles en conflit d'intérêt en même temps.
On définit les deux règles suivantes:

- **Propriété simple**

Le sujet peut accéder à un objet demandé si seulement l'objet appartient au même ensemble de données de compagnie.

- **propriété en étoile**

Un sujet ne pourra écrire dans un objet si et seulement la propriété simple lui donne l'autorisation d'y accéder **[39].**

III.1.3. Contrôle d'accès à base de rôles (Role Based Access Control : RBAC)

Ce modèle a été mis en œuvre par le NST (National Institute of Standard and Technology) en 1992 **[Web.10].**
Il a pour but de simplifier l'administration de la politique de contrôle d'accès aux données. Plutôt que de donner directement des permissions aux utilisateurs, on définira différents rôles possibles pour l'utilisation du système d'exploitation, avec des droits d'accès associés. Ensuite chaque utilisateur a accès à une liste de rôle, suivant son activité. Un seul rôle peut être actif à un moment donné **[40].**
On peut améliorer les modèles discrétionnaires en créant des rôles qui sont des ensembles d'autorisation. Les autorisations sont octroyées aux rôles et les rôles aux utilisateurs.

Pour pouvoir réaliser une action sur un objet un utilisateur doit ouvrir une session et activer celui de ses rôles qui contient l'autorisation de réaliser cette action.
La figure **II.3** représente la hiérarchie du modèle RBAC et les interactions entre système **[Web.11].**

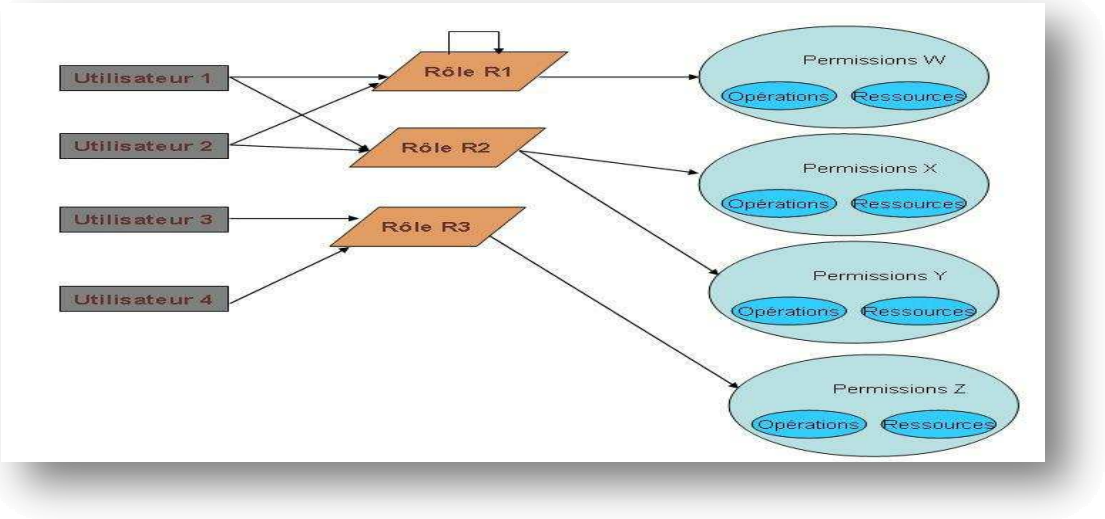


Figure II.3:Exemple de modèle RBAC

IV. Méthode de cryptage

Le cryptage est l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un message dont le contenu ne doit être connu que de son émetteur et de son destinataire **[41]**. C'est aussi un moyen de transformation des données dont le but est de masquer leur contenu, d'empêcher leur modification ou leur utilisation illégale. On distingue deux grandes catégories de méthodes: le cryptage symétrique et le cryptage asymétrique.

IV.1. Le cryptage symétrique

Le cryptage symétrique (aussi appelé cryptage de clé sécrète) permet de transformer des données en clair avec une clé sécrète et le résultat obtenu sont des données chiffrées. Il consiste à effectuer le chiffrement et déchiffrement de ces données à l'aide d'une même clé. C'est à dire que l'émetteur utilise une clé sécrète pour chiffrer les données et le destinataire utilise la même clé pour les déchiffrer.
Exemple de méthodes symétriques: **DES, AES.**
La figure **II.4** illustre un schéma du principe du chiffrement symétrique selon la référence **[42].**

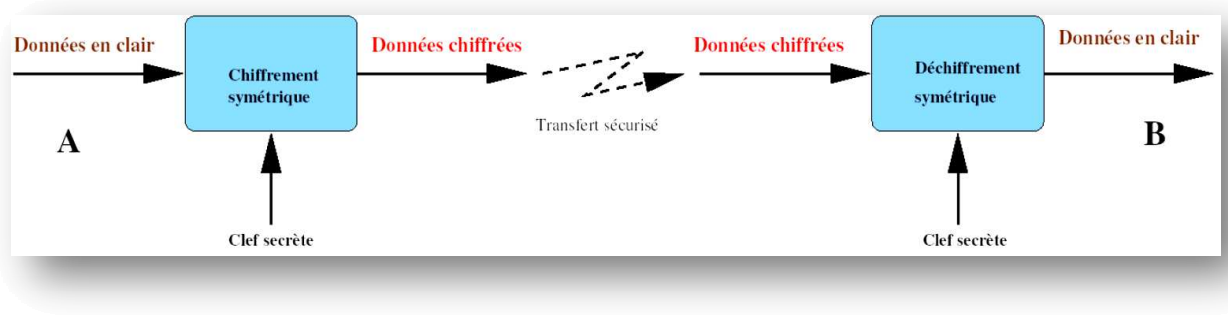


Figure II.4:Principe du chiffrement symétrique

IV.2. Le cryptage asymétrique

Le cryptage asymétrique (aussi appelé cryptage de clé publique/privée) est aussi une méthode de chiffrement des données qui permet l'utilisation de deux clés dont une clé publique qui sert à chiffrer et une clé privée servant à déchiffrer. Ici l'émetteur dispose de deux clés dont une clé publique qu'il envoie au destinataire et une clé privée qu'il conserve sans la divulguer à quiconque. Il doit être impossible de déduire la clé privé de la clé publique.

Exemple de méthodes asymétriques: **RSA, SSL.**

La figure **II.5** illustre un schéma du principe du chiffrement asymétrique selon la référence **[43].**

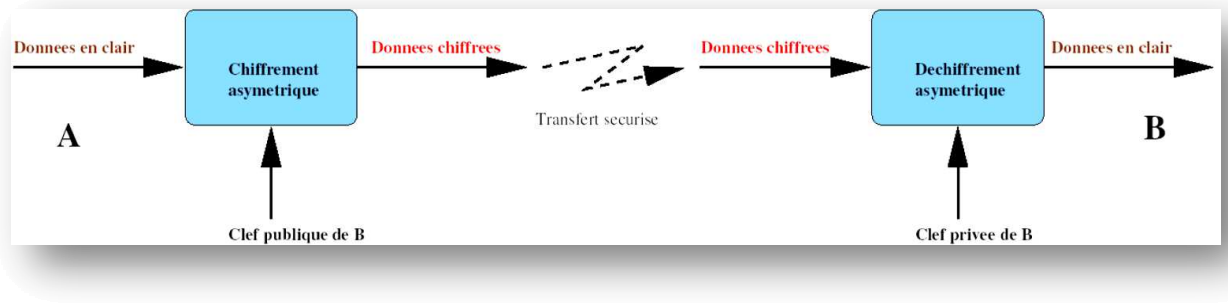


Figure II.5: Principe du chiffrement asymétrique

Dans le cadre de notre stage, il nous a été demandé d'étudier et de mettre en œuvre le standard AES.

V. Algorithme AES

Advanced Encryption Standard ou AES (soit « standard de chiffrement avancé » en français) est un algorithme de chiffrement et de déchiffrement symétrique. Il permet de transmettre un message confidentiel à travers un canal non sécurisé **[44]**. Pour AES les blocs de données en entrée et en sortie sont des blocs de 128 bits, c'est-à-dire qu'il opère sur des blocs de 128 bits texte clair qu'il transforme en blocs cryptés de 128 bits par une séquence d'opérations ou rondes(round), à partir d'une clé de 128, 192 ou 256 bits **[web.12].** Suivant la taille de celle-ci, le nombre de rondes diffère : respectivement 10, 12 et 14 rondes. AES utilise une même clé secrète pour le chiffrement et le déchiffrement.

Les clés secrètes ont au choix suivant la version du système : 128 bits (16 octets), 192 bits (24 octets) ou 256 bits (32 octets). Le chiffrement et le déchiffrement s'effectue de la même manière et sont composés de ronde. Le nombre de rondes dépend de la longueur de la clé et du message clair.

Pour comprendre le fonctionnement interne d'AES il faut commencer par l'envisager dans son schéma bloc comme les montres la figure**II.6**.Les différentes opérations seront détaillées successivement par la suite. C'est un algorithme itératif. Il est découpé en trois blocs ; pour le processus de chiffrement chaque bloc compte des opérations à faire ;

Bloc 1 : première étape (Initial Round), c'est la plus simple des étapes. Elle ne compte qu'une seule opération : AddRoundKey.

Bloc 2 : deuxième étape (N Rounds), cette étape est constituée de N itérations comportant chacune les quatre opérations suivantes :

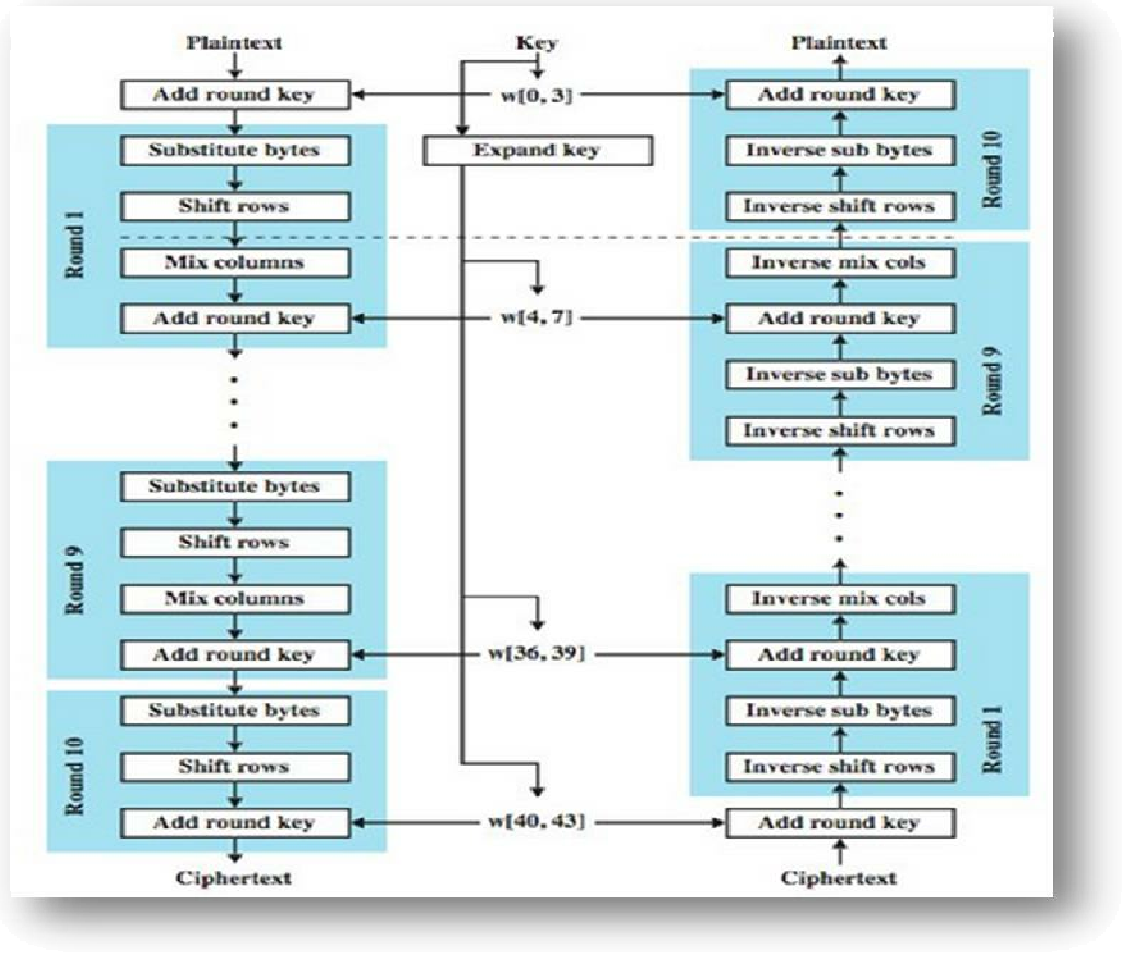
- **Sub_Bytes (substitution par octet),**
- **Shitf_Rows (décalage par ligne),**
- **Mix_Columns (mélange par colonne),**
- **AddRound Key (addition de la clé ronde).**

Bloc 3: troisième étape (Final Round), cette étape est quasiment à l'une des N itérations du deuxième bloc. La seule différence est qu'elle ne comporte pas l'opération « Mix_Columns »

Pour le processus de déchiffrement de toutes les opérations réalisées lors du chiffrement sont réversibles, à condition d'avoir la clé bien étendue car à chaque étape et pour chaque itération une nouvelle clé sera déduite.

