

Application pour la gestion des comptes bancaires

5.1 Introduction

Après avoir présenté notre cryptosystème qui a donné de bons résultats en termes de temps d'exécution et de niveau de sécurité. Pour bien éclaircir l'efficacité de cryptosystème ; on va l'intégrer dans une application client / Serveur de gestion des comptes bancaires. Ce dernier, nous permet un échange sécurisé des données.

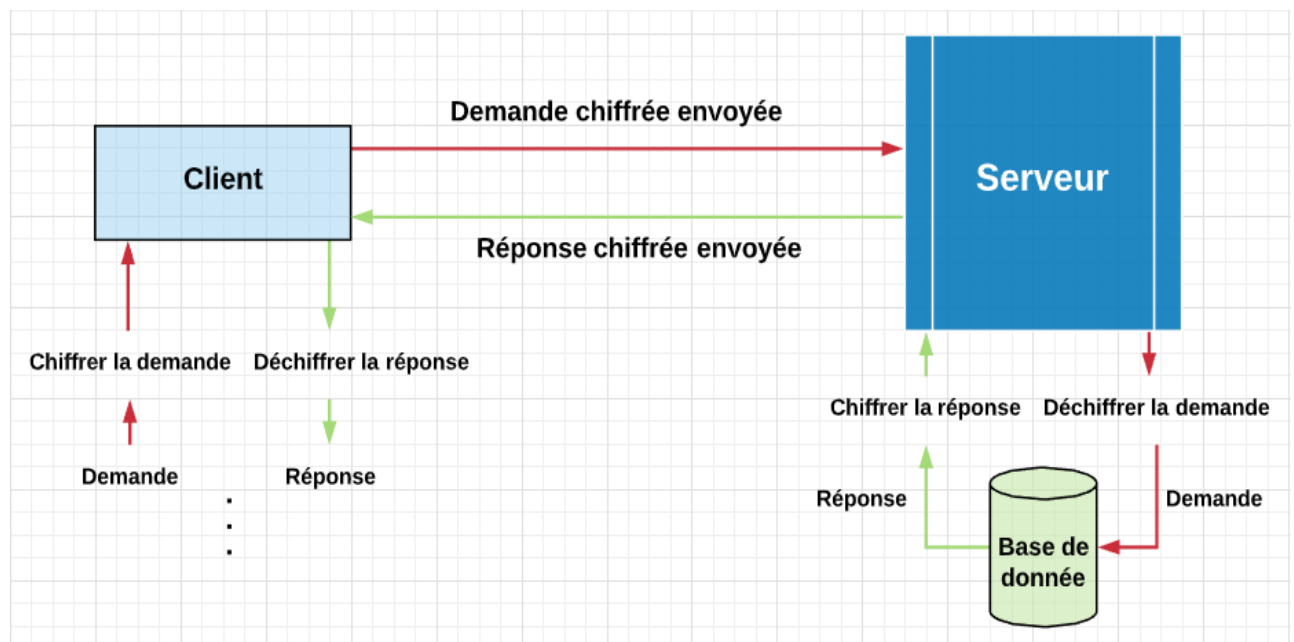


Figure 5.1 : Schéma intégration du cryptosystème dans une application client serveur.

5.2 Analyse et conception

5.2.1 Présentation UML

UML est un langage de modélisation graphique conçu pour fournir une méthode normalisée pour visualiser la conception d'un système. C'est un support de communication performant qui permet grâce à sa représentation graphique, de concevoir des solutions, de faciliter la comparaison et de les évoluer. Il est couramment utilisé en développement logiciel et en conception orientée objet.

5.2.2 Diagramme de cas d'utilisation

Il est utilisé pour donner une vision globale du comportement fonctionnel d'un système logiciel. Un cas d'utilisation représente une unité discrète d'interaction entre un utilisateur et un système. Il est une unité significative de travail. Dans un diagramme de cas d'utilisation, les utilisateurs sont appelés acteurs, ils interagissent avec les cas d'utilisation.

Un acteur participe au moins à un cas d'utilisation qui peut être un utilisateur humain ou un autre système. Ce dernier interagit directement avec le système étudié.

Dans notre application de gestion des comptes bancaires, nous avons trois acteurs qui sont :

1. Client : D'abord, le client fait un échange de clé cryptographique avec le serveur ensuite il accède au système via un contrôle d'accès (login et mot de passe). Puis il peut effectuer l'une ou plusieurs parmi les opérations suivantes :

- Consulter solde.
- Transfer d'argent.
- Changer mot de passe.
- Afficher la liste des transactions.

2. Employé : Premièrement, il fait un échange de clé cryptographique avec le serveur ensuite il accède au système via un contrôle d'accès (login et mot de passe). Enfin il peut effectuer l'une ou plusieurs parmi les opérations suivantes :

Créer compte client.

- Dépôt (versement) d'argent.
- Retrait d'argent.
- Transfert d'argent.
- Affichage de la liste des comptes.

3. Administrateur : Au premier lieu, il échange la clé cryptographique avec le serveur ensuite il accède au système via un contrôle d'accès (login et mot de passe). Enfin il peut effectuer l'une ou plusieurs parmi les opérations suivantes :

- Créer compte employé
- Afficher la liste des employés.
- Supprimer compte employer.
- Modifier compte employer.
- Afficher la liste des comptes client.

- Modifier compte client.
- Supprimer compte client.
- Afficher la liste des clients.
- Afficher la liste des transactions.
- Afficher la liste des opérations.

5.2.2.1 Diagramme de cas d'utilisation Client

Le diagramme de cas d'utilisation client représente les interactions du client avec le système comme nous les illustrons dans le diagramme suivant :

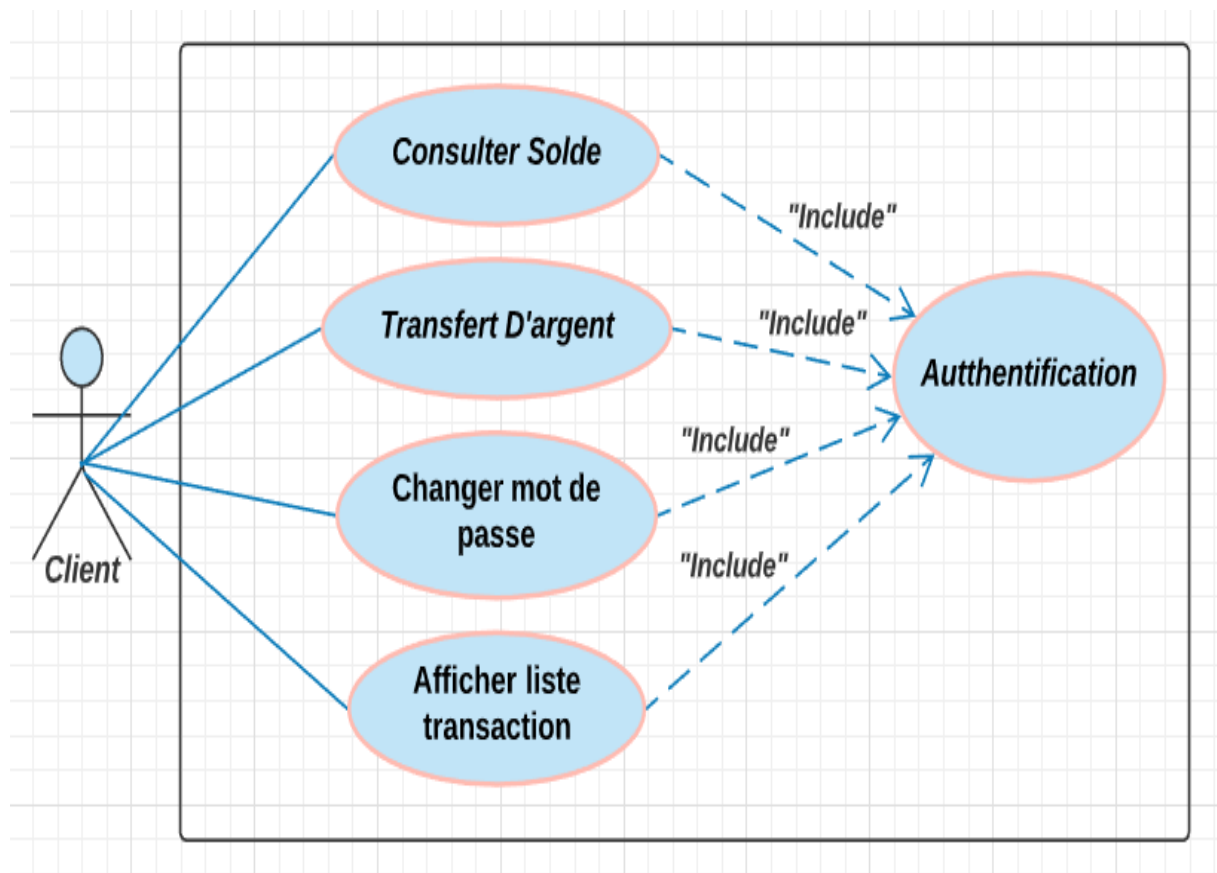


Figure 5.2 : diagramme de cas d'utilisation client.

