

ECOLE SUPERIEUR D'INFORMATIQUE SALAMA

République Démocratique du Congo

Province du Haut-Katanga

www.esisalma.org



MISE EN PLACE D'UN SYSTEME AUTOMATIQUE DE GESTION DE RETRAIT
DES ENFANTS DES ECOLES MATERNELLES AVEC LA TECHNOLOGIE NFC

« Cas de la ville de Lubumbashi »

*Travail présenté et défendu en vue de l'obtention du
grade d'ingénieur technicien en informatique*

Par : MANGI KYANDIKO Patrick

Option : Télécommunications et Réseaux

Directeur: Mr MUKANDA Papy

Co-directeur: Mr HEMEDY Saleh

Septembre 2019

EPIGRAPHE

«Travail avec courage et persévérance, car la ténacité
permet d'atteindre l'excellence !»

Didier Court

DEDICACE

A vous mes parent Michel KABO et Brigitte PANDE

A vous mes frères et Sœurs

REMERCIEMENTS

A notre Dieu des armés lui qui est le maître de temps et des circonstances, lui qui a permis à ce que mon passage à ESIS puisse être un succès pour moi, une satisfaction pour mes parents et une joie pour mes frères et sœurs infiniment merci mon Dieu.

Que monsieur Papy MUKANDA ainsi que monsieur Saleh HEMEDY pour avoir accepté la direction et la codirection de ce travail malgré les temps parfois difficiles trouvez ici l'expression de notre profonde gratitude ;

Nous tenons également à dire un grand merci à tout le corps professoral de l'ESIS en général et en particulier celui de la filière réseau pour leur encadrement et orientation lors de notre passage sur le banc de l'école.

A vous mes parents Michel KABO et Brigitte PANDE merci pour votre soutien à mon égard étant à une grande distance de vous, vous avez montré votre amour, votre soutien pour qu'aujourd'hui que je puisse arriver à la fin de mon premier cycle je suis reconnaissant pour vos efforts merci pour tous que le Dieu des armés puisse vous bénir et vous donner la bonne santé et tout ce que vous désirez.

A vous mes tantes et oncle : Irène MULE, Matty M, Lydia KAULO, Michou PANDE, Docteur Jean Marie.

A vous mes frères et sœurs Inès MUNGOYANGA, Ariane MWEPU, Chatty CIME, Gael KABO, Guy PANDE, Musa BEYA pour votre amour et votre soutien je vous dis merci

A nos condisciples et compagnons de lutte avec qui, unis par le sort nous avons cheminé tout au long de notre cursus. Nous pensons : Alex DITUNGA, Héritier MULUNDA.

A tous nos amis de notre entourage l'internat IEM Kamolondo je vous dis merci.

Sans oublié mes ami(e)s qui m'ont aidé durant ce parcours d'une manière ou d'une autre Christvie MBWEY, Belange YAV, Aline BINTI, Ornella KALUNGA, Chris MWAMBA, Gloire KAFWALUBI, Caleb KAWAYA, Grive MULAJI MUPASA Jean-Luc , Steven MONGA, Francis JELEMANI, Moise SOMPO, Gael KYANDA, Christian LUMBU, Trésors NGONGO, David VILA, Ghad BANZE, John JADIKA, Gloire KAMINYE, Marose KET-HILA, Djo MIKOMBE.

LISTE DES FIGURES

Figure 2. 1 Diagramme de cas d'utilisation du système envisagé	23
Figure 2. 2 Diagramme de séquence montrant le processus de création de compte.....	24
Figure 2. 3 processus d'authentification	25
Figure 2. 4 Diagramme de séquence pour l'inscription d'un élève	26
Figure 2. 5 Diagramme de séquence pour la présence des élèves	27
Figure 2. 6 Diagramme de séquence pour le retrait d'un élève	28
Figure 2. 7 Diagramme d'activité de l'inscription à la présence	30
Figure 2. 8. Diagramme d'activité pour le retrait	31
Figure 2. 9 model logique de données	32
Figure 3. 1 code barre	38
Figure 3. 2 code QR.....	38
Figure 3. 3 Principe de fonctionnement de la RFID	40
Figure 3. 4 Une étiquette RFID	41
Figure 3. 5 le fonctionnement NFC/RFID	46
Figure 4. 1 Fonctionnement de la solution	50
Figure 4. 2 lecteur de carte NFC.....	51
Figure 4. 3 Présentation de WampServer	54
Figure 4. 4 Connexion à la base de données.....	54
Figure 4. 5 Création d'une nouvelle base de données et des tables.....	55
Figure 4. 6 Page d'accueil de l'application.....	55
Figure 4. 7 Formulaire d'inscription.....	56
Figure 4. 8 Le matricule de l'élève	56
Figure 4. 9 les élèves inscrits à l'école	57
Figure 4. 10 Affichage des élèves inscrits	57

LISTE DES TABLEAUX

Tableau 3. 1 Description du processus de fonctionnement de la RFID.....	40
Tableau 3. 2 Les fréquences d'utilisation	44
Tableau 3. 3 caractéristiques de la NFC	48