La figure **II.6** illustre le schéma bloc d'AES.

Plaintext (texte clair) --- ciphertext (texte chiffré)



a)Chiffrement **b) Déchiffrement**

Figure II.6: Schéma bloc d'AES

- **Les étapes de l'algorithme AES-128 bits**
  - **Découpage des données et des clés sous forme matricielle**

Comme tout système cryptographique symétrique, AES dispose de deux entrées à savoir le texte clair à chiffrer (plaintext) et la clé de chiffrement (key). La longueur de la clé est fixe (128bits), ainsi la longueur du texte clair est variable d'une application a une autre. Or, AES étant un algorithme de bloc, il doit commencer par découper le texte clair selon la longueur de la clé. Ensuite le bloc de texte clair en cours de chiffrage ainsi que la clé sont mis sous forme matricielle.

La figure **II.7** illustre la forme du texte clair et de la clé AES-128

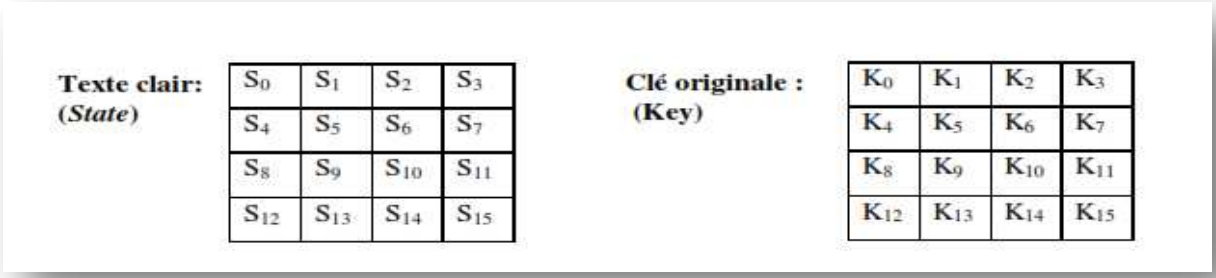


Figure II.7 : Forme du texte clair et de la clé AES-128

Pour la version 128 bits de l'algorithme, les matrices obtenues sont carrées c'est-à-dire la matrice est de Nc=4 (Nc désigne le nombre de colonnes) et Nl (Nl désigne le nombre de lignes).Elle compte 16 éléments chacun de ses éléments contient 1 byte.

❖ **Chiffrement**

Lorsque les matrices seront formées, le processus de chiffrement peut commencer :

- **Bloc 1**

Première étape – round 0 : Consiste à combiner la matrice du texte clair (state) (voir figure 15) avec la clé originale. Cette opération s'appelle Add Round Key .Elle consiste à additionner modulo 2 (OU exclusif ou XOR) chaque byte de la matrice du texte clair avec son homologue de la matrice de la clé originale (key) (voir figure 15). On obtient ainsi une nouvelle matrice appelée matrice « Etat ». Elle constitue la matrice d'entrée de l'étape suivante.

- **Bloc 2**

Deuxième étape – rounds 1-9 : Cette partie du processus de chiffrement dépend de la taille de la clé utilisée. Comme il a été déjà démontré la taille de la clé change le nombre d'itérations « N ». Chacune de ses N itérations effectuent successivement les quatre opérations détaillées ci-dessous :

✓ **Sub bytes**

Cette opération consiste à remplacer chaque byte de la matrice d'Etat par une autre valeur. La substitution se fait à l'aide d'une table S-Box. Les bytes que cette table contient sont les bytes de remplacement. Le Tableau **II.2** illustre **la table S-Box.**

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tableau II.2 : Table S-Box

La substitution se fait de la manière suivante, pour chaque élément de cette matrice procéder comme suit :

- Le premier caractère hexadécimal indique une ligne de la S-Box tandis que le deuxième indique une colonne
- Le byte se trouvant à l'intersection colonne – ligne dans la S-Box est celui qui doit être substitué à celui de la matrice Etat.

✓ **Shift Rows**

Cette opération consiste à décaler des lignes dans la matrice Etat. De faibles changements dans le texte clair impliquent de grands changements dans le texte chiffré. Le décalage ne modifie pas les valeurs des bytes, mais change leur ordre et on obtient une nouvelle matrice Etat. Le décalage se fait comme suit :

- La première ligne n'est pas décalée.
- La deuxième ligne est décalée d'un 1 byte vers la gauche.
- La troisième ligne est décalée de 2 bytes vers la gauche.
- La quatrième ligne est décalée de 3 bytes vers la gauche.

✓ **Mix Columns**

Elle consiste à multiplier une matrice constante avec une matrice Etat. L'opération Mix columns est particulièrement laborieuse puisque les Si-1 autres éléments de la matrice doivent tous être calculés de cette manière (Si est le nombre d'élément de la matrice Etat, pour AES-128 bits, Si=16 éléments).

La figure**II.8** illustre l'opération Mix Columns

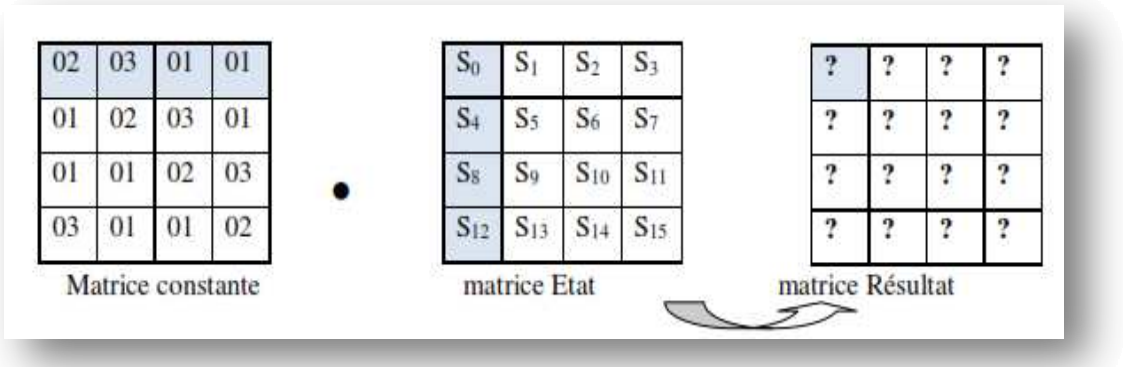


Figure II.8 : L'opération Mix Columns

- ✓ **Add Round Key**

Lors du processus de chiffrement, AES transforme la clé (matrice key). A chaque itération (round), une matrice clé différente est utilisée (roundN key). Ceci permet d'éliminer les attaques liées à la clé en faisant disparaitre la symétrie. Pour obtenir les 10 nouvelles clés nécessaires AES procède à une opération appelée Key Scheduling ou Key Expansion (cette opération sera expliquée au point suivant). Si la clé change à chaque rond l'opération Add Round Key reste simple. Elle consiste, tout comme celle de la première étape à additionner modulo2 (XOR) la matrice Etat et la clé itération en cours (roundN key).

- ❖ **Bloc 3**

Troisième étape - round 10 : C'est une étape identique à l'un des N itérations de la deuxième étape. La seule différence est que, dans cette dernière itération l'opération Mix Columns n'est pas effectuée.

Extension de la clé (Key Expansion) : Il s'agit ici de voir comment AES opère pour réduire les N+1 clés secondaires dont il a besoin pour aboutir au texte chiffré. On considère les deux matrices suivantes Rcon (elle est donnée et constante) et la clé originale (key).

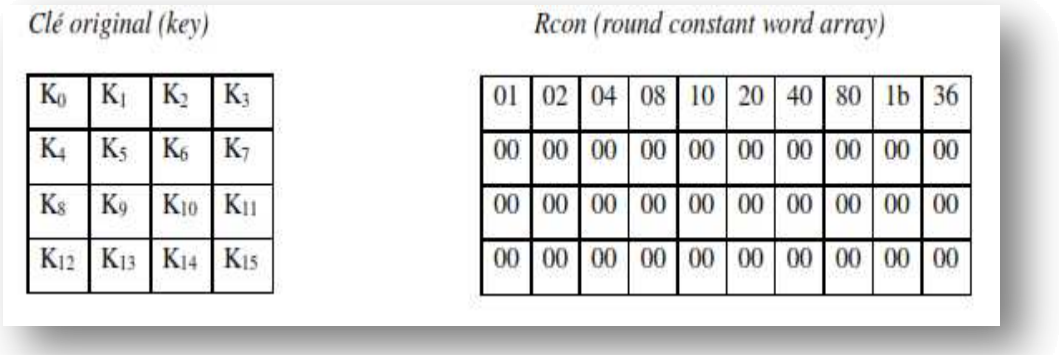


Figure II.9 : Matrice utilisée dans l'extension des clés

Les quatre vecteurs composant la matrice clé sont appelés Mots (Words, ce sont des mots de 32 bits). On commence par calculer le cinquième vecteur Wi :

Wi-4			Wi-1	Wi
K_0	K_1	K_2	K_3	?
K_4	K_5	K_6	K_7	?
K_8	K_9	K_{10}	K_{11}	?
K_{12}	K_{13}	K_{14}	K_{15}	?

On prend le vecteur Wi-1 auquel on applique une opération appelée Rot Word qui consiste en un simple décalage des quatre bytes du vecteur vers le haut. Au résultat on applique encore l'opération SubBytes :

Wi-1	*RotWord*(Wi-1)	SubBytes {*RotWord*(Wi-1)}
K_3	K_{15}	K'_3
K_7	K_7	K'_7
K_{11}	K_{11}	K'_{11}
K_{15}	K_3	K'_{15}

Le vecteur obtenu (SubBytes {RotWord (Wi-1)}) doit encore être additionné modulo2 avec le vecteur Wi-4 ainsi que le premier vecteur de la matrice Rcon :

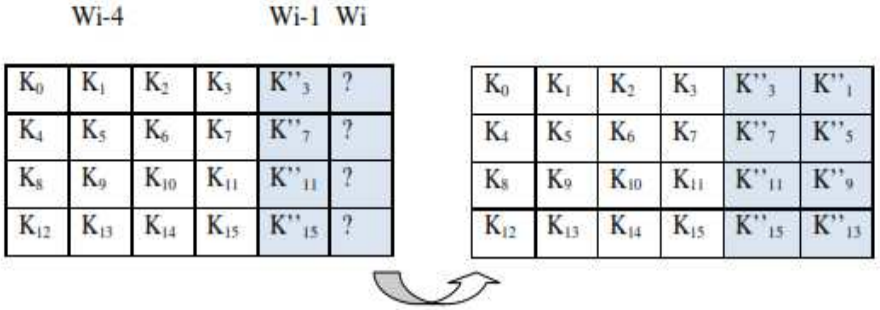
Wi-4		*Rcon(colonne1)*		*SubBytes{RotWord(Wi-1)}*	*Wi*
K_0	⊕	01	⊕	K'_3	K''_3
K_4		00		K'_7	K''_7
K_8		00		K'_{11}	K''_{11}
K_{12}		00		K'_{15}	K''_{15}

Le vecteur résultant de cette addition est Wi.