5.2.2.2 Diagramme de cas d'utilisation employé

Le diagramme de cas d'utilisation employé représente les interactions d'employé avec le système comme nous les illustrons dans le diagramme suivant :

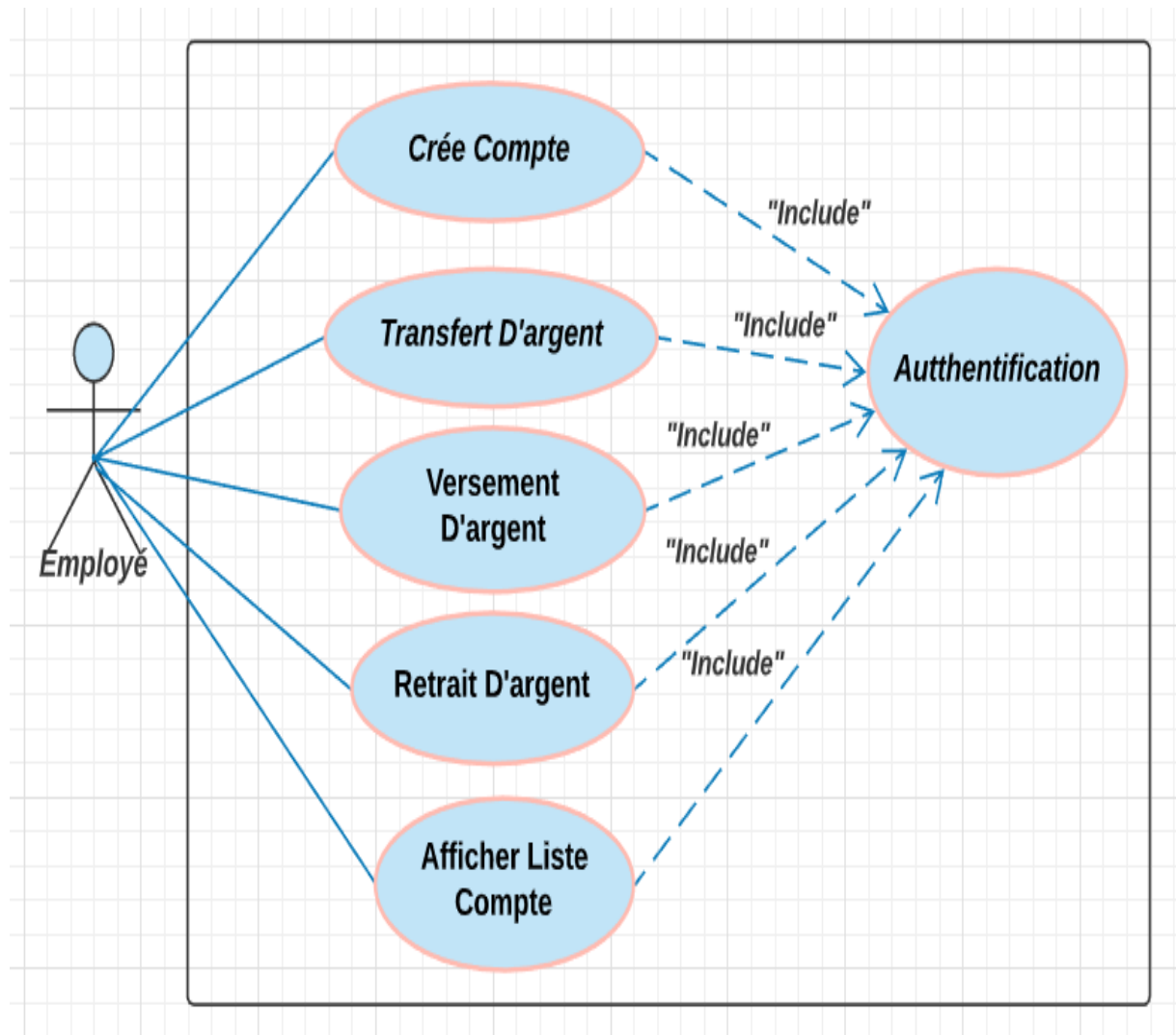


Figure 5.3 : diagramme de cas d'utilisation employé.

5.2.2.3 Diagramme de cas d'utilisation Administrateur

Le diagramme de cas d'utilisation Administrateur représente les interactions d'administrateur avec le système comme nous les illustrons dans le diagramme suivant :

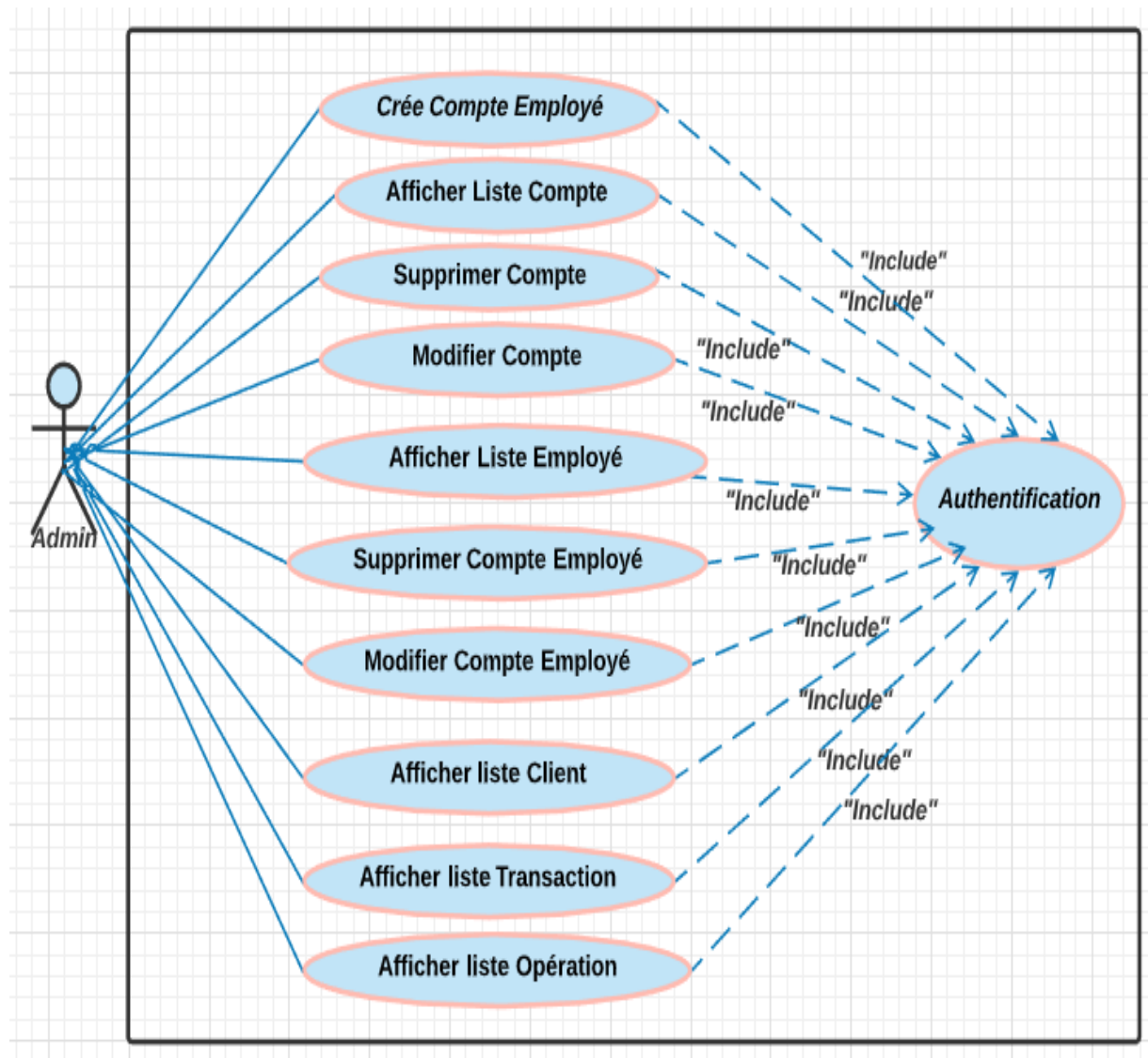


Figure 5.4 : diagramme de cas d'utilisation Administrateur.

5.2.2 Diagramme de classe

Ce diagramme permet de donner la représentation statique du système à développer. Cette représentation est centrée sur les concepts de classe et d'association. Chaque classe se décrit par les attributs et les opérations.

Un diagramme de classe se définit comme un ensemble de classes contenant des attributs et des opérations, reliées les unes aux autres par des relations et ceci ayant des conditions de participation (cardinalités).

Une classe décrit un groupe d'objets ayant les mêmes propriétés (attributs), un même comportement (opérations) et une sémantique commune. Un attribut est une propriété élémentaire d'une classe qui prend une valeur. Une opération est une fonction applicable aux objets d'une classe. Elle est également appelée méthode.