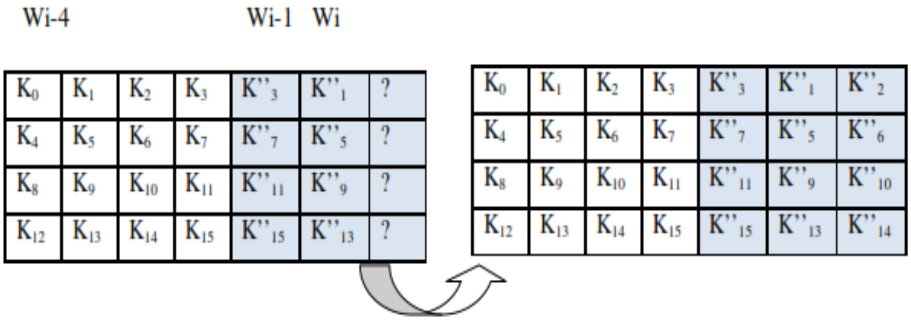
Il constitue le premier des quatre vecteurs de la deuxième clé :

K_0	K_1	K_2	K_3	K''_3
K_4	K_5	K_6	K_7	K''_7
K_8	K_9	K_{10}	K_{11}	K''_{11}
K_{12}	K_{13}	K_{14}	K_{15}	K''_{15}

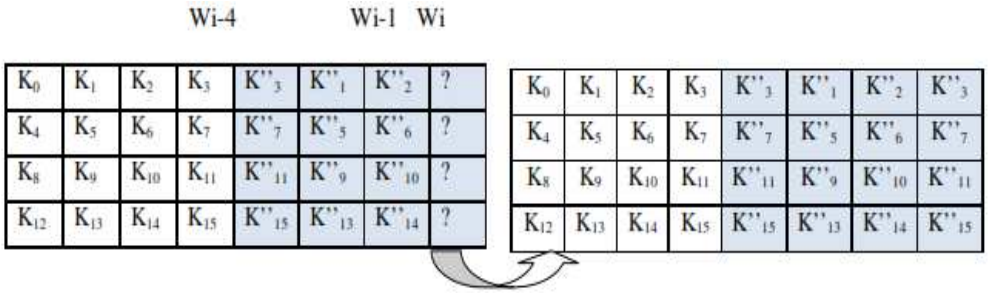
Le deuxième vecteur de la deuxième clé s'obtient plus simplement que le premier. En effet, il est donné par Wi=Wi-4 Xor Wi-1 :



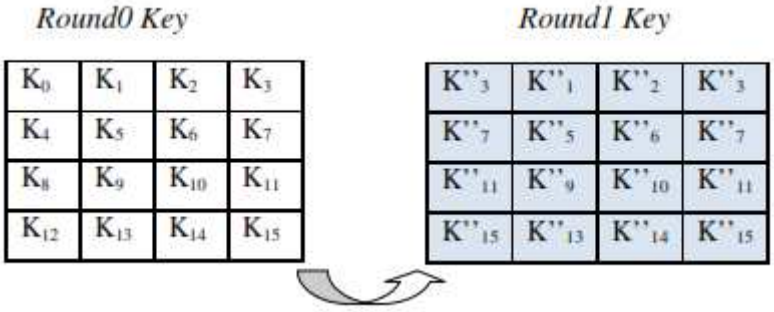
Le troisième vecteur de la deuxième clé s'obtient de la même manière que la deuxième. On a donc à nouveau Wi=Wi-4 Xor Wi-1



Le quatrième et dernier vecteur de la deuxième clé s'obtient de la même manière que le deuxième et troisième Wi=Wi-4 Xor Wi-1 :



Les quatre vecteurs de la deuxième clésont maintenant définis. La matrice key a doublé de taille. Elle contient pour l'instant les clés du round 0 et 1.



Il reste à faire 9 fois l'intégralité de cette démarche d'extension de la clé pour trouver les 9 autres clés secondaires.

❖ **Déchiffrement**

Lors du processus de déchiffrement, toutes les opérations déjà définies lors du chiffrement sont réversibles, pour déchiffrer on doit procéder comme suit :

- Le destinataire procède à l'extension de la clé de la même manière que l'émetteur a procédé lors du chiffrement.
- Les additions modulo 2 (Xor) effectuées lors de l'opération Add Round Key sont réversibles (en effet, (A Xor B) Xor B) = A
- L'opération SubBytes est inversée en utilisant la table Box inverse (Inverse S-Box).Si par exemple la S-Box indique le byte F7 (ligne 2, colonne 6) alors la Inverse S-Box restituera le byte 26 (ligne F, colonne 7).
- Les décalages Shift Rows sont inversés, c'est à dire effectués vers la droite.
- La multiplication matricielle de l'opération Mix Columns nécessite une autre matrice constante que celle utilisée en chiffrement. Une fois la matrice inverse obtenue, la manipulation est la même que pour l'opération Mix Columns faite lors du chiffrement.

VI. Conclusion

Dans cette partie nous avons abordé les définitions et les concepts majeurs de la sécurité des données. Pour renforcer cette sécurité pour qu'elle soit satisfaisante on a fait appel au cryptage qui est un moyen de transformer les données dans le but de masquer leur contenu, d'empêcher leur modification ou utilisation illégale. Parmi les méthodes de cryptage nous nous intéressons au cryptage symétrique.

Ainsi le point le plus important de cette partie réside dans le chiffrement symétrique d'où l'algorithme AES qui fait l'objet de notre travail. Dans la section suivante nous essayerons de sécuriser notre entrepôt de données spatiales notamment les requêtes multidimensionnelles à travers l'algorithme AES 128 bits.

I. Introduction

Après avoir détaillé les données nécessaires à la conception de notre système, à l'aide des éléments définis et expliqué dans les chapitres précédents. Cette démarche permis de mieux comprendre le système d'aide à la décision spatiale qui est comment construire un modèle décisionnel qui tentera de répondre aux objectifs que nous nous sommes fixés. Pour se faire, nous allons présenter les outils utilisés et la plateforme utilisée pour la modélisation de notre entrepôt de données spatiales (EDS), création du cube, comment l'analyser, voir l'avantage de l'algorithme AES 128 bits et enfin passé à la partie suivante qui concerne l'implémentation et la réalisation de notre projet.

II. Conception de la solution

Concernant notre projet nous allons nous intéresser à la planification urbaine. Notre travail est constitué de trois parties :

Première partie : appliquer les principes des systèmes d'information géographiques afin d'extraire les données utiles à une bonne modélisation.

Deuxième partie : appliquer les techniques de l'OLAP pour l'analyse et le suivi des données de la planification urbaine qui permettrait à l'expert à la fois de prendre des décisions, comprendre, prédire, et expliqués les situations auxquelles il fait face, ainsi de valider le modèle. Le modèle décisionnel proposé servira le Suivi de la réalisation des Bâtiment pour essayer d'intervenir au niveau décisionnel qui va décider de la politique publique à suivre en utilisant les technologies géo-décisionnelles les plus avancées (Datawarehouse, Datamart, SIG, cube, OLAP, SOLAP)

Troisième partie : et enfin essayer d'appliquer notre algorithme AES 128 bits sur les requêtes entre l'interface SOLAP et notre cube plus précisément au niveau des résultats de nos requêtes ce qui est le but principal de notre projet.

III. Modèle décisionnel proposé

Avant de présenter en détail notre modèle décisionnel proposé pour la planification urbaine, nous donnons en quelques lignes, un bref aperçu sur le domaine de l'aide à la décision et les systèmes Interactifs d'aide à la décision.

III.1. L'aide à la décision

L'aide à la décision consiste à assister les décideurs et les aider à mieux exprimer leurs choix et préférence vis-à-vis d'une situation donnée. On ne cherche donc pas une vérité, mais bien à établir une démarche permettant aux décideurs d'apprendre sur le problème pour mieux faire le choix.

III.2. Les Systèmes Interactifs d'Aide à la Décision (SIAD)

Un SIAD est « un système informatisé qui utilise les connaissances sur un sujet particulier afin d'aider le responsable lors de la prise de décision dans une catégorie de problèmes peu ou pas structurés » **[45].**

En s'appuyant sur les éléments de la planification urbaine et les quatre fonctions principales d'un SIAD citées par [**45**]. Ce modèle suit les étapes de l'approche décisionnelle spatiale proposées par **[46].**

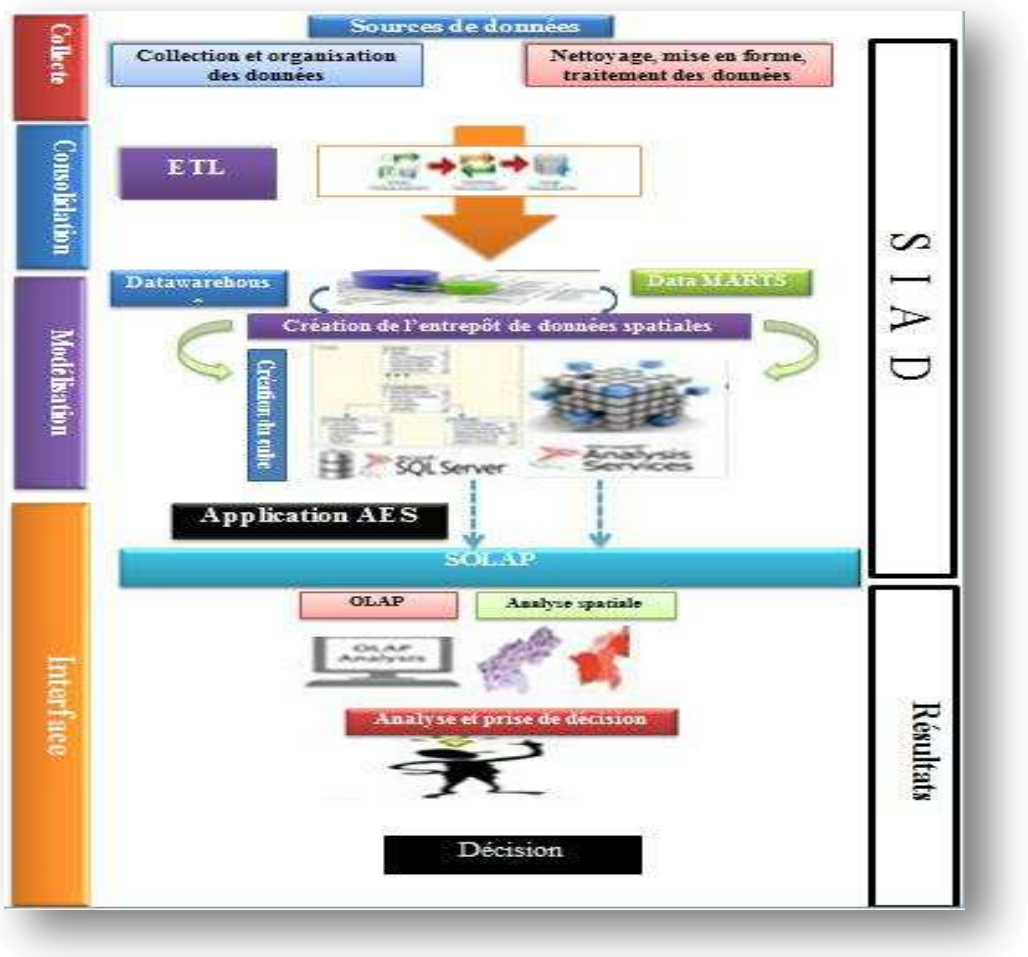


Figure III.1 : Architecture de notre système

Dans le modèle décisionnel proposé pour la planification urbaine, nous distinguons quatre fonctions fondamentales à savoir : la **Collecte, la Consolidation, la Modélisation et l'Interface.**

III.2.1. Fonction Collecte

Cette première étape se charge de la collection des différentes données de la planification provenant des différentes « **bases de données sources »** ou « **bases de production »** et les emmagasiner dans des bases de données spécialisées « **Entrepôts de données »** et **« Magasins de données ».**

On alimente la base de données depuis les sources par un système de chargement de données **ETL (Extraction, Transformation et Chargement)** destiné à **extraire** des données de diverses sources (bases de données de production, fichiers, Internet, etc.),qui sont souvent hétérogènes en les rendant homogènes, les transformer et les charger dans un entrepôt de données **afin de les analyser [47].**

III.2.2. Fonction Consolidation (structuration et stockage)

Élément central qui permet aux applications décisionnelles de bénéficier d'une source d'information commune, homogène, normalisée et fiable qui masque la diversité de l'origine des données provenant de différentes sources. La fonction de consolidation est généralement assurée par la gestion des métadonnées, qui assurent l'interopérabilité entre les données.

Cette phase comporte tous les outils de création d'un entrepôt de données (ED) en passant par sa Conception, sa modélisation et sa structuration.

- **Conception**

Ceci concerne la conception multidimensionnelle des données dans des cubes ou hyper cubes. Un entrepôt de données peut héberger des milliers de variables mais quelques dizaines seulement sont exploitées pour une activité décisionnelle particulière. Pour cela on utilise des outils décisionnels comme les tableaux, les cubes et les hyper cubes. La conception du Data Warehouse s'articule essentiellement autour de la mémorisation des données dans une base de données unique. L'identification des besoins permettra de sélectionner dans le système d'information opérationnel les données nécessaires pour l'élaboration des informations demandées et les mémoriser dans une base unique.

- **Modélisation dimensionnelle**

L'indicateur de succès d'un projet de Data Warehouse est sa capacité de fournir les informations nécessaires au moment souhaité. Pour aboutir à ce niveau de succès, il faut se baser sur plusieurs niveaux de détails de données, ce qui est assuré par la modélisation multidimensionnelle. La modélisation multidimensionnelle permet la représentation explicite des hiérarchies et même la possibilité de manipuler à la fois le contenu et la structure des données **[6].**

- **Structuration en cubes multidimensionnels**

Les Data Warehouse sont destinés à la mise en place de systèmes décisionnels. Ces systèmes, devaient répondre à des objectifs différents des systèmes transactionnels, on fait ressortir très vite la nécessité de recourir à un modèle de données simplifié et aisément compréhensible. La modélisation dimensionnelle permet cela. Elle consiste à considérer un sujet d'analyse comme un cube à plusieurs dimensions, offrant des vues en tranches ou des analyses selon différents axes et utilise des opérateurs spécifiques aux cubes pour répondre de manière pertinente aux requêtes des utilisateurs.

III.2.3. Fonction Modélisation (Outils d'analyse et d'interprétation)

Cela concerne la phase d'analyse en ligne chargée de la création du cube à partir de l'ED déjà mis en place. Cette étape contient les outils OLAP (On Line Analytical Processing) à savoir les outils d'Analyse, les outils de restitution des données sous différentes formes (graphiques ou tableaux) et les outils d'administration.

- **Analyse des données**

Cette phase est le but du processus d'entreposage des données. Elle doit permettre toutes les analyses nécessaires pour la construction des indicateurs recherchés.

- **Restitution des résultats d'analyse**

L'étape de restitution se fait en utilisant des outils clients d'un entrepôt de données.

Tous les outils pouvant synthétiser, explorer, confirmer, expliquer, prédire les données sont des outils de restitution. Différents types d'usagers nécessitent différents outils d'exploitation de données. Il en existe pour cela cinq principaux types : les logiciels requêteurs, les logiciels de création de rapports, les tableaux de bord, les outils OLAP et SOLAP etc.)

- **Administration**

La fonction d'administration consiste à assurer la qualité et la pérennité des données aux différents applicatifs ; la maintenance ; la gestion de configuration ; les mises à jour; l'organisation, l'optimisation et la mise en sécurité du système d'information. La phase d'analyse et de restitution des données conditionne le choix de l'architecture de l'ED et de sa construction.

III.2.4. Fonction Interface

Cette fonction assure le contrôle **d'accès** des utilisateurs**,** la **visualisation** des résultats d'analyse sous différentes formes : tableaux de bord, graphiques, corrélation, simulation, la prise en charge des **requêtes** d'où l'application de l'algorithme **AES 128 bits** qui est une méthode qui permet de **chiffrer** les résultats de nos requêtes **multidimensionnelles.**

III.3. Outils d'investigation

Nous avons utilisé, pour l'élaboration de notre modèle décisionnel proposé, les outils d'investigation suivants :

III.3.1. Outil OLAP (cube ou hyper cube)

« Technologies permettant de collecter, stocker, traiter et restituer des données multidimensionnelles à analyser »

L'interrogation permet de connaitre, mesurer et prévoir (prise de décisions) au travers de la manipulation des données du magasin. On peut considérer plusieurs opérations de manipulation:

- Consultation des données d'un tableau et génération de graphiques;
- Requêtage graphique sur une base de données;
- Application des opérateurs multidimensionnels.

III.3.2. Outil d'affichage cartographique (SIG)

Le SIG est définit comme un système informatique de matériel, de logiciel, et de processus conçu pour permettre la collecte, la gestion, la manipulation, l'analyse, la modélisation et l'affichage de données à référence spatiale afin de résoudre des problèmes complexes de gestion. Les SIG différent selon leurs domaines d'applications et les demandes qu'ils doivent satisfaire. Toutefois, ils ont en commun des fonctionnalités nommées les « 5A » : Abstraction, Acquisition, Archivage, Affichage et Analyse.

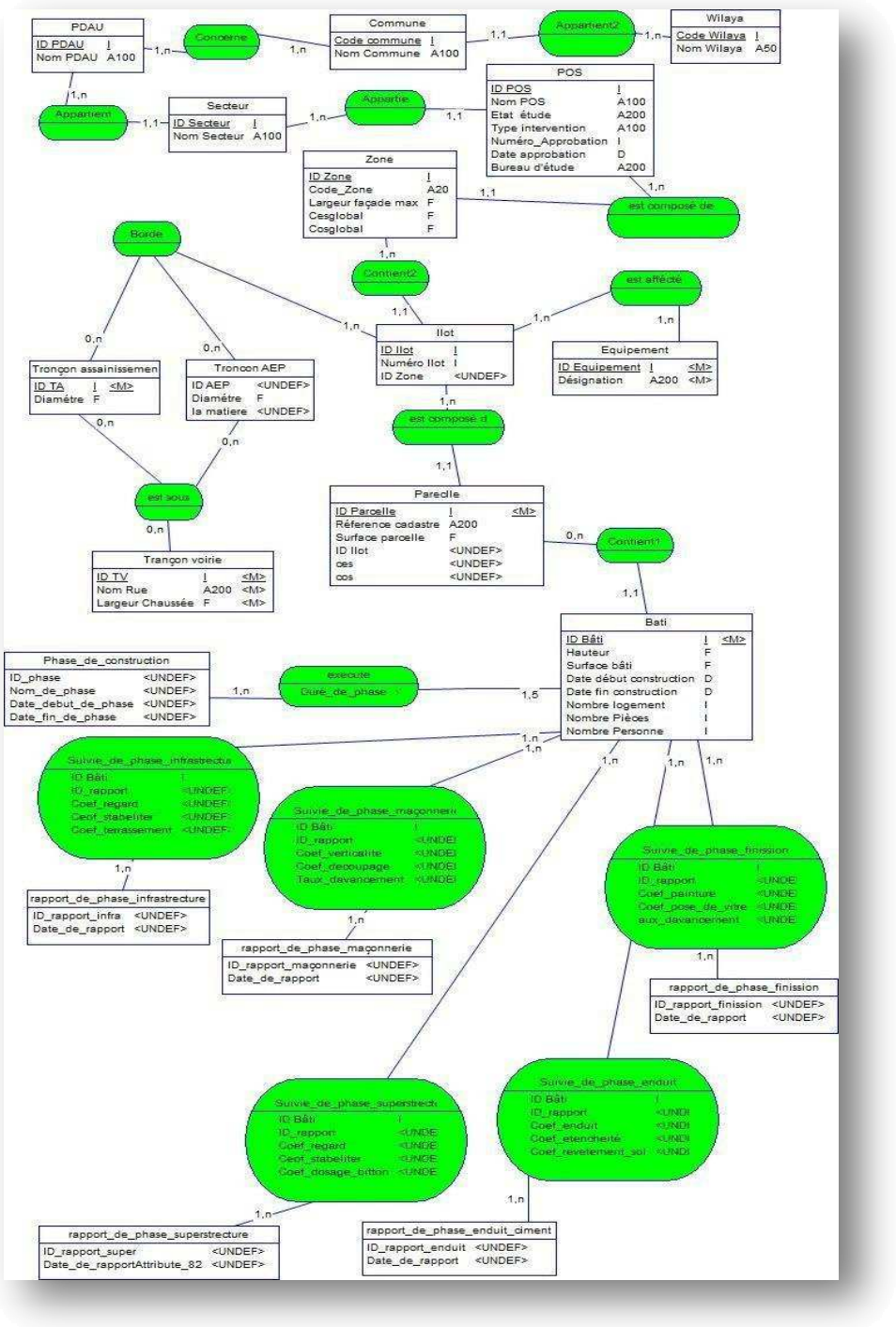
III.3.3. Outil de chiffrement de données (AES 128 bits)

Il offre des étapes qui peuvent aider à chiffrer et déchiffrer nos données pour garantir leur confidentialité. On a choisi parmi les algorithmes de chiffrement **AES 128 bits** qui permet de transmettre un message confidentiel à travers un canal non sécurisé. Il a pour but de transformer les blocs de 128 bit données claires en blocs de 128 bits données cryptés.

Notre choix était porté sur cet algorithme « **AES 128 bits**» pour ses avantages multiples tel que la rapidité à chiffrer les données, et plus la longueur de cette clé est importante, plus il sera difficile à déchiffrer les données. Néanmoins elle a quelques inconvénients à signaler tel que la confidentialité des données chiffrées d'un algorithme symétrique repose uniquement sur la protection de la clé secrète de chiffrement, si cette clé est découverte alors les données peuvent être déchiffrées.

IV. Les données de l'étude

- **Structuration de la base de données** : Notre projet va être structuré sur une partie de cette base de données, qui est construite sur le modèle conceptuel de données(MCD), comme illustré dans la figure **III.2** suivante :



FigureIII.2 : Modèle conceptuel de donnée

Ceci nous a permis de construire un modèle multidimensionnelle en étoile qui contient les tableaux en dessous, comme il est montré dans la figure suivante:

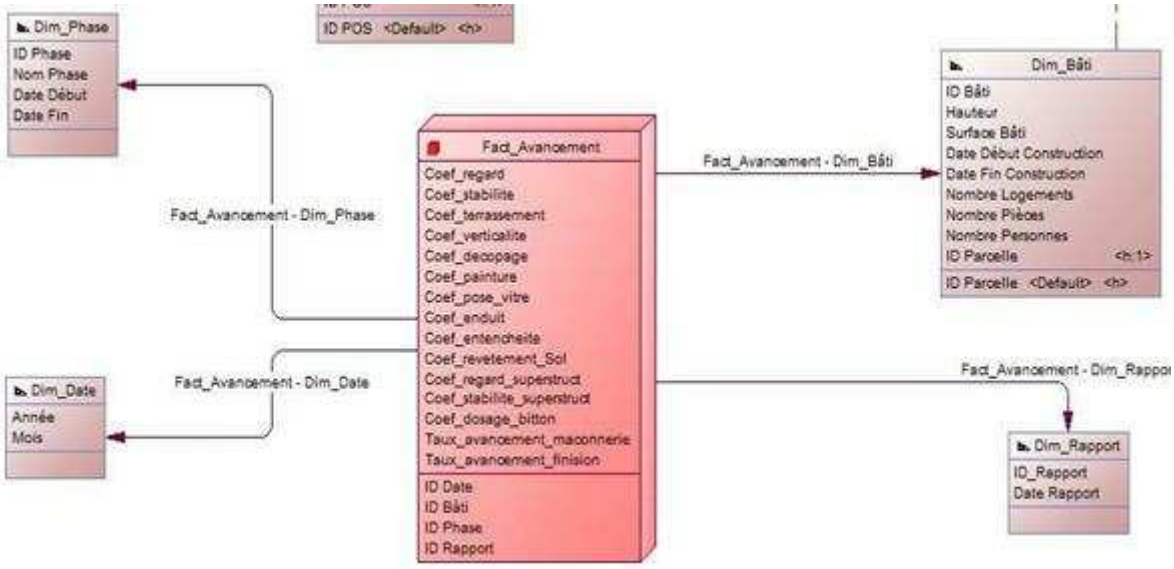


Figure III.3 : Modèle multidimensionnel

Une fois notre modèle construit, nous sommes passés par une sélection, un nettoyage, et un traitement de ces données, nous avons procédé par la suite à la création de notre entrepôt de données, l'intégration de nos données sélectionnées, nettoyées et traitées, pour cela nous avons utilisé des outils qui permettent de réalisé cette tache (Microsft SQLServer 2012).

- **Les données de la planification (données tabulaires)**

Les données de la planification utilisées dans notre étude, sont extraites d'un fichier Excel qui nous a été parvenu de la direction de l'urbanisme de la willaya de Mostaganem.

- **Les données vecteurs**

Pour notre projet, le deuxième type de données utilisées est les données contenu dans le projet de suivi réalisé dans ArcGis, qui contient les différentes couches utilisé dans la réalisation de ce projet (couche bâti, Ilot, parcelle, zones, etc.)

V. Les outils de développements utilisés

Notre choix était porté sur l'outil Microsoft SQL server 2012 pour implémenter notre base de données, l'outil Arc Gis pour le développement de notre système d'information géographique et Netbeans pour le développement de notre interface.

- **Microsoft SQL Server 2012**

Microsoft SQL Server est une application utilisée pour créer des bases de données informatiques pour la famille des systèmes d'exploitation de Microsoft Windows. Il fournit un environnement utilisé pour produire des bases de données accessibles à partir des postes de travail, du web ou d'autres média tels qu'un assistant numérique personnel **[Web.12].**

- **ArcGis 10.1**

Nous avons choisi ArcGIS 10 Desktop qui est une suite intégrée d'applications SIG professionnelles. Il existe trois niveaux de licence offerts pour ArcGIS : ArcView, ArcEditor et ArcInfo, Les autres composants d'ArcGIS sont ArcCatalog, ArcScene et ArcGlobe. ArcMap, ArcToolbox et Model Builder **[Web.13].**

- **Java sous Netbeans 8.2**

Java est un langage robuste qui peut être exploité pour développer un large éventail de programmes utilisant une interface utilisateur graphique, pouvant être appliqués en réseau pour se connecter à des bases de données, et offrant d'autres fonctionnalités toutes plus sophistiquées les unes que les autres.

La bibliothèque fournie en standard avec Java couvre de nombreux domaines (gestion de collections, accès aux bases de données, interface utilisateur graphique, accès aux fichiers et au réseau,…, sans compter toutes les extensions qui s'intègrent sans difficulté à Java) donc la bibliothèque très riche **[Web.14].**

L'API JDBC (Java DataBase Connectivity), apparue dès la JDK 1.1, permet de développer des applications capables de se connecter à des serveurs de bases de données par le biais d'un pilote.

VI. Création du projet

VI.1. Source de données

La création de notre projet, nécessite en premier lieu la détermination de la source de données, qui va être utilisée pour la construction de notre entrepôt, premièrement nous avons procédé à une extraction(collection),transformation(mise en forme, traitement, nettoyage), pour les chargés dans notre Data Warehouse, pour cela nous nous sommes basés sur des données vectoriel et tabulaire, pour le suivi des chantiers du projet urbain, à la fin nous avons obtenu des fichiers Excel extraits de la géodatabase, qui serons notre source de données pour la suite de la création du projet.