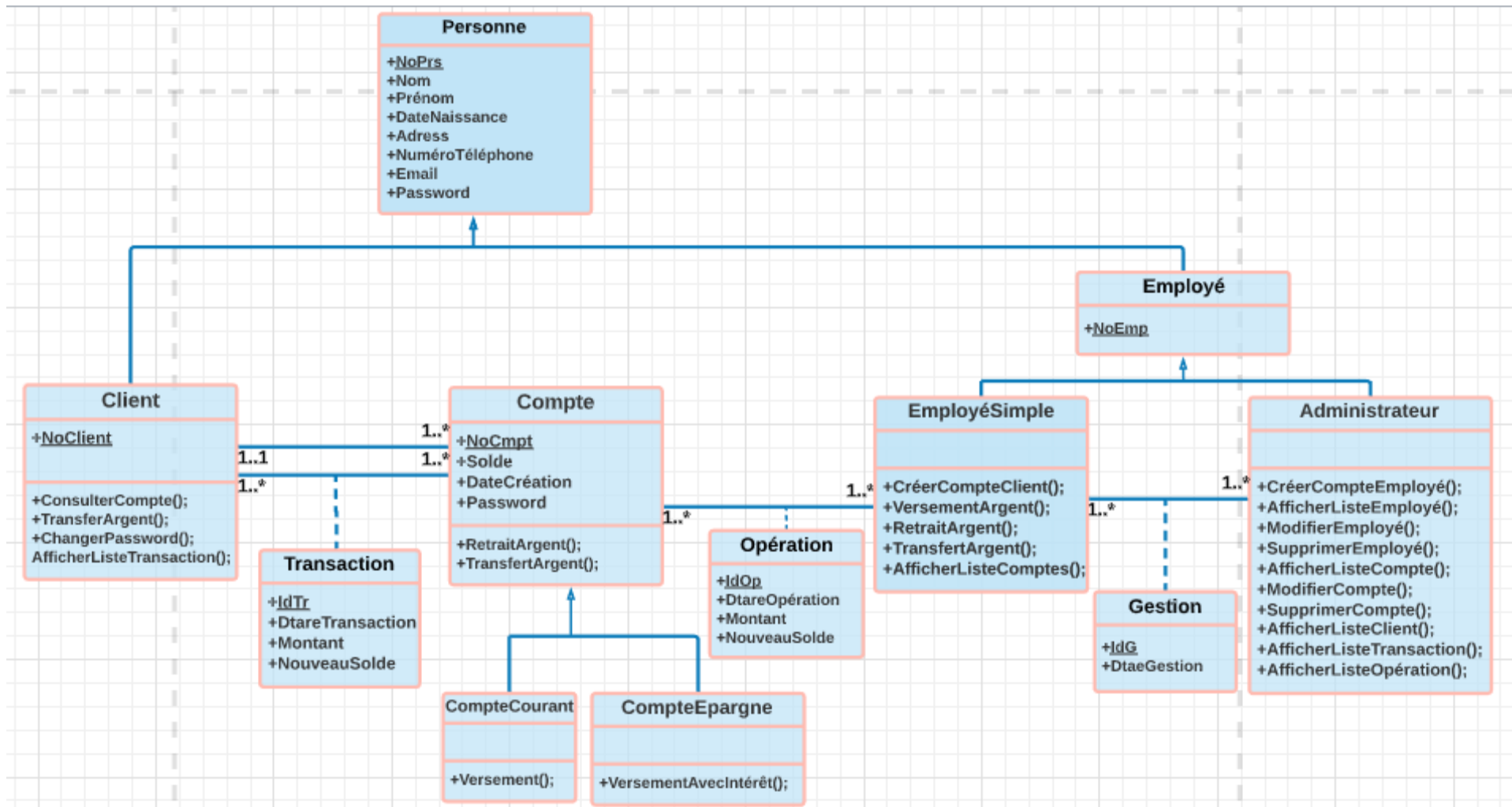


Figure 5.5: diagramme de classe.

5.3 Implémentation

5.3.1 Environnement et outils de développement

Avant de commencer la présentation de notre application, nous allons tout d'abord, citer les outils utilisés lors du développement.

Langage java

C'est un langage de programmation orienté objet, développé par Sun Microsystems. Il possède de nombreuses caractéristiques. Ce langage permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris). Java est également portable, rapide, sécurisé et fiable. [42]

JDK (JAVA Development Kit)

L'environnement dans lequel le code JAVA est compilé pour être transformé en bytecode (code intermédiaire) afin que la machine virtuelle de JAVA (JAVA Virtual Machine) puisse l'interpréter. [43]

Netbeans IDE

NetBeans est un environnement de développement intégré (EDI). Placé en « open source » par Sun en juin 2000 sous licence CDDL et GPLv2 (Common development and Distribution License). En plus de Java, il permet également de supporter différents autres langages, comme Python, C, C++, JavaScript, XML, Ruby, PHP et HTML.

Il contient toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, éditeur graphique d'interfaces et de pages Web). NetBeans constitue par ailleurs une plateforme qui permet le développement d'applications spécifiques « bibliothèque Swing ». [44]

SQLiteManager

Pour créer la base de données, nous avons utilisé SQLite Manager.

SQLite Manager est un système de gestion de base de données SQLite. Il associe une interface conviviale à une vitesse fulgurante et des fonctionnalités avancées.

SQLite Manager permet de travailler avec une large gamme de bases de données.

SQLite 3 : bases de données standard, bases de données en mémoire, bases de données cryptées AES 128/256 / RC4, base de données cryptée SQLCipher et également avec le serveur cubeSQL. [45]

Le modèle client/serveur**Sockets TCP**

Le protocole TCP offre un service en mode connecté et fiable. Les données sont délivrées dans l'ordre de leur émission.

La procédure d'établissement de connexion est dissymétrique. Le serveur, attend des demandes de connexion que le client lui envoie.

Une fois l'étape d'établissement de connexion effectuée, le fonctionnement redevient symétrique.

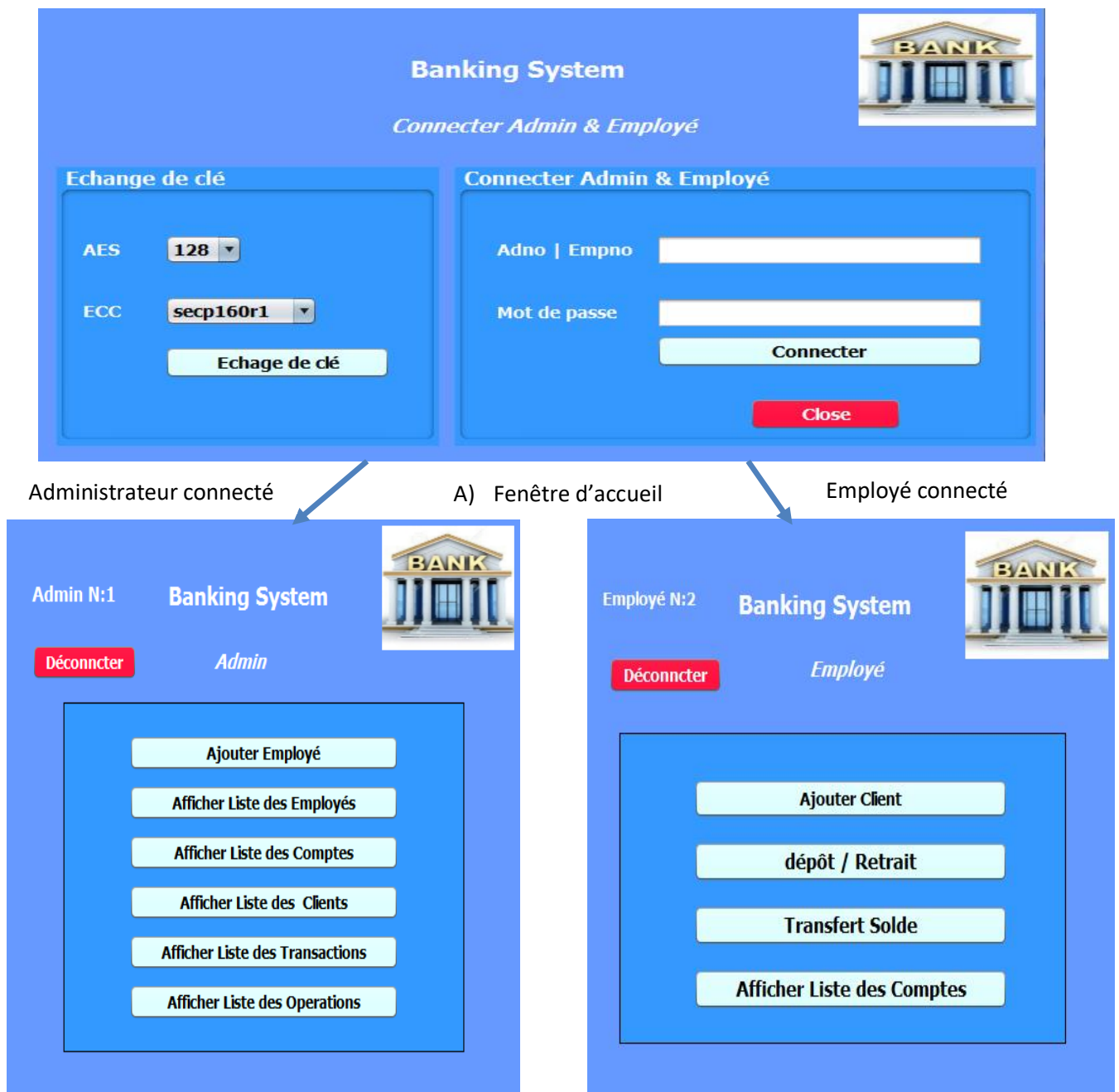
Il est à noter que côté serveur on utilise deux sockets : l'un, appelé socket d'écoute, reçoit les demandes de connexion et l'autre, appelé socket de service, sert pour la communication. En effet, un serveur peut être connecté simultanément avec plusieurs clients.

5.4 Présentation des interfaces de l'application

Dans cette section, nous présentons les interfaces de notre application que nous avons réalisée.

5.4.1 Fenêtre d'accueil administrateur et employé

Cette page permet aux employés et administrateurs d'échanger la clé et de connecter. Si un employé connecte la fenêtre employé s'ouvre. Si un Administrateur connecte la fenêtre Administrateur s'ouvre.



B) Fenêtre d'administrateur C) Fenêtre d'employé
Figure 5.6: ouverture de fenêtre d'administrateur ou d'employé à partir de la fenêtre d'accueil.

5.4.2 La fenêtre Administrateur

Elle assure l'accès aux interfaces suivantes: Ajouter employé, Afficher liste des employés, Afficher liste des comptes, Afficher liste des clients, Afficher liste des transactions, Afficher liste des opérations.

5.4.2.1 La fenêtre Ajouter employé

A partir de cette page l'administrateur peut ajouter un employé comme l'indique la figure ci-dessous :

Admin N: 1 **Banking System** 

Ajouter Employé

Empno: 23

Nom: Lebsir

prénom: Nacer

Date Naissance: 02 / 02 / 1998

Adress: EIMilia

Numéro telephone: 0665022487

Email: leb.nacer10@gmail.com

Grade: Admin


Mot de passe: *****

Ajouter Employé

Reset

Close

Message

 New account Emplie created
Empno = 23
Nom = Lebsir
Prénom= Nacer
Date naissance = 02-02-1998
Adress= EIMilia
numéro téléphone = 0665022487
Email = leb.nacer10@gmail.com
Grad = Admin

OK

Figure 5.7 : Fenêtre Ajouter employé.

5.4.2.2 La fenêtre Afficher liste employés

Cette page sert à afficher la liste des employés et nous permet de chercher un employé par : Empno, Nom, Prénom, Date de naissance, Adresse, Numéro téléphone, Email et Grade. Comme elle nous permet de modifier les informations d'un employé et de supprimer un autre.