VI.2. Création de l'entrepôt de données spatiales

Dans cette première étape, nous allons expliquer les phases de création et administration de notre base de données et des différentes tables (dimensions), ainsi que leurs champs dans le moindre détail grâce au SQL Server Management Studio, installé avec SQL Server 2012.Il permet de réaliser avec une grande facilité, la plupart des taches communes aux bases de données, de la création de la base jusqu'à la modification de données. Quelques clics suffisent et pas besoin de taper la moindre requête.

VI.2.1. Création d'entrepôt de données spatiales avec « SQL Server management studio »

Avant de pouvoir réaliser une quelconque opération, il nous faut tout d'abord accéder à SQL Server Management Studio. Maintenant commençons par la création de la base de données. Dans la page d'accueil de la fenêtre de SQL Server management studio, un formulaire composé d'un champ de texte, d'une liste et d'un bouton nous permet de spécifier le nom de la base, que nous avons nommé **« Base Urbain»,** ainsi que le type d'interclassement (si aucun n'est spécifié, le type "par défaut" sera utilisé).

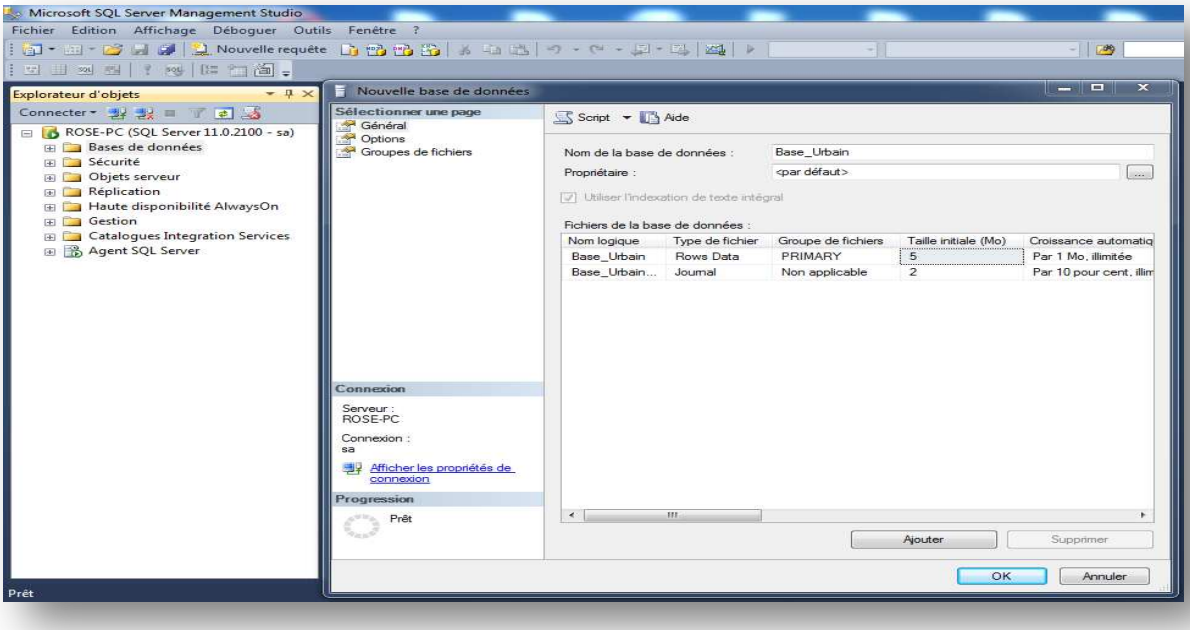


Figure III.4 : Création de la Base urbain

Après validation, on accède à une autre section ou nous pouvons créer les tables de notre base.

VI.2.2. Création des tables

Pour cela, nous nous sommes basé sur notre modèle multidimensionnel élaboré à partir du MCD conçu pour la réalisation du projet du suivi urbain, qui est un modèle en étoile modélisant les dimensions et la table de fait qui va contenir les mesures nécessaires pour la bonne modélisation de notre base, et pour faire les bonnes analyses. La création des tables est aussi simple. Il suffit d'aller dans la base de données « **Base Urbain** » crée auparavant, cliquer sur le sous dossier Table, et choisir New Table. Une nouvelle fenêtre s'affiche dans laquelle il faudra saisir le nom de la table en premier et les champs suivis de leurs types :

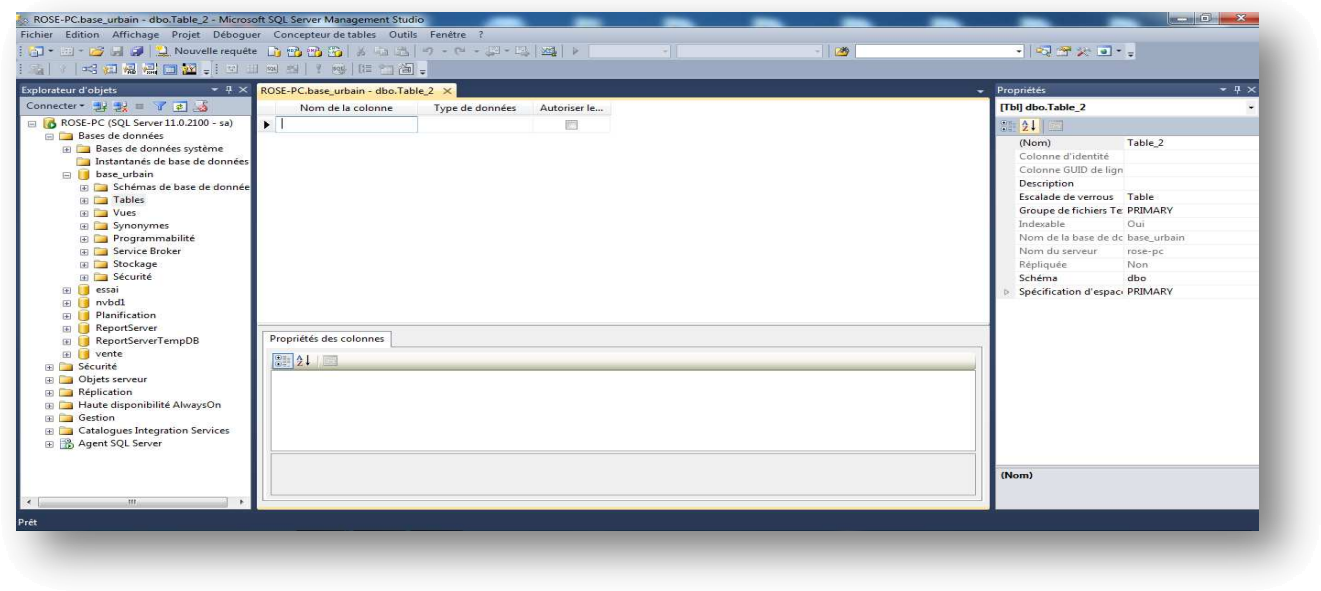


Figure III.5 : Création des tables

Comme exemple, nous allons créer la table « Bâti » .Elle contient cinq champs. Une nouvelle page nous permettra d'attribuer à chacun des quatre champs : ID Bâti, ID_Nom_Bati, Date_Debut_Construction, Date_Fin_Construction, Hauteur_Bati.

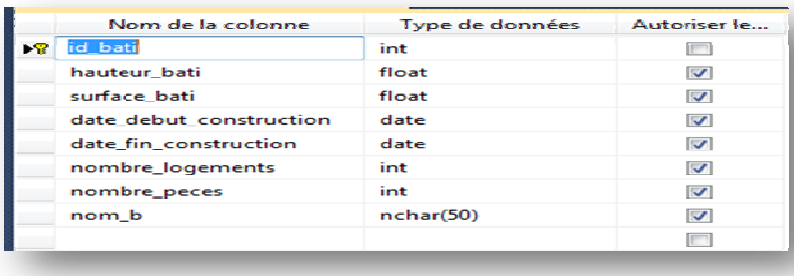


Figure III.6 : Remplissage des champs de la table Bâti

Après avoir terminé la création de la table, pour le reste des tables de la base de données on applique le même principe, après on passe au remplissage des tables en utilisant les données obtenu de l'application de l'ETL, ceci va nous permettre de passé à la création des relations qui existe entre les tables.

VI.2.3. Création des relations

Cette partie consiste à crée les relations qui existe entre les tables de notre base de données. Pour la réaliser il suffit d'un clic droit sur Database Diagrams, choisir New DataBase Diagrams.

Une fenêtre va s'ouvrir pour choisir parmi les tables de la base de données, les quelles seront concerné par la création des relations, comme il est illustré dans la figure suivante :

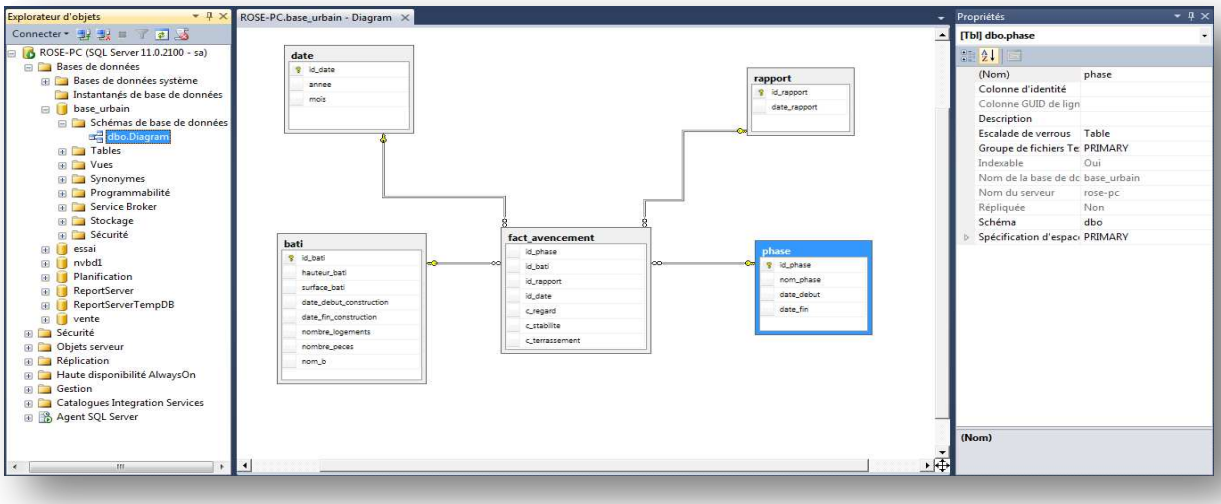


Figure III.7 : Modélisation multidimensionnelle

Pour notre modèle on a la table de fait (FactAvancement) qui a des relations avec les tables Bâti, Rapport, Phase, Date ou on a pour chaque date donnée un rapport concernant une phase pour bâti, de ce principe on modélise notre table de fait, qui contient les mesure permettant de suivre l'évolution de la réalisation des phases pour chaque bâti, de même que notre base de données.

VI.2.4. Création du cube de données

Nous allons travailler sur un entrepôt de données spatiales qui se nomme « planification urbaine ». Pour la modélisation de notre cube nous allons utiliser comme outil analysis services, il va contenir les dimensions et la table de fait crées, on va introduire les 4 dimensions suivantes : Bâti, Phase, Rapport, Date, qui sont en relation avec la table de fait, ce qui a permis de faire une analyse sur le taux d'avancement en fonction de la date, du rapport élaboré, de la phase de construction, et du bâti choisi.

De ce point on va commencer à modéliser notre cube ou nous allons obtenir un modèle en étoile en fonction des dimensions et des mesures choisie.

Pour cela on a commencé par la création d'un projet Analysis Services, qui est la première étape de la création du cube, en suite on va définir la source de données, qui est notre base de données qui existe déjà ;ceci va nous permettre de faire appel aux tables de notre base, qui vont constituer la base de la modélisation, cela après qu'on a bien choisi les dimensions et les mesures, analysis services permet de réaliser cette tâche.

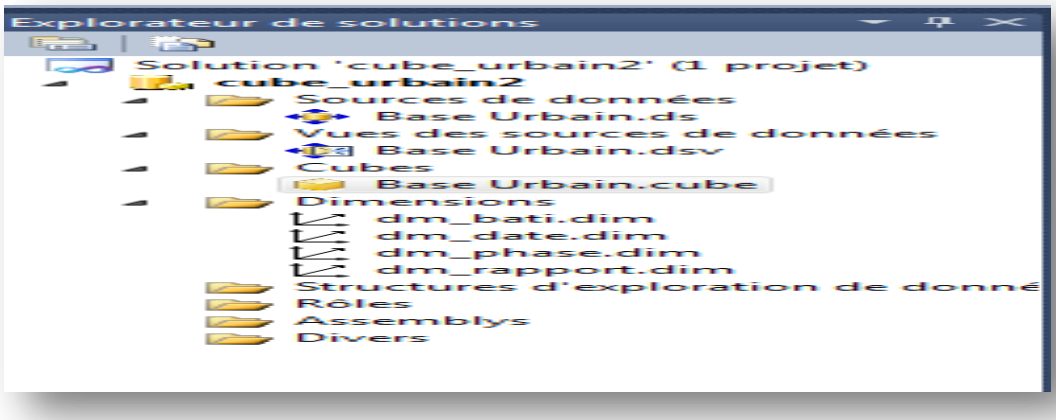


Figure III.8 : Dimensions crées

L'étape suivante consiste à la création des dimensions et leurs hiérarchies, comme expliqué dans les étapes précédentes on 4 dimensions qu'on va créer dans notre projet, on a choisi pour chaque dimension les attributs nécessaire à la création du cube, et qui vont être utilisé pour la création de la hiérarchie de la dimension, pour faciliter l'analyse, par exemple prenons la dimension bâti ou on a créé la hiérarchie comme le montre dans la figure ci-dessous:

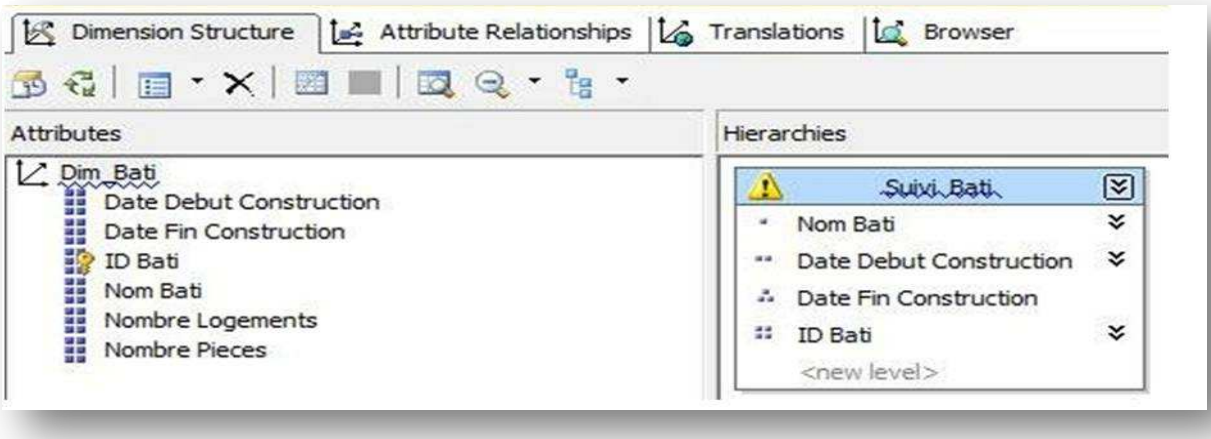


Figure III.9 : Hiérarchie pour la dimension Bâti

Une fois fini avec la création des dimensions et leur hiérarchie, nous allons passer à la création de notre cube qui consiste à définir une source de donnée view, qui offre la possibilité de choisir les dimensions et les tables de fait , ou on va spécifier la table de fait et les dimensions qui vont contenir les attributs et les mesures qu'on utilisera pour faire notre analyse selon plusieurs dimensions, ce qui nécessite une bonne sélection de ces éléments qui vont être utilisé pour la création du cube, dans notre cas on a choisi les tables de notre base de données.

Notre cube sera modélisé sur un modèle en étoile, contenant les 4 dimensions (Bâti, Date, Phase, Rapport), qui explique le processus suivit pour la modélisation ou un rapport est généré périodiquement concernant la phase de construction du bâti, de ce principe on va modéliser notre cube. La figures ci-dessous illustre le résultat obtenu de la création de notre cube en présentant les dimensions utilisées, la table de fait et les mesures et le modèle obtenu.

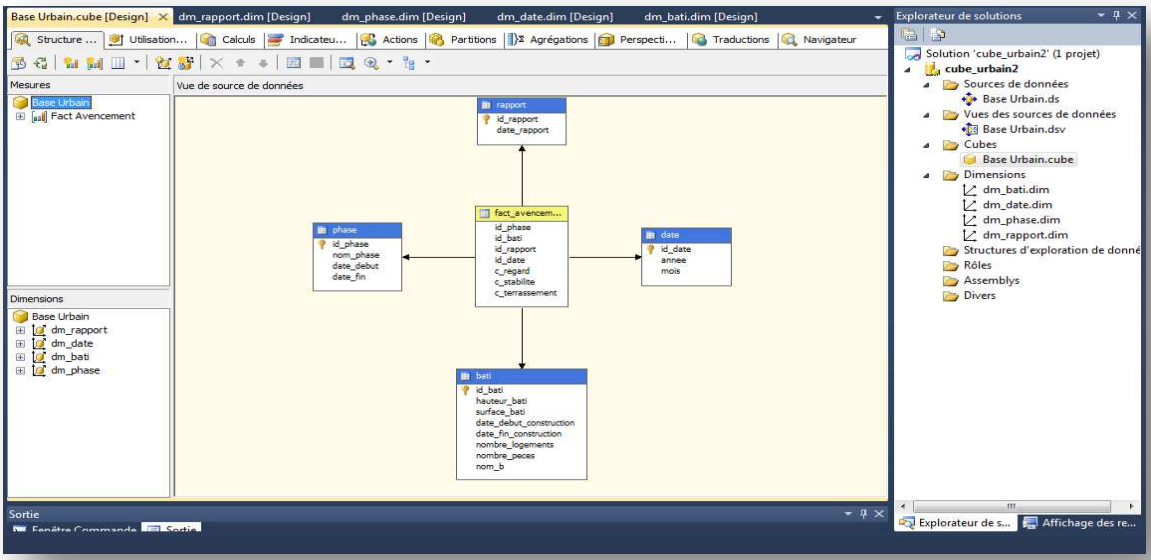


Figure III.10: Résultat obtenu de la création du cube

On a créé notre cube qui a abouti à un modèle en étoile en suivant les étapes décrites précédemment, ceci nous permettra de faire des analyse sur le cube on fonction de plusieurs dimension, nous avons fait quelque analyse sur notre cube, pour décrire l'état actuel de l'évolution de la réalisation du projet de suivi, nous avons aboutis à ces résultats en appliquant un OLAP sur notre cube.

Ce qui revient à utiliser des requêtes MDX ou on va préciser les dimensions et mesures pour l'exécution de cette dernière, pour le premier exemple choisie la requête est la suivante :

SELECT NON EMPTY { [Measures].[c Regard], [Measures].[c Stabilite], [Measures].[c Terrassement] } ON COLUMNS, NON EMPTY { ([dm_bati].[Id Bati].[Id Bati].ALLMEMBERS * [dm_bati].[Nom B].[Nom B].ALLMEMBERS * [dm_bati].[Surface Bati].[Surface Bati].ALLMEMBERS * [dm_bati].[Nombre Logements].[Nombre Logements].ALLMEMBERS * [dm_bati].[Hauteur Bati].[Hauteur Bati].ALLMEMBERS) } DIMENSION PROPERTIES MEMBER_CAPTION, MEMBER_UNIQUE_NAME ON ROWS FROM [Base Urbain]. La figure suivante montre le résultat obtenu.

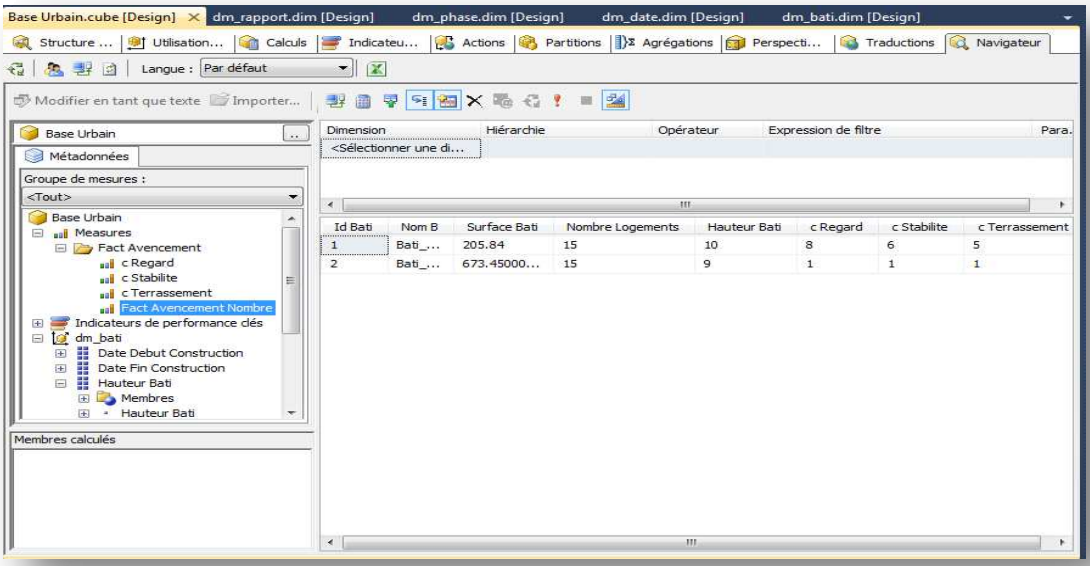


Figure III.11: Résultat obtenu de l'analyse du cube

L'exécution de la requête précédente de notre exemple à donner le résultat illustré dans la figure **III.11**, on a choisi de voir l'état d'avancement de chaque bâti en fonction des taux d'avancement pour chaque phase. Cela nous a permis de déterminer les bâtis finis, et ceux en retard et dans quelle phase ils sont. Ceci est l'un des points forts qu'offre l'application de l'OLAP sur le cube en utilisant les requêtes multidimensionnelles. L'OLAP effectué sur le cube nous a montré des résultats satisfaisant, ou nous avons pu décrire les états de l'avancement de la réalisation du suivi des chantiers du projet selon plusieurs dimensions.

VII. Développement de l'application SOLAP

Après avoir créé, analysé notre cube, on va passer à l'analyse spatiale qui n'est rien d'autre que l'intégration d'un SIG sous ArcGis. Après cela, on va essayer de combiner l'OLAP et le SIG d'où la création d'un Olap spatial. Pour ce faire, on va décrire les étapes à suivre pour la conception de notre Olap spatial et enfin les résultats obtenus à travers les interfaces suivantes. Dans ce qui suit, nous présenterons les différentes vues de l'application. La figure suivante représente l'interface principale de notre application.

Figure III.12: Interface principale

- **L'administrateur (Admin)**

La figure suivante représente la page utilisée pour l'authentification de l'administrateur en cliquant sur le bouton Admin.

Figure III.13 : Authentification Administrateur

Après l'identification de l'administrateur, la figure suivante permet d'afficher les choix possibles pour ce dernier.

Figure III.14: Consultation de la base de données

S'il clique sur le choix consulter la base de données, Il aura le choix entre des requêtes multidimensionnelles en langage MDX ou relationnelles en langage SQL, ensuite il saisit ses requêtes, il clique sur exécuter qui lui renvoi les données géographiques à travers une carte et les données attributaires à travers un tableau selon le résultat de la requête demandée. Cela se résume sur la figure ci-dessous :

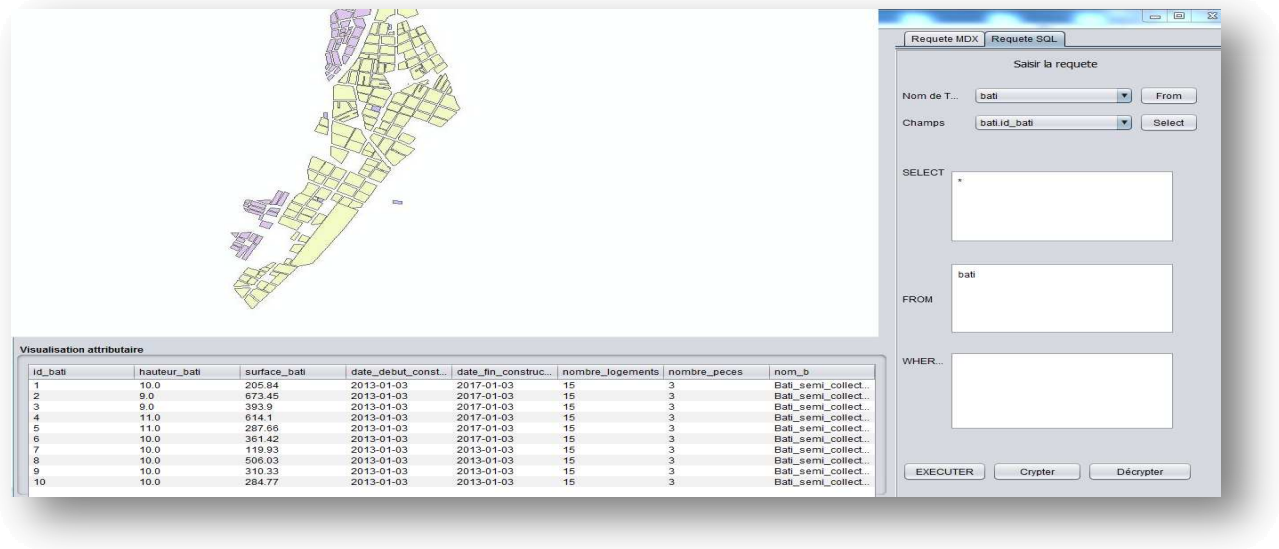


Figure III.15 : Résultat de l'exécution de la requête

Dans ce qui suit, nous proposons d'utiliser un algorithme de chiffrement afin de chiffrer les résultats des requêtes des utilisateurs stockés dans notre base afin de mieux sécuriser leurs données. Nous avons choisi l'algorithme AES pour réaliser cette opération.