System Banking

Admin N: 1

Liste des Employés

Information Employé

Serch By: All

Empno	Nom	Prénom	Date Naissance	Adress	Numéro Téléphone	Email	Grad
1	Lebsir	Samir	16-08-1991	Oran	0790012004	lebsir0@gmail...	Admin
2	Lebsir	Nassim	11-11-1987	Jijel	0659684523	nassiloucou...	Employee
7	Boukhchem	Djamal	04-04-1992	Oran	0665069529	djamal0@qma...	Admin
12	Keroum	Ahmed	09-12-1997	Jijel	0798120433	ahmed@gmail...	Admin
13	Abdeltif	Hind	17-10-1990	Annaba	0698789632	hind@gmail.com	Admin
17	Lebsir	Adem	12-12-1982	Jijel	0555896321	Adem@gmail...	Employee
18	Nahal	Mohamed	10-07-1998	Blida	0798178456	mohamed@g...	Employee
22	Lebsir	Nacer	02-02-1998	ElMilia	0665022487	leb.nacer10@...	Admin

Figure 5.8 : Fenêtre Afficher liste des employés.

System Banking

Admin N: 1

Liste des Employés

Information Employé

Serch By: Empno

12

Empno	Nom	Prénom	Date Naissance	Adress	Numéro Téléphone	Email	Grad
12	Keroum	Ahmed	09-12-1997	Jijel	0798120433	ahmed@gmail...	Admin

Figure 5.9 : recherche employé par Empno=12.

The screenshot shows the 'System Banking' interface. On the left, there is a form for 'Information Employé' with fields for Empno, Nom, Prénom, Date Naissance, Adress, Numéro Téléphone, Email, and Grade. The 'Grade' dropdown is set to 'Admin'. Below the form are buttons for 'Modifier information', 'Supprimé employé', and 'Close'. On the right, a table titled 'Liste des Employés' displays search results for 'Jijel'. The table has columns for Empno, Nom, Prénom, Date Naissance, Adress, Numéro Téléphone, Email, and Grad. Two employees are listed: one with Empno 2 (Lebsir Nassim) and one with Empno 12 (Keroum Ahmed).

Empno	Nom	Prénom	Date Naissance	Adress	Numéro Téléphone	Email	Grad
2	Lebsir	Nassim	11-11-1987	Jijel	0659684523	nassicoucou...	Employee
12	Keroum	Ahmed	09-12-1997	Jijel	0798120433	ahmed@gmail...	Admin

Figure 5.10 : recherche employé par Adresse = Jijel.

The screenshot shows the 'System Banking' interface with the 'Liste des Employés' table displaying results for 'All'. The 'Adress' column for the first employee (Empno 1) is circled in red. In the left sidebar, the 'Modifier information' button is also circled in red. The 'Grade' dropdown is set to 'Admin'. Below the form are buttons for 'Supprimé employé' and 'Close'.

Empno	Nom	Prénom	Date Naissance	Adress	Numéro Téléphone	Email	Grad
1	Lebsir	Samir	16-08-1991	Alger	0790012004	lebsir0@gmail...	Admin
2	Lebsir	Nassim	11-11-1987	Jijel	0659684523	nassicoucou...	Employee
7	Boukhchem	Djamal	04-04-1992	Oran	0665069529	djamal0@qma...	Admin
12	Keroum	Ahmed	09-12-1997	Jijel	0798120433	ahmed@gmail...	Admin
13	Abdeltif	Hind	17-10-1990	Annaba	0698789632	hind@gmail.com	Admin
17	Lebsir	Adem	12-12-1982	jijel	0555896321	Adem@gmail...	Employee
18	Nahal	Mohamed	10-07-1998	Blida	0798178456	mohamed@g...	Employee
22	Lebsir	Nacer	02-02-1998	ElMilia	0665022487	leb.nacer10@...	Admin

Figure 5.11 : Modification des informations de l'employé.

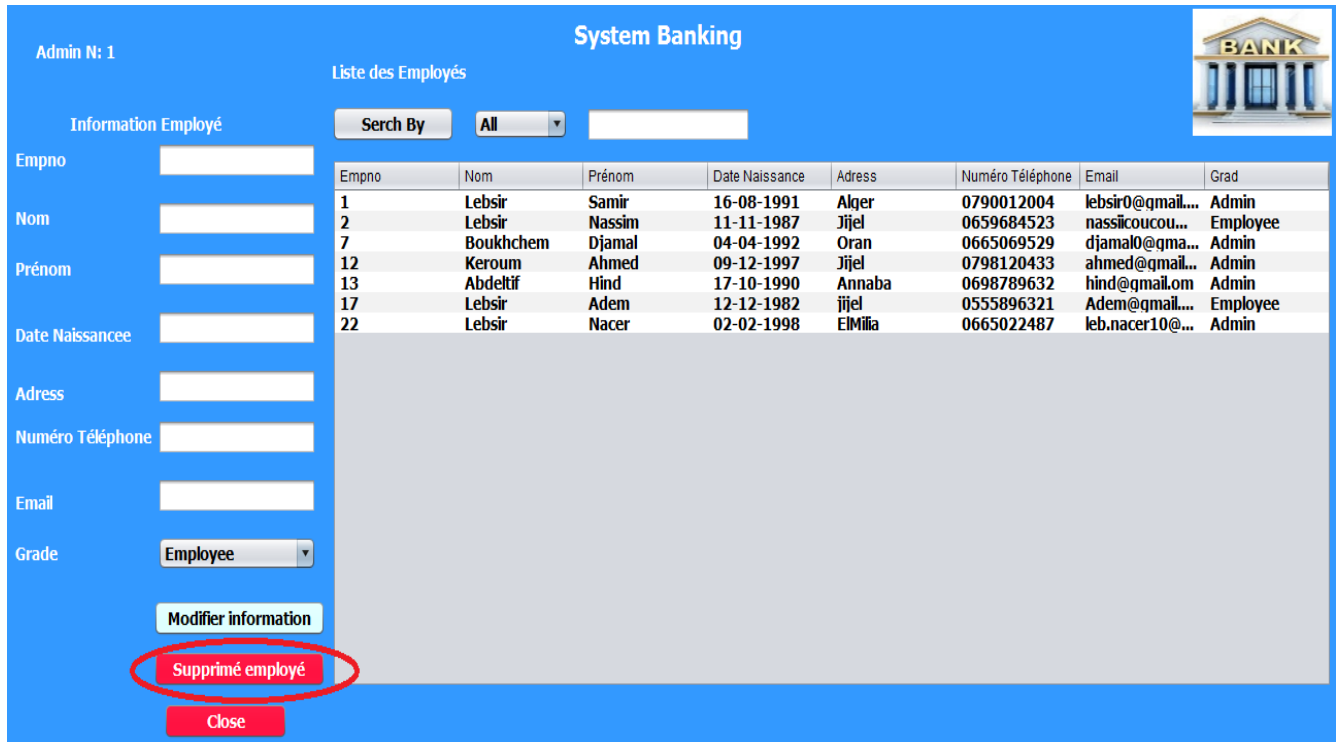


Figure 5.12 : Suppression de l'employé Empno=18.

5.4.2.3 La fenêtre Afficher liste des comptes

Cette page sert à afficher la liste des comptes et nous permet de chercher un compte par : NoCmpt, NoClient, Type et Date de création. Comme elle nous permet de modifier les informations d'un Compte et de supprimer un autre.

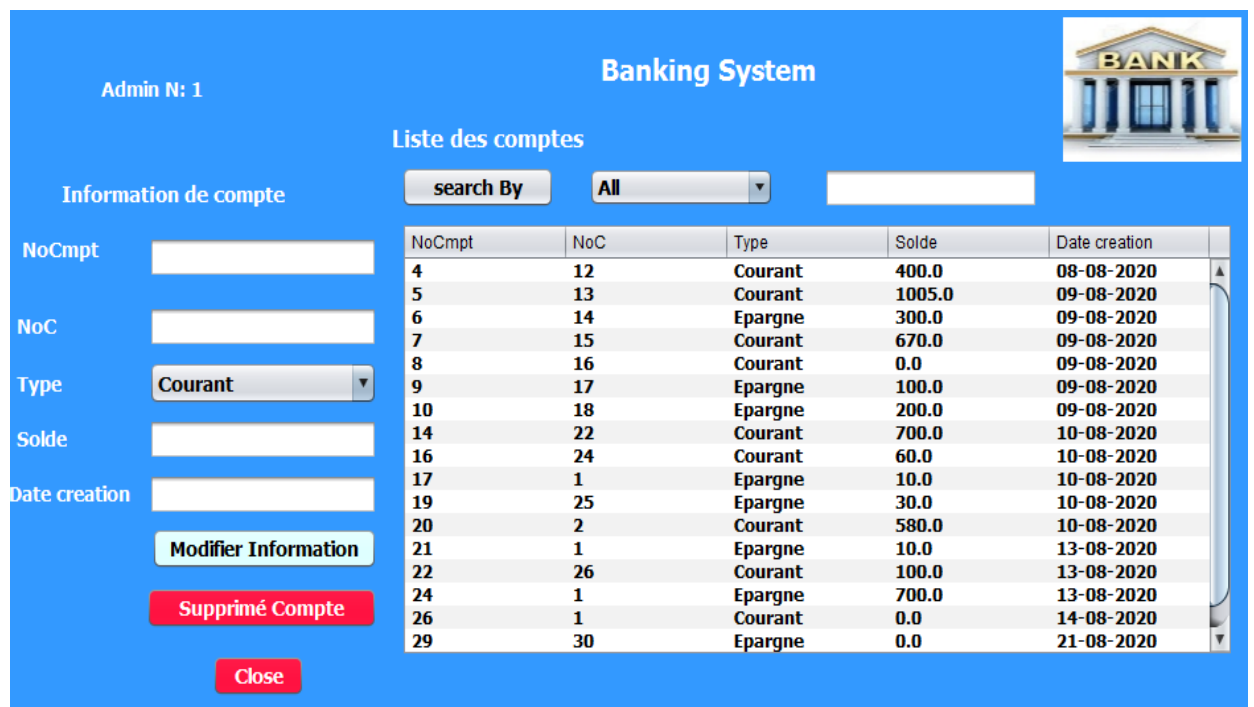


Figure 5.13 : fenêtre Afficher liste des comptes.