VIII. Application de l'algorithme AES

Après avoir fait un tour sur les résultats obtenus de ces analyses ,qui nous montrent un aperçu de la puissance et la facilité qu'offre le SOLAP, ce qui va apporter une grande aide à la prise de décision et à l'analyse spatiale, reste maintenant à choisir l'algorithme à appliquer sur nos requêtes multidimensionnelles, pour obtenir des résultats plus riches et sécurisées, qui répondent aux besoins des décideurs .

Le choix de l'AES reste une étape importante, vus le grand besoin des requêtes demandées des utilisateurs, pour notre cas comment au mieux choisir un chiffrement efficace, qui va être utilisé pour la confidentialité des données de notre entrepôt afin de répondre aux objectifs fixés.

Pour l'accomplissement de cette tâche, on va appliquer l'algorithme sur les résultats des requêtes demandés par les utilisateurs. Ainsi l'utilisateur saisi une requête via l'interface SOLAP. Cette requête est soumise à une transformation pour qu'elle puisse être exécutée sous le format chiffré. Cette nouvelle forme de requête est envoyée vers le serveur, lequel l'exécute et renvoi les résultats chiffrés vers l'utilisateur.

Pour cela, on va générer une vue pour chaque requête demandée. Après on va essayer de crypter par l'AES le résultat de chaque vue et l'envoyer vers l'utilisateur et c'est au niveau de ce dernier que les données cryptés seront décrypter et enfin afficher. Nous allons montrer les résultats obtenus à travers les interfaces fournies par l'application de l'algorithme AES.

L'inscription d'un nouvel utilisateur, sa validation est en attente du a la validation par l'administrateur. Il propose un contrôle d'accès sur le nombre de tentatives erronés d'authentification avant de désactiver un compte existant.

Pour l'application de l'AES 128 bits sur les résultats de nos requêtes, on a deux méthodes à suivre :

Chiffrement et déchiffrement : Pour le **chiffrement**, on découpe en blocs de 128 bits nos données claires à qui on ajoute notre clé secrète de 128 bits aussi qu'on transforme en matrice de [4x4]. Une fois finie, notre matrice passe à une série de transformations/permutations/sélections. Les données s'exécutent par l'opération ronde, qui subit une transformation de substitution, décalage de rangées, déplacement de colonnes (sauf à la dernière ronde), addition d'une "clef de ronde" qui varie à chaque ronde. Ainsi, le **déchiffrement** subit les mêmes étapes mais dans le sens inverse.

Les figures suivantes nous montrent les résultats du chiffrement et du déchiffrement des requêtes par l'AES.

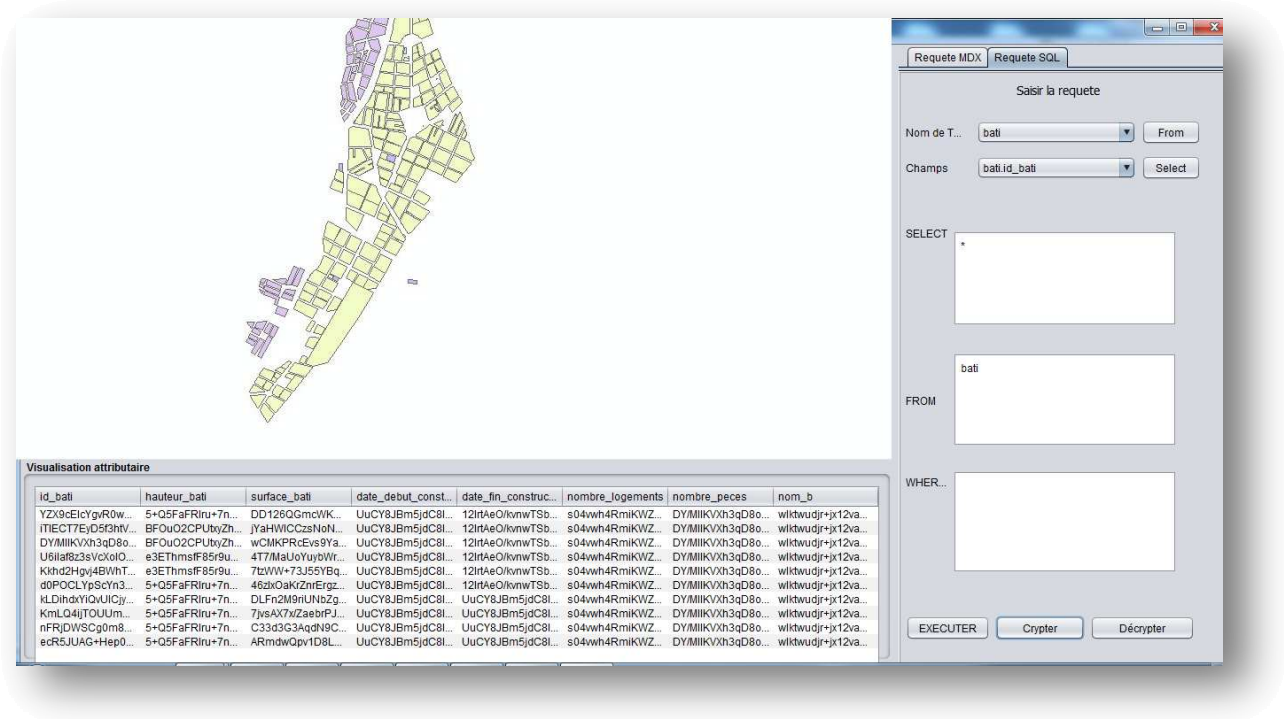


Figure III.16: Chiffrement des résultats des requêtes

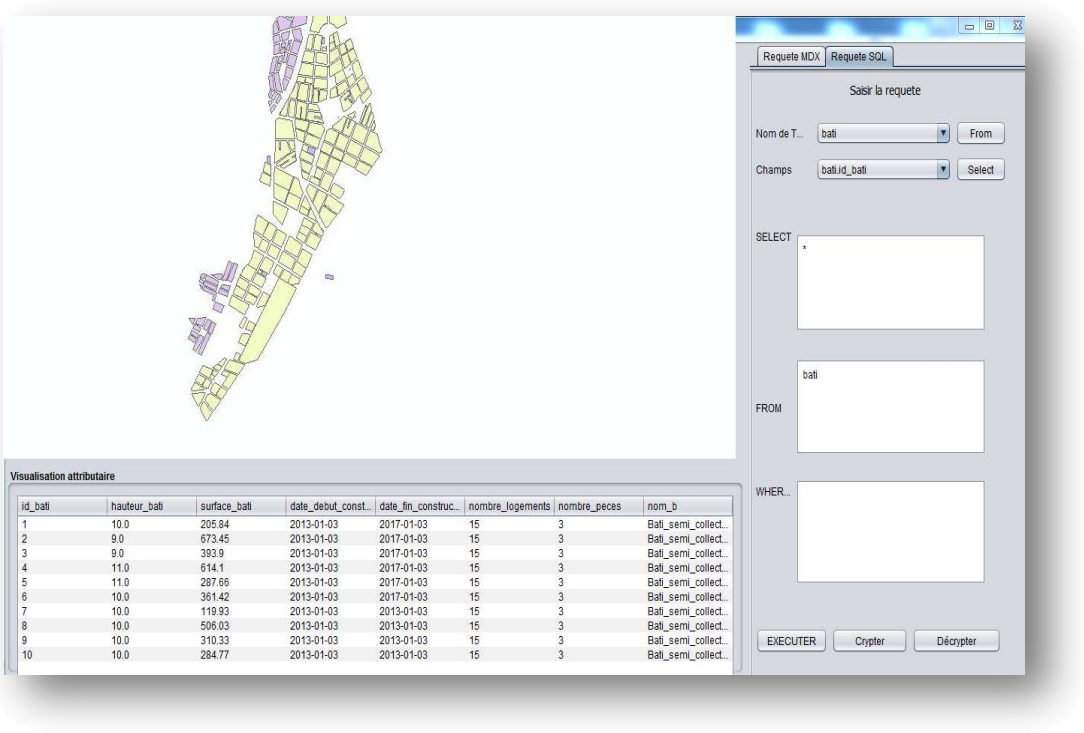


Figure III.17 : Déchiffrement des résultats des requêtes.

AES est un algorithme sur car l'utilisation de la S-Box de l'opération SubBytes (subtitution des bites) constitue une réelle difficulté pour les attaques. L'opération Mix Colomn (mélange des colonnes) combinée avec Shift Rows (décalage de rangées) fait que, après des nombreuses itérations, tous les bytes de sortie dépendent de tous les bytes d'entrée et l'utilisation des clés secondaires construites par extension de la clé originale complique les attaques liées à la clé.

IX. Conclusion

Ce chapitre était consacré essentiellement au développement de notre système Interactif d'Aide à la Décision proposé pour la planification urbaine, d'une application java crée sous NetBeans et basée sur le concept SOLAP fondé sur l'intégration de l'outil OLAP réalisé sous SQL server 2012 et l'outil SIG développé sous ArcGis et enfin à l'application de notre algorithme AES 128 bits.

Précisément, dans ce chapitre, Nous avons découvert les capacités de SQL server 2012 en termes de création d'entrepôt de données spatiales, de déploiement de cube mais également une méthode de chiffrement de l'algorithme AES 128 bits en terme d'efficacité de chiffrements des données pour empêcher toute divulgation non autorisées des données liées aux utilisateurs .L'application a atteint son objectif majeur qui n'est autre que l'application de l'AES sur notre cube de données dédié à la planification urbaine. Ainsi nous pouvons conclure que les deux parties SOLAP et l'algorithme AES sont entièrement opérationnelles.

Conclusion générale

L'informatique décisionnelle apporte des solutions nouvelles pour la modélisation, l'interrogation et la visualisation de données dans un objectif d'aide à la décision. Les modèles multidimensionnels sont des modèles qui permettent de structurer les données pour l'analyse décisionnelle en explicitant la notion de dimension.

L'intégration des données spatiales dans les systèmes OLAP est un enjeu majeur. En effet, l'information géographique est très fréquemment présente implicitement ou explicitement dans les données, mais généralement sous-employée dans le processus décisionnel. Le couplage de systèmes OLAP et de Systèmes d'Informations Géographiques au sein du système OLAP Spatial (SOLAP) est une voie prometteuse.

Nous pensons que la combinaison de la technologie SOLAP une fois conçue et mise en œuvre avec l'application de l'algorithme AES 128 bits devient très intéressante car elle peut déboucher sur une analyse des données plus riches et plus sécurisées.
L'avantage du SOLAP est de fournir une analyse en ligne, une visualisation simple et rapide des données, une vision multidimensionnelle des données et une analyse spatio-temporelle sur une carte géographique. L'AES quant à elle, permet de sécuriser des données pour garantir leur confidentialité.

Cette combinaison ne peut être qu'au bénéfice de l'utilisateur final dans la mesure où ces deux branches sont complémentaires et concourent toutes au même but. L'idée est de voir dans quelle mesure on pourrait adapter les solutions existantes au couple AES/SOLAP. L'avantage que peut offrir un tel couplage est l'optimisation du temps consacré au chiffrement symétrique AES en permettant de se focaliser sur un sous ensemble intéressant de donnée sécurisées.
Il est évident que l'implémentation d'un tel couplage ne sera pas sans difficultés et devra être effectuée sous le respect de certaines contraintes. En effet, contrairement au SOLAP, l'AES étant un système de chiffrement à clé secrète, il existe toujours le risque de voir la clé récupérée par une personne quand elle est transmise d'un correspondant à l'autre. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les données cryptées ou authentifiées avec cette clé.

De la norme de cryptage de données, la distribution des clés reste le problème majeur du cryptage symétrique. (Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ?) . Les moyens à déployer pour garantir la distribution sécurisée des clés correspondants sont très onéreux, ce qui constitue un inconvénient supplémentaire de l'AES.
Nous espérons que ce modeste travail profitera largement à notre université ainsi qu'aux futurs étudiants et ouvrira des perspectives sur des applications regroupant d'autres services.
Nous pensons, qu'il serait intéressant d'implémenter un autre algorithme de chiffrement (RSA ou MD5).

Bibliographies

[1]: W. H. Inmon ; « Building the Data Warehouse Third Edition» ; Wiley Computer Publishing 2002. (consulté le 25.02.2015).