5.4.2.4 La fenêtre Afficher liste des clients

Cette page sert à afficher la liste des Clients et nous permet de chercher un client par : NoClient, Nom et Prénom, Date de naissance, Adresse, Numéro de téléphone et Email.

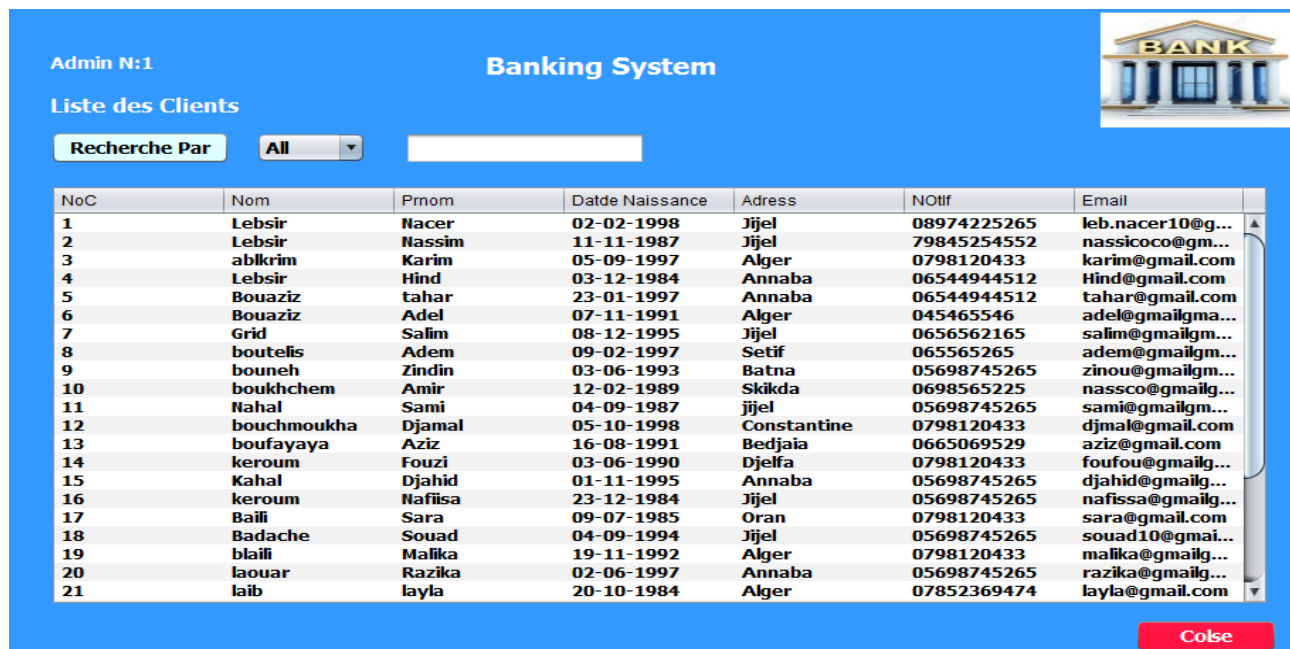


Figure 5.14 : fenêtre Afficher liste des comptes.

5.4.2.5 La fenêtre Afficher liste des transactions

Cette page sert à afficher la liste des transactions et nous permet de chercher une transaction par : Id, NoCmpt, Date, Type et Fait Par.

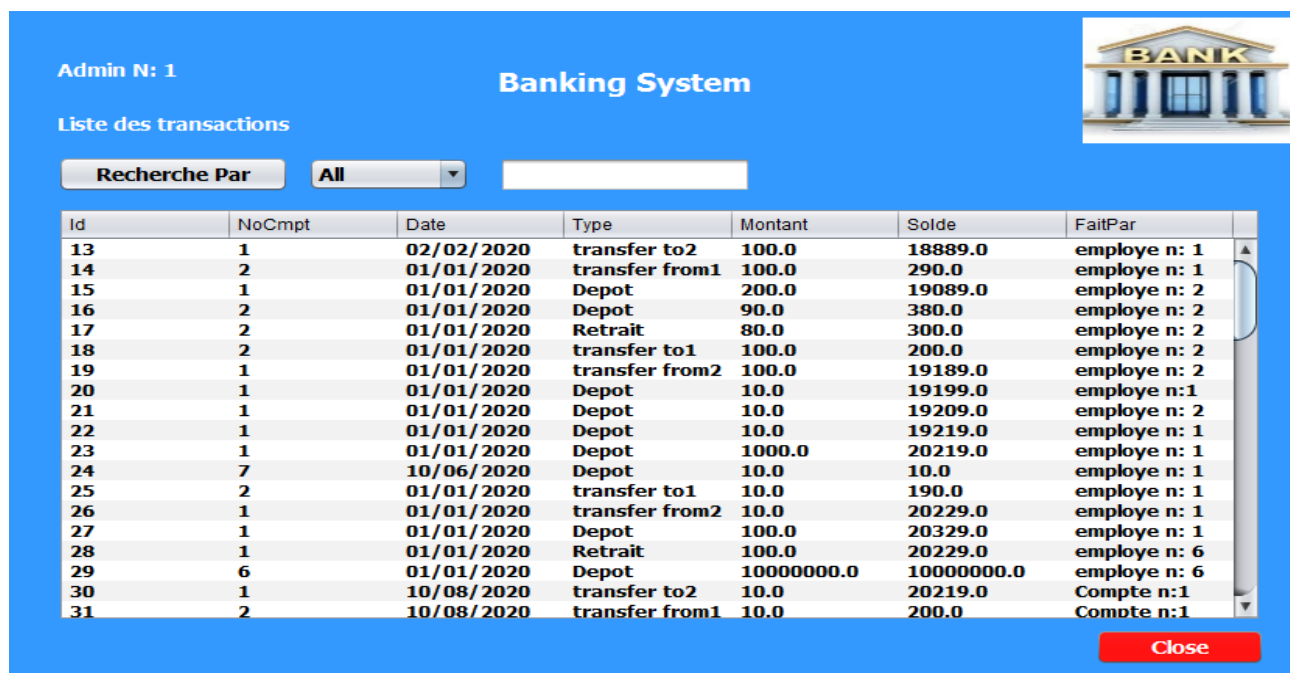
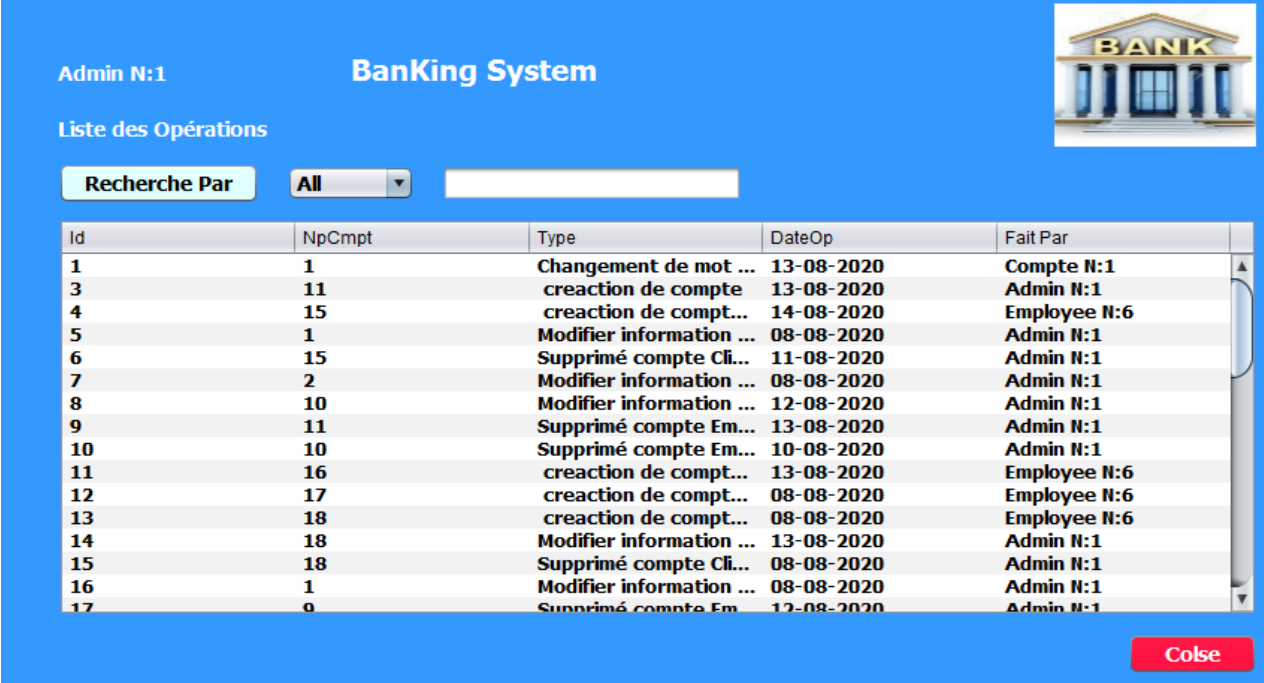


Figure 5.15 : fenêtre Afficher liste des transactions.

5.4.2.6 La fenêtre Afficher liste des Opérations

Cette page sert à afficher la liste des opérations et nous permet de chercher une opération par : Id, NoCmpt, Date, Type et Fait Par.



Admin N:1 **Banking System**

Liste des Opérations

Recherche Par **All**

Id	NpCmpt	Type	DateOp	Fait Par
1	1	Changement de mot ...	13-08-2020	Compte N:1
3	11	creation de compte	13-08-2020	Admin N:1
4	15	creation de compt...	14-08-2020	Employee N:6
5	1	Modifier information ...	08-08-2020	Admin N:1
6	15	Supprimé compte Cli...	11-08-2020	Admin N:1
7	2	Modifier information ...	08-08-2020	Admin N:1
8	10	Modifier information ...	12-08-2020	Admin N:1
9	11	Supprimé compte Em...	13-08-2020	Admin N:1
10	10	Supprimé compte Em...	10-08-2020	Admin N:1
11	16	creation de compt...	13-08-2020	Employee N:6
12	17	creation de compt...	08-08-2020	Employee N:6
13	18	creation de compt...	08-08-2020	Employee N:6
14	18	Modifier information ...	13-08-2020	Admin N:1
15	18	Supprimé compte Cli...	08-08-2020	Admin N:1
16	1	Modifier information ...	08-08-2020	Admin N:1
17	9	Supprimé compte Em...	12-08-2020	Admin N:1

Colse


Figure 5.16 : fenêtre Afficher liste des Opérations.

5.4.3 Fenêtre d'accueil employé

Elle assure l'accès aux interfaces suivantes: Ajouter compte client, versement ou retrait d'argent, transfert de solde et afficher liste des comptes.

5.4.3.1 Fenêtre Créer compte client

Elle assure l'accès aux deux interfaces suivantes: Ajouter nouveau client ou ancien client comme l'indique la figure ci-dessous :



Employee N: 2 **Bankin System**

Créer Compte

Ancien Client Nouveau Client

Colse

Figure 5.17 : fenêtre Créer compte client.

5.4.3.1.1 Fenêtre Ajouter Nouveau client

A partir de cette page l'employé peut ajouter un nouveau compte client :

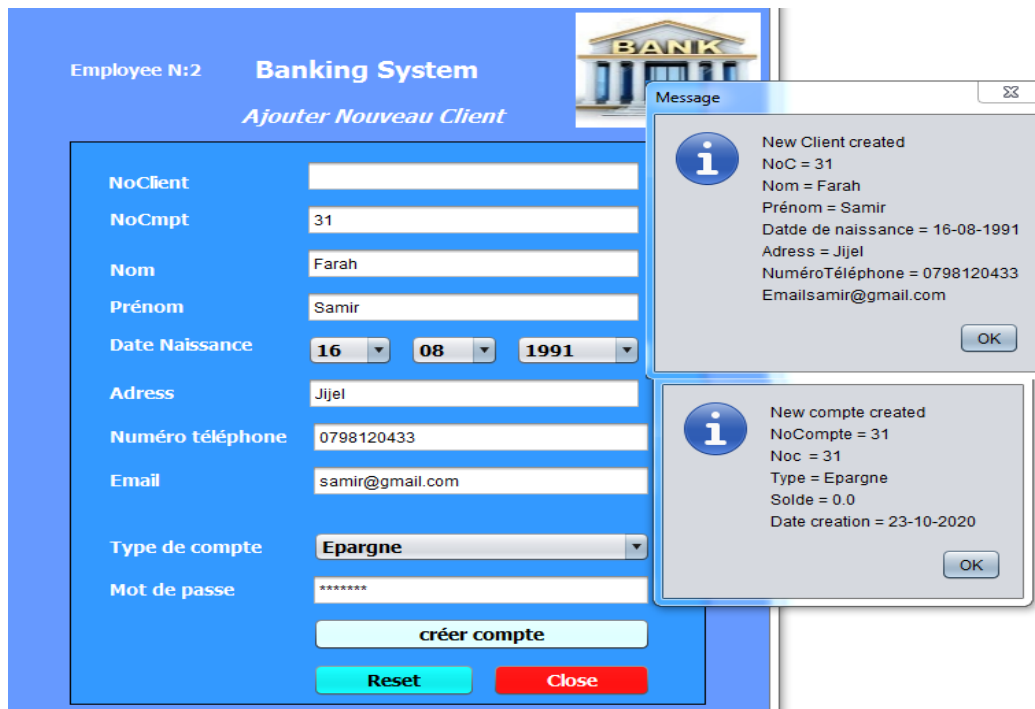


Figure 5.18 : fenêtre Ajouter nouveau client.

5.4.3.1 .2 Fenêtre créer compte ancien client

A partir de cette page l'employé peut créer un compte pour un ancien client :

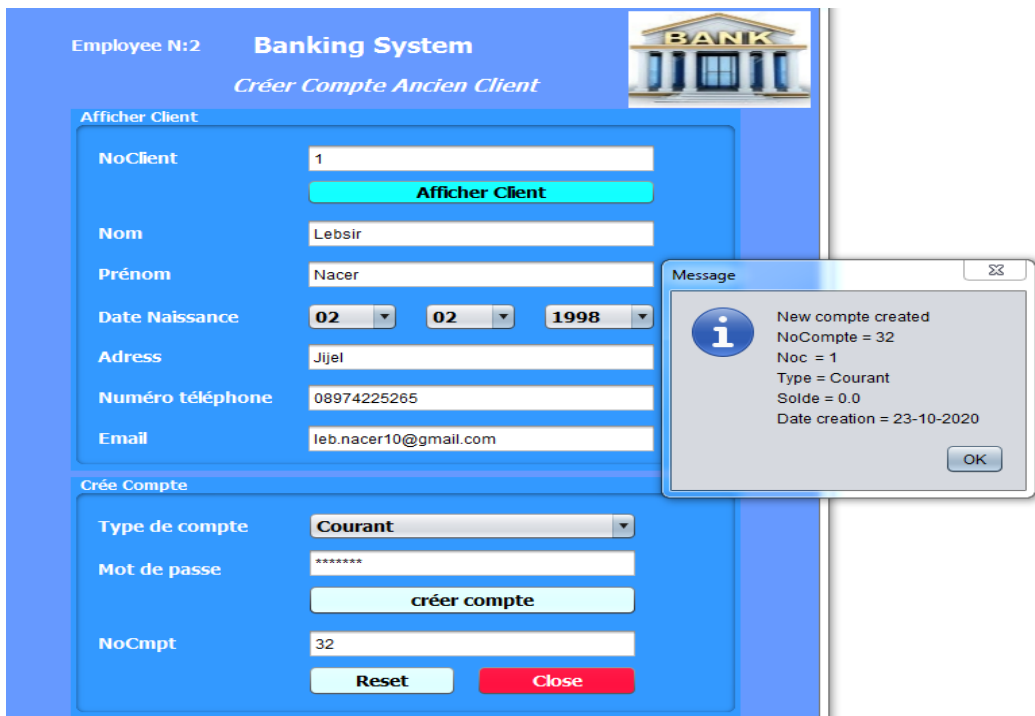


Figure 5.19 : fenêtre créer compte ancien client.

5.4.3.2 Fenêtre versement et retrait d'argent

A partir de cette page l'employé peut faire un versement ou un retrait d'argent d'un compte.



Figure 5.20 : fenêtre versement et retrait d'argent.

5.4.3.3 Fenêtre transfert solde

A partir de cette page l'employé peut faire un transfert d'argent d'un compte à un autre.

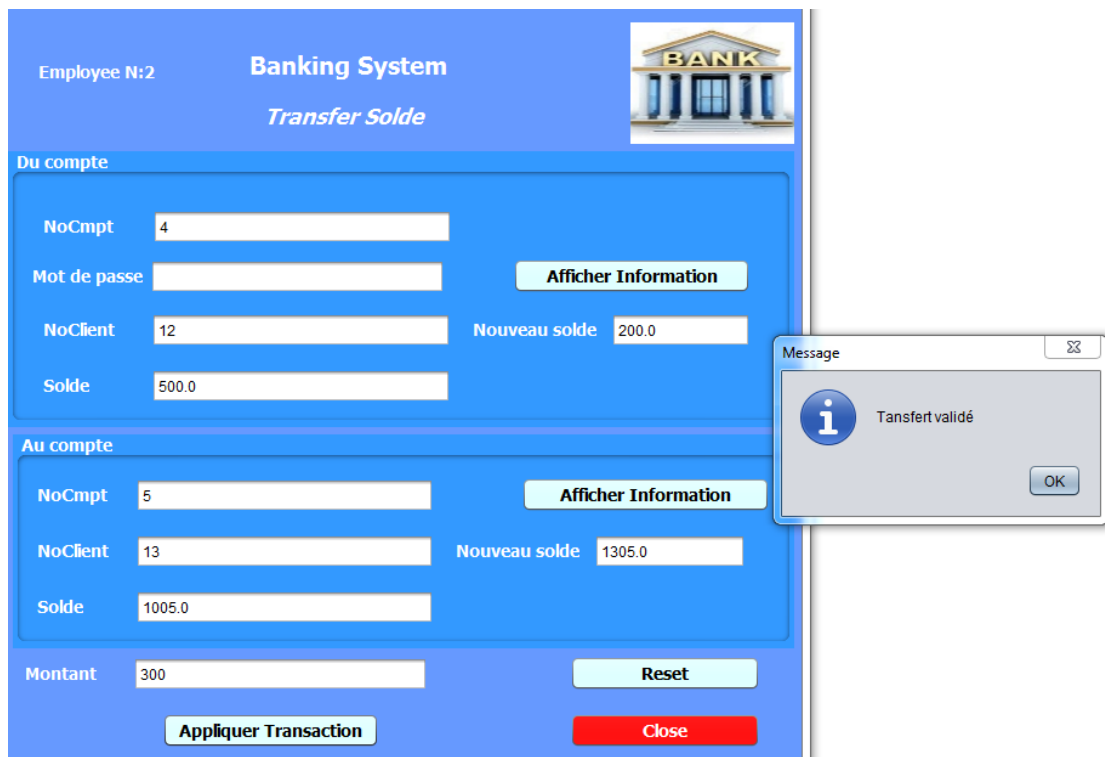
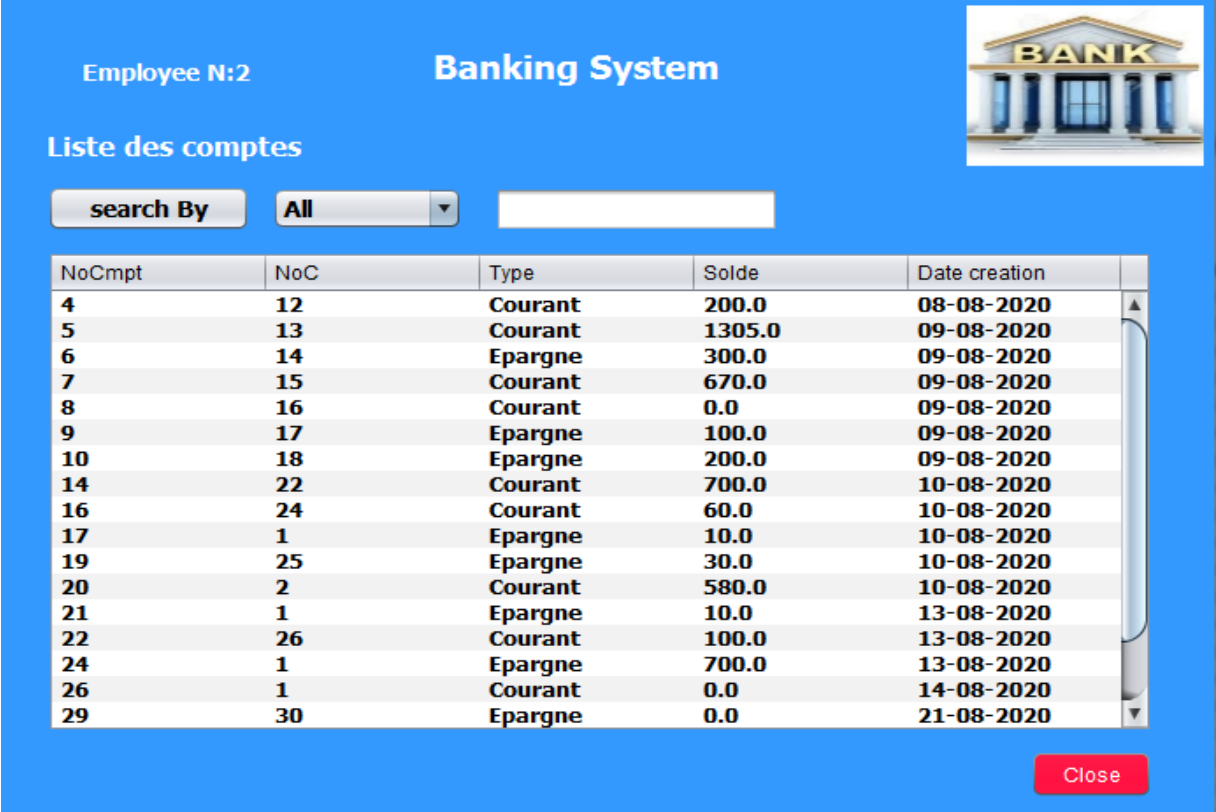