[2]: B. Inmon; What is a Data Warehouse; Article; http://www.billinmon.com; 2000. (consulté le 02.01.20014)

[3]: R. Kimball et M. Ross ; « Entrepôts de Données : Guide Pratique de Modélisation Dimensionnelle 2ème édition » ; Vuibert 2002. (consulté le 05.06.2009)

[4]: Chuck Ballard, Dirk Herreman, Don Schau, Rhonda Bell, Eunsaeng Kim, Ann Valencic; Data Modeling Techniques for Data Warehousing; International Technical Support Organization; http://www.redbooks.ibm.com; février 1998. (consulté le 10.08.2010)

[5] : Yazid. Grim et Fleur Anne Blain. Tutoriel "Conception d'un entrepôt de données(DataWarehouse)".http://grim.developpez.com/cours/businessintelligence/concepts/conceptiondatawarehouse/. (consulté le 03.6.2005)

[6] : Zemri Farah Amina.Vers un Système Interactif d'Aide à la Décision pour la Surveillance Epidémiologique : Couplage SOLAP et Datawarhouse. Thèse de magister en informatique soutenue le 09/10/2011.Université d'Oran. Algérie. (consulté le 03.03.2015)

[7] : R. Kimball ; « Entrepôts de données : Guide pratique du concepteur de Data Warehouse »; Wiley Computer Publishing 1996. (consulté le 19.12.2007)

[8] : BÉDARD Yvan. Spatial OLAP. 2ème Forum annuel sur la R-D, Géomatique VI: Un monde accessible, 13-14 Novembre,1997, Montréal. (Consulté le 25.06.2013)

[9] : BÉDARD Yvan, PROULX Marie-Josée et RIVEST Sonia. Enrichissement de l'OLAP pour l'analyse géographique: exemples de réalisation et différentes possibilités technologiques. Revue des Nouvelles Technologies de l'Information - Entrepôts de données et l'Analyse en ligne, 2005, 1-20 p. (consulté le 16.10.2003)

[10]: STEFANOVIC Nebojsa, HAN Jiawei et KOPERSKI Krzysztof. Object-Based Selective Materialization for Efficient Implementation of Spatial Data Cubes. IEEE Transactions on Knowledge and Data Engineering, 2000, Vol. 12, n° 6, 938-958 p. (consulté le 23.02.2015)

[11]: TOBLER W. R., "Cellular geography", In Gale S. Olsson G. (eds) Phylosophy in Geography, Dortrecht, Reidel, p.379-86, 1979. (Consulté le 24.06.2014)

[12]: EGENHOFER M.J. and SHARMA J., "Topological Relations Between Regions in R2 and Z2", Advance in Spatial Databases, 5th International Symposium, SSD'93 p. 316-331.Singapore, June 1993, Springer-Verlag. (consulté le 12.12.2013)

[13]: KOUBA Zdenek, MATOUSEK Kamil et MIKSOVSKÝ Petr. On Data Warehouse andGIS Integration. In : IBRAHIM Mohamed T., KÜNG Josef et REVELL Norman. 11thInternational Conference on Database and Expert Systems Applications, 04-08 Septembre,2000, Londres, UK. Londres, UK : Springer, 2000 (Lecture Notes in Computer Science 1873)604-613 p. (consulté le 08.11.2012)

[14]: RIVEST Sonia, BÉDARD Yvan, PROULX Marie-Josée, NADEAUM Martin,HUBERT Frederic et PASTOR Julien. SOLAP: Merging Business Intelligence with Geospatial Technology for Interactive Spatio-Temporal Exploration and Analysis of Data.

Elsevier : Journal of International Society for Photogrammetry and Remote Sensing, 2005, Vol. 60, n° 1, 17-33 p. (consulté le 07.10.2007)

[15] : RIVEST Sonia. Investigation des modes d'intégration physique entre un serveur de base de données multidimensionnelle et un SIG. Rapport de DEA Informatique, Laval : Université Laval, Canada, 2000, 84 p. (consulté le 12.11.2003)

[16]: HERNANDEZ Vera, VOSS Angi, GÖHRING Wolf et HOPMANN Cornelio. Sustainable decision support by the use of multi-level and multi-criteria spatial analysis on the Nicaragua Development Gateway. In : From pharaohs to geoinformatics Proceedings of FIG Working Week 2005 and 8th International Conference on the Global Spatial Data Infrastructure, 16-21 Avril 2005, Le Caire, Egypte. (consulté le 14.03.2002)

[17]: (Stolte et al., 2003) STOLTE Chris, TANG Diane et HANRAHAN Pat. Multiscale visualization using data cubes. IEEE Transaction on Visualization and Computer Graphics, 2003, Vol. 9, n° 2, 176–187 p. (consulté le 17.03.20014)

[18]: MALINOWSKI Elzbieta et ZIMÁNYI Esteban. Spatial Hierarchies and Topological Relationships in SpatialMultiDimER model. In : JACKSON Mike, NELSON David et STIRK Sue. 22nd British National Conference on Databases, 5-7 Juillet 2005, Sunderland, UK. Berlin Heidelberg : Springer, 2005, 17-28 p. (Lecture Notes in Computer Science 3567). (consulté le 29.03.2014)

[19]: RIVEST Sonia, BÉDARD Yvan et MARCHAND Pierre. Towards better support for spatial decision-making: defining the characteristics of Spatial On-Line Analytical Processing, Geomatica, Journal of the Canadian Institute of Geomatics, 2001, Vol. 55, n° 4, 539-555 p. (Rivest et al. 2003) RIVEST. (consulté le 23.06.2002)

[20] : MALINOWSKI Elzbieta et ZIMÁNYI Esteban. Representing spatiality in a conceptual multidimensional model. In : PFOSER Dieter, CRUZ Isabel F. et RONTHALER Marc. 12th ACM International Workshop on Geographic Information Systems, 12-13 Novembre, 2004,

Washington, DC, USA. New York, USA : ACM Press, 2004, 12-22 p. (consulté le 14.13.2013)

[21]: SAMPAIO Marcus Costa, SOUSA Andre Gomes et BAPTISTA Cláudio. Towards a logical multidimensional model for spatial data warehousing and OLAP. In : SONG Il-Yeol et VASSILIADIS Panos. 9th ACM International Workshop on Data Warehousing and OLAP, 10 Novembre, 2006, Arlington, Virginia, USA. New York, USA : ACM Press, 2006, 83-90 p. (consulté le 03.05.2005)

[22]: FIDALGO Robson N., TIMES Valeria C., SILVA Joel et SOUZA Fernando F. GeoDWFrame: A Framework for Guiding the Design of Geographical Dimensional Schemas. In : KAMBAYASHI Yahiko, MOHANIA Mukesh K. et WÖß Wolfram. 6th International Conference on Data Warehousing and Knowledge Discovery, 1-3 Septembre, 2004, Saragosse, Espagne. Berlin Heidelberg : Springer, 2004, 26-37 p. (Lecture Notes in Computer Science 3181). (consulté le 03.08.2010)

[23]: MARCHAND Pierre, BRISEBOIS Alexandre, BÉDARD, Yvan et EDWARDS Geoffrey. Implementation and evaluation of a hypercube-based method for spatio-temporal exploration and analysis. Elsevier : Journal of the International Society of Photogrammetry and Remote Sensing, 2003, Vol. 59, n° 1, 6-20 p. (consulté le 10.09.2005)

[24] : L'Intelligence des risques, Sécurité, Sûreté, Environnement, Management IFIE 2006. Bernard Besson et Jean-Claude Possin. (consulté le 16.06.2014)

[25]: Information Technologie Security Evaluation Criteria, European Comunities, juin 1991. (consulté le 28.07.2013)

[26]: S. Black, V. Varadharajan. "A Multilevel Security Model for a Distributed Object Oriented System Networks and Communications". HP Laboratories Bristol HPL, 90-74.1990. (consulté le 03.12.2009)

[27]: National Computer Security Center, A guide to Understanding discretionary Access Control in Trusted systems, 1987. (consulté le 16.01.2010)

[28]: Dastjerdi, A., Pieprzyk, j., "Security In Databases : A survey Study",1996, http://citeseer.ist.psu.edu/baraani-dastjerdi96security.html. (consulté le 19.03.2010)

[29]: B. Lampson. "Protection" 5th Princeton Symposium on Information Sciences and Systems. 1971. (consulté le 26.03.2014)

[30] : Jacques Le Maitre, « Sécurité des bases de données », Université du Sud Toulon-Var. (consulté le 27.03.2010)

[31]: S. Black, V. Varadharajan. "A Multilevel Security Model for a Distributed ObjectOriented System Networks and Communications". HP Laboratories Bristol HPL, 90-74.1990. (consulté le 09.08.2007)

[32]: D. E. Denning, A lattice model of secure information flow, Communications of the ACM, 19(5): 236-243, May 1976. (consulté le 24.01.2015)

[33]: Pierangela Samarati and Sabrina de Capitani diVimercati, Access Control: Policies, Models, and Mechanisms, FOSAD 2000, LNCS 2171, pages 137-196, 2001. (consulté le (consulté le 26.03.2014)

[34]: D. E. Bell and L. J. Lapadula, Secure computer systems: Mathematical foundations, Technical Report ESD-TR-73-278, vol. 1, The Mitre Corp., Bedford, MA, 1973. (consulté le (consulté le 06.06.209)

[35]: M. Harrison, W. Ruzzo, J. Ullman. "Protection in operating systems". Communications of the ACM. 461–471. 1976. (consulté le 19.05.2003)

[36]: National Computer Security Center. Trusted network interpretation of the trusted computer system evaluation criteria. July 1987. (consulté le 26.02.2015)

[37]: J. Mclean, The specification and modeling of computer security, Computer, 23(1): 916, January 1990. (consulté le 14.03.2015)

[38] : Stéphan Hadinger, Le contrôle d'accès au SI, projet IS@ France Télécom, www.rd.francetelecom.fr/ fr/conseil/mento20/chapitre7.pdf. (consulté le 26.09.2012)

[39]: "The Chinese Wall Security Policy", IEEESymposium on Security and Privacy, Oakland, Californie, 1-3 mai 1989, IEEE Computer Society Press, pp. 206-214. (consulté le 22.07.2015)

[40] : Ferraiolo, D. F. et Kuhn, D. R. (1992). Role-based access controls. In 15th National Computer Security Conference, pages 554–563, Baltimore, MD, USA. (consulté le 30.01.2014)

[41] : STINSON D. « Cryptographie - Théorie et pratique, Thompson Publishing, 1996 ». (consulté le 13.06.2009)

[42]: DIFFIE W., HELLMAN M.E., « New directions in cryptography ». IEEE Transactions on Information Theory, vol. 26, n°6, p. 644-654, 1976. (consulté le 15.24.2005)

[43] : STINSON D., Cryptographie - Théorie et pratique, Thompson Publishing, 1996. (consulté le 24 .04.2005)

[44]: FIPS-197, Announcing the Advanced Encryption Standard (AES). 104. Samarati. P, Jajodia. S, "data security". Research and practice. I S 20(7): 537-556(95). (consulté le 03.09 .2008)

[45]: Ghyslaine PHILIE, Jean- philippe LEMAY, Isabelle ST JEAN, Cindy GEE, Nicolas PASTOR ; Le système d'information d'aide à la décision (SIAD) Le 17 avril 2007.

[46]: Olivier Teste. Modélisation et manipulation d'entrepôt de données complexes et historisés. Thèse de doctorat en informatique soutenue le 18/12/2000.Université Paul Sabatier de Toulouse. France.

[47]: Yazid. Grim et Fleur Anne Blain. Tutoriel "Conception d'un entrepôt de données(DataWarehouse)".http://grim.developpez.com/cours/businessintelligence/concepts/conceptiondatawarehouse/ (consulté le 25.03.2015)

Webographies

[web.1]: http://www.kheopstech.com/fr/jmap/solap.jsp(consulté le 1.09.2007).

[web.2]: https://www.lri.fr/~herschel/courses_ws1314/resources/04_requetes.pdf.(consulté le 02.06.2014

[web.3]: http://eric.univ-lyon2.fr/~kaouiche/inf9002/mdx.html .(consulté le17.06.2009)

[web.4]: http://www.cartographie.ird.fr/publi/documents/sig1.pdf (consulté le 26.03.2014)

[web.5]: http://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es_spatiales. (consulté le 06.03.2015)

[web.6]:https://www.academia.edu/5138784/cours_SIG_syst3A8me_dinformation (consulté le 29.02.2010)

[web.7]: http://fr.wikipedia.org/wiki/Confidentialit%C3%A9. (consulté le 30.03.2014)

[web.8]: http//www.securiteinfo.com. (consulté le 02.10.2005)

[web.9]: http://www.commentcamarche.net. (consulté le 26.05.2005)

[web.10]: http://www.alcyonix.com. (consulté le 16.12.2014)

[web.11]: http://www.journaldunet.com. (consulté le 26.03.2014)

[web.12]: http://www.securite-informatique.gouv.fr. (consulté le 31.12.2010)

[web.13]: https://www.microsoft.com/fr-fr/download/details.aspx?id=29062 (consulté le 26.03.2006)

[web.14]: http://www.esri.com/news/arcnews/spring12articles/introducing-arcgis-101.html (consulté le 26.09.2014)

[web.15]: http://netbeans.developpez.com/cours/ (consulté le 26.03.2007)

Liste des figures et des tableaux