Figure 5.21 : fenêtre transfert d'argent.

5.4.3.4 Fenêtre Afficher liste des comptes

Cette page sert à afficher la liste des comptes et nous permet de chercher une compte par : NoCmpt, NoClient, Type et Date de création.



Employee N:2 **Banking System**

Liste des comptes

search By All

NoCmpt	NoC	Type	Solde	Date creation
4	12	Courant	200.0	08-08-2020
5	13	Courant	1305.0	09-08-2020
6	14	Epargne	300.0	09-08-2020
7	15	Courant	670.0	09-08-2020
8	16	Courant	0.0	09-08-2020
9	17	Epargne	100.0	09-08-2020
10	18	Epargne	200.0	09-08-2020
14	22	Courant	700.0	10-08-2020
16	24	Courant	60.0	10-08-2020
17	1	Epargne	10.0	10-08-2020
19	25	Epargne	30.0	10-08-2020
20	2	Courant	580.0	10-08-2020
21	1	Epargne	10.0	13-08-2020
22	26	Courant	100.0	13-08-2020
24	1	Epargne	700.0	13-08-2020
26	1	Courant	0.0	14-08-2020
29	30	Epargne	0.0	21-08-2020

Close

Figure 5.22 : fenêtre afficher liste des comptes.

5.4.4 Fenêtre d'accueil client

Cette page permet au client d'échanger la clé et de connecter.



Banking System Client

Connecter Compte Client

Echange de clé

AES 128

ECC secp160r1

Echange de clé

Connecter Client

NoCmpt

Mot de passe

Connecter

Close

Figure 5.23 : fenêtre d'accueil client.

5.4.4.1 Fenêtre profil client

Cette page sert à afficher les informations de compte : NoCmpt, NoClient, Type de compte, Solde, date de création de compte. Comme elle permet au client de faire un transfert de solde à un autre compte, afficher la liste des transactions de compte et changer le mot de passe.

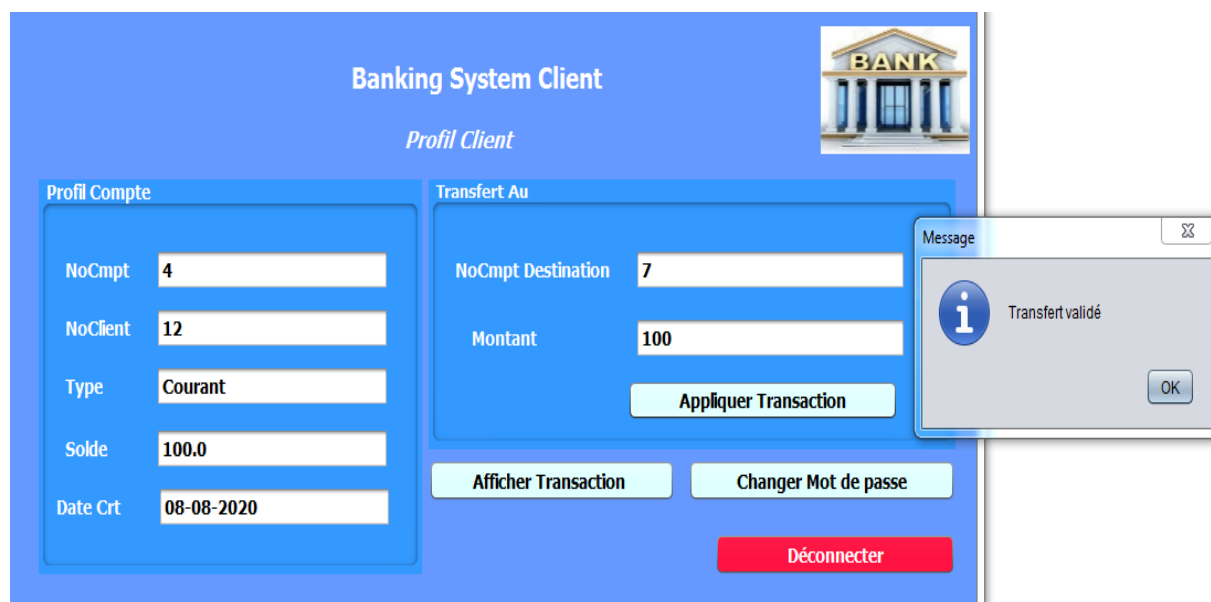


Figure 5.24 : fenêtre profil client.

5.4.4.2 Fenêtre liste transaction de compte

Cette page sert à afficher la liste des transactions de compte.

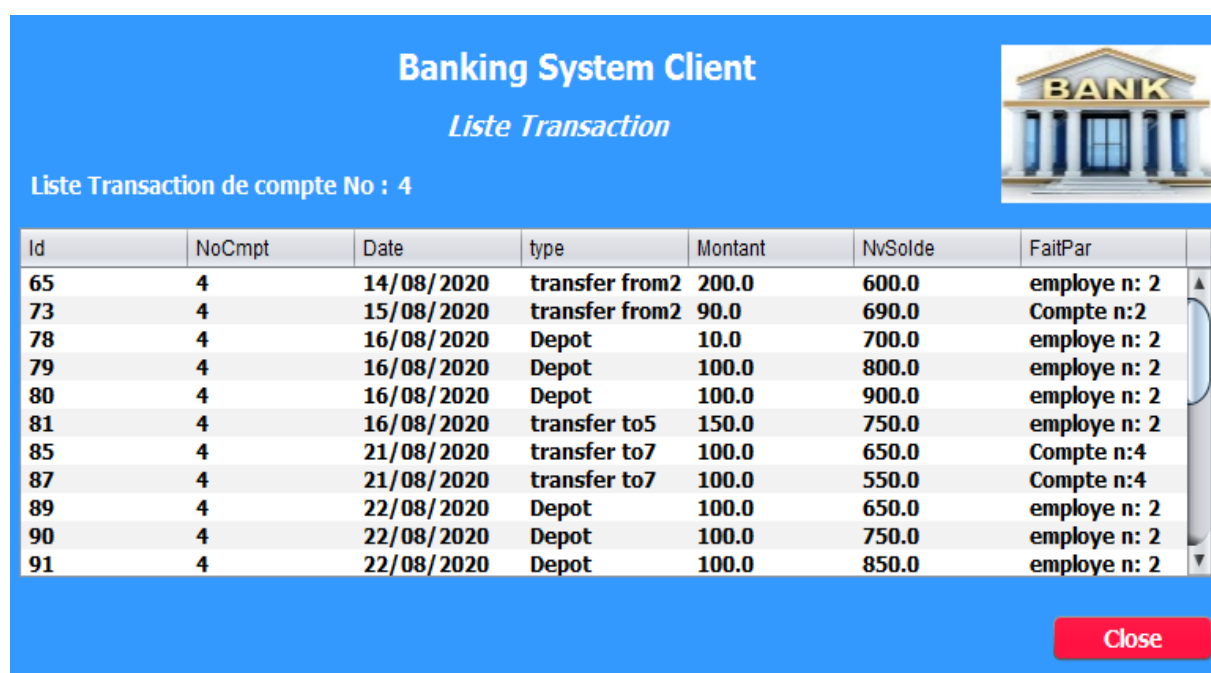


Figure 5.25 : fenêtre liste transactions compte no 4.

5.4.4.3 Fenêtre changer mot de passe

Cette page permet au client de changer le mot de passe.



Figure 5.26 : fenêtre changer mot de passe.

5.5 Conclusion

Au cours de ce chapitre, nous avons présenté une implémentation d'une application client serveur de gestion des comptes bancaires et les différentes phases de la réalisation de cette dernière. Nous commençons par une conception générale à travers une modélisation UML. Ensuite nous avons recensé les différentes technologies logicielles utilisées pour le développement.

Enfin, nous avons exposé certaines captures d'écrans qui illustrent les différentes facettes de notre application.

Conclusion générale

Conclusion générale

Le travail réalisé dans le cadre de notre mémoire s'intéresse aux problématiques liées à la sécurité des données sensibles sur les dispositifs mobiles qui ont fait l'objet de recherches.

À la lumière de l'étude mentionnée précédemment, nous avons proposé un Cryptosystème de chiffrement hybride qui fournit une amélioration de niveau de sécurité au sein d'un terminale mobile et prend en compte les caractéristiques de ce dernier. Ce modèle fournit aux applications un bon niveau de sécurité avec un temps d'exécution rapide.

Le cryptosystème proposé est basées sur la méthode de chiffrement symétrique AES et la technique de cryptographie à base des courbes elliptiques qui présentent les points forts de ce modèle. En effet, La méthode de chiffrement AES qui fournit un bon niveau de sécurité temps d'exécution rapide. Le cryptosystème ECC permet l'échange de clé secrète. Ainsi nous avons réalisé une application client-serveur de gestion des comptes bancaires afin d'implémenter la méthode de chiffrement hybride proposée.

Nous envisageons de faire une extension de notre système vers d'autres réseaux ayant des terminaux limités en terme de capacité des ressources. Ainsi nous envisageons de montrer mathématiquement le gain du niveau de sécurité apporté par notre système par rapport à l'AES et ECC, la perspective la plus dure est d'effectuer des attaques afin de trouver des failles de notre système.

Bibliographie

- [1] G.Pujolle, *Les Réseaux*. 9^e édition. Eyrolles, livre informatique, 2018.
- [2] F.Lemainque, *Tous sur les réseaux sans fil*. Dunod, livre informatique, 2009.
- [3] S.Maamar, A.Lamia, G.Leila et B.Azeddine, *Etude des Performances des Protocoles de Routage dans les Réseaux Mobiles Ad-Hoc*. 4th International Conference on Computer Integrated Manufacturing CIP'2007.03-04, November 2007.
- [4] S.Pierre et M.Maurice, *Introduction aux réseaux mobiles*. GeninovInc, livre informatique 2008.
- [5] Pujolle, Vivier et Al agha, *Réseaux De Mobiles Et Réseaux Sans Fil*, livre informatique. 2001.
- [6] <https://www.apprendre-en-ligne.net/crypto/bibliotheque/PDF/IntroToCrypto.pdf>
- [7] B.Mouchira et B.Azeddine, *Sécurité des Echanges dans un Réseau de Nœuds Mobiles*. Edition universitaires européennes EUE.25, 2017.
- [8] B.Wafa, *Sécurisation des données sensibles sur téléphone mobile / dispositif d'assistant numérique personnel (PDA)*. PhD thesis, Université Abderrahmane Mira de Béjaia, thèse de doctorat, 2007-2008.
- [9] T.Emin Islam, *Security in Context-aware Mobile Business Applications*. Université Mannheim (Turk), thèse de doctorat, 2008.
- [10] O. K. Boyinbode et R. O.Akinyede, *Mobile Learning: An Application of Mobile And Wireless Technologies in Nigerian Learning System*. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.11, November 2008.
- [11] A. Achraf, *Innovation Technologique Dans Les Réseaux Mobiles Et Création De La Valeur: Cas De La Banque Mobile*. Laboratoire de Management Interdisciplinaire Transculturel GET/Institut National des Télécommunications France, octobre 2004.
- [12] Wen-Chen Hu, Chung-wei Lee et Weidong Kou, *Advances In Security And Payment Methods For Mobile Commerce*, Article, 2004.
- [13] L.Bloch et C.Wolfhugel, *Sécurité informatique principes et méthode*. 2^e édition, Eyrolles, livre informatique, 2005.

- [14] J.Walters, Z.Liang, S.Weisong and V.Chaudhary, *Wireless Sensor Network Security: A Survey*. Security in Distributed, Grid, and Pervasive Computing Yang Xiao, Auerbach Publications, CRC Press. 2006.
- [15] CH.Noureddine, *La sécurité des communications dans les réseaux VANET*, mémoire de magistère, 2010.
- [16] Gay pujolle et Davor Males, *WI-FI par la pratique*, livre informatique, septembre 2002.
- [17] I.Bilogrevic, M.Jadliwala and J.Hubaux, *Security Issues in Next Generation Mobile Networks: LTE and Femtocells*. Laboratory for computer Communications and Applications (LCA1), EPFL, Lausanne, Switzerland.
- [18] CH.Alaaedine, *Detection and Reaction against DDoS Attacks in Cellular Networks*. Projet de fin d'étude, The Communication Networks and Security Research Laboratory, l'école supérieure de communication de Tunis, 2006- 2007.
- [19] *Le Grand Livre de SecuriteInfo.com*, livre informatique, Édition du 6 novembre 2006.
- [20] GH.Mohamed, *Proposition d'un Framework Pour Limiter la Propagation des Malwares dans la Communication des Mobiles*. Université Mohammed - V – AGDAL Rabat. thèse de doctorat.2014.
- [21] S.H.Nawal, *Conception et réalisation d'un système collaboratif pour les experts métier à base d'agent et des algorithmes de cryptage*. Université Ahmed ben Bella d'Oran, thèse de doctorat. 2017.
- [22] R.Dumont, *Cryptographie et Sécurité informatique*, livre informatique, 2009 - 2010.
- [23] B.Rabab, *Sécurité des images Numériques compressées JPEG*. Université Djillali Liabès de Sidi Bel Abbes, thèse de doctorat.03 juin 2019.
- [24] A.Nassima et CH.Hamida, *Etude sur l'Applicabilité de la Cryptographie Asymétrique aux Réseaux de Capteurs sans Fil*. Université Abderrahmane Mira de Béjaïa, thèse de master.2012.
- [25] W.Stallings, *Cryptography and Network Security : Principles and Practice*, Sixth Edition, livre informatique, 2014.
- [26] J.-P.Aumasson, *Serious Cryptography A Practical Introduction to Modern Encryption*, No Starch Press, Article, 2018.
- [27] D.Stinson, *Cryptography: Theory and Practice*. CRC Press, livre informatique, 2005.
- [28] B.Mohamed Kamal, *Approche Cryptographique basé sur les algorithmes génétique pour la sécurité des réseaux Adhoc*. PhD thesis, Université d'Oran, thèse de doctorat.

- [29] M.Dubois, *Conception, développement et analyse de systèmes de fonction booléennes décrivant les algorithmes de chiffrement et de déchiffrement de l'Advanced Encryption Standard*. ParisTech, l'école Nationale Supérieure de Paris, thèse de doctorat. 2018.
- [30] Y.SHOU, *Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs*. PhD thesis, Université de Franche-Comté, thèse de doctorat, 2014.
- [31] G.Seroussi I.Blake, G.Seroussi and N.Smart, *Elliptic curves in cryptography*. Cambridge university press, Article, 1999.
- [32] V. Gayoso Martinez, C. Sanchez Avila J. Espinosa Garcia et L. Hernandez Encinas, *Elliptic curve cryptography. java implementation issues*, Article, 2005.
- [33] Vincent Verneuil, *Courbes elliptiques et attaques par cannaux auxiliaires*. Science et Technologie, Article, 2009.
- [34] A.Singh et R.Singh, *Various attacks over the elliptic curve-based cryptosystems*. International Journal of Engineering and Innovative Technology (IJEIT), 2015.
- [35] S.Pontié, *Sécurisation matérielle pour la cryptographie à base de courbes elliptiques*. PhD thesis, Université Grenoble Alpes, thèse de doctorat, 2016.
- [36] B.Hichem. *Sur la sécurité de l'information par le biais des courbes elliptiques*. PhD thesis, Université Djillali Liabes Faculté Des Sciences exactes, Sidi Bel Abbés, thèse de doctorat, 2018.
- [37] C.Gonçalves, *Cryptographie Avancée Courbes elliptiques*, livre informatique, 2015.
- [38] I.Lotfi, *Cryptographie à base de courbes elliptiques*. PhD thesis, Ecole Nationale Supérieure d'Informatique, thèse de doctorat, 2017.
- [39] <https://www.secg.org/SEC2-Ver-1.0.pdf>.
- [40] https://fr.wikipedia.org/wiki/Pretty_Good_Privacy.
- [41] https://en.wikipedia.org/wiki/GNU_Privacy_Guard.
- [42] P.Crescenzo. *OFL : Un modèle pour paramétrer la sémantique opérationnelle des langages à objets application aux relations inter-classes*. PhD thesis, l'Université de Nice-Sophia Antipolis, thèse de doctorat, 2001.
- [43] <http://www.oracle.com/technetwork/java/javase/tech/index.html>.
- [44] https://www.techno-science.net/de_nition/5346.html.
- [45] <https://sqlabs.com/sqlitemanager>.
- [46] B.Mouchira, *Sécurité des échanges dans un réseau de nœuds mobiles*, Université El Hadj LAKHDER – BATNA, thèse de Magistère en Informatique, 2012.

- [47] M.Boutora et D.Benami, *Conception, Etude et Réalisation d'un Cryptosystème Hybride de Transmission d'Images*, Université Mouloud Mammeri TIZI-OUZOU, thèse de Master académique, 2015.
- [48] H.Nadjib, *Study and Analysis of a Hybrid Image Encryption Algorithm Using Chaos and Generating Functions*, Université Mohammed Saddik BenYahia JIJEL, thèse de Master, 2019.
- [49] K.Karima et G.Halima, *Modèle de cryptographie à base des courbes elliptiques pour les réseaux mobiles*, Université Mohammed Saddik BenYahia JIJEL, thèse de Master, 2019.