LISTE D'ACRONYMES

CAB : Code à Barre

ISBN : International Standard Book Number

EAN : European Article Numbering

CUP : Code Universel des Produits

PDF 417 : Portable Data File

QR : Quick Response

RS-232 (EIA 232 ou TIA 232) :

USB : Universal Serial Bus

EPC : Electronic Product Code

ASIC : Specific Integrated Circuit

ERP : Enterprise Ressource Planning

HF : Haute Fréquence

RF : Radio Fréquence

UHF : Ultra Haute Fréquence

LF : Low Frequency (Basse Fréquence)

RFID : Radio Frequency Identification

NFC : Near Field Communication

ISO : Organisation Internationale de Normalisation

CEI : Communauté des Etats Indépendants

CNIL : Commission Nationale de l'Informatique et des Libertés

DAB : Distributeur Automatique de Billet

TPE : Terminal de Paiement Electronique

NFC IP-1 : Near Field Communication Interface and Protocol

AINSSI : Autorité Nationale en matière de Sécurité et de défense des Systèmes d'Information

Mhz : Mégahertz

KHz : Kilohertz

 TABLE DES MATIERES

Table des matières	
EPIGRAPHE	I
DEDICACE	II
REMERCIEMENTS.....	III
LISTE FIGURES.....	V
LISTE TABLEAUX.....	VI
LISTE ACRONYMES	VII
TABLE DES MATIERES	IX
AVANT-PROPOS	XII
INTRODUCTION GENERALE	1
0.1 Présentation du sujet	1
0.2 Problématique	1
0.3 Hypothèse	2
0.4 Etat de la question.....	2
0.5 Etat de l'art.....	3
0.6 Choix du sujet	3
0.6.1 Contexte du projet.....	3
0.7 Délimitation du travail	4
0.8 Méthodes et technique	4
0.8.1 Méthodes.....	4
0.8.2 Techniques	5
0.9 SUBDIVISION DU TRAVAIL.....	5
0.10 Outils logiciels et équipements utilisés.....	6
0.10.1. Logiciels.....	6
CHAPITRE 1 : ETUDES SECURITAIRES DANS LES ECOLES MATERNELLES ET DESCRIPTION DU SYSTEME EXISTANT	7
1.1 Introduction partielle.....	7
1.2 Etude de la sécurité et menace dans les écoles	7
1.3 Les types de menaces dans les écoles	8

1.3.1 Risques généraux	8
1.3.2 Risque liés à la criminalité.....	8
1.3.3 Manières dont une personne parvient à accéder au sein de l'école sans autorisation.....	10
I.4 Le diagnostic de sécurité	11
1.4.1 Le contrôle des accès	11
1.4.2 Mesures nécessaires	12
1.4.3 Mesures organisationnelles.....	12
1.4.4 Mesures architecturales et mécaniques.....	12
I.4.5 Politique relative aux portes	12
1.4.6 Les mesures électroniques	12
1.5 Plan de sécurité des écoles maternelles	13
I.6 Description du système existant	14
1.6.1 Sources d'information.....	14
1.6.2. Fonctionnement du système existant	14
1.7 Menace.....	15
1.7.1 Menaces liées au système	15
1.7.2 Menace du à l'indisponibilité de parents	16
1.7.3 Menaces liées aux perturbations de l'environnement.....	16
1.8 Critique du système	16
1.8.1 Point fort	16
1.8.2 Point faible.....	17
1.9 Orientation	17
1.10 Conclusion partielle	19
CHAPITRE 2 : SPECIFICATION DE BESOIN ET CONCEPTION LOGIQUE DE LA SOLUTION	20
2.1 Introduction partielle.....	20
2.2 Analyse et spécification de besoin.....	21
2.3 Formulation du besoin	21
2.3.1 Besoin non fonctionnel	22
2.3.2 Besoin fonctionnel	22

2.4 Modélisation du système envisagé	22
2.4.1 Diagramme de cas d'utilisation	23
2.4.2 Diagramme de séquence	24
2.4.5 Diagramme d'activé.....	30
2.5 Conception du système de gestion de base de données	32
2.5.1 Model logique de données	32
Chapitre 3 : ETUDE TECHNOLOGIQUE ET CONCEPTION PHYSIQUE DE LA SOLUTION	34
3.1 Introduction partielle.....	34
3.2 Raison de s'authentifier	34
3.3 Les technologies d'identification.....	34
3.4 Identification par la biométrie.....	35
3.3.1 Contexte d'utilisation de la biométrie.....	35
3.3.2. Famille de système de biométrie	35
3.5 Indentification par les codes	37
3.5.1 Le code-barres.....	37
3.5.2. La RFID	40
3.5.3 La NFC	44
3.6. Critères de choix de la technologie.....	48
3.7 Conclusion partielle	49
CHAPITRE 4 : IMPLEMENTATION DE LA SOLUTION	50
4.1 Introduction partielle.....	50
4.2 Environnement de travail.....	51
4.2.1 Environnement matériel.....	51
4.2.2. Outils de développement de l'application	52
4.3 Présentation de l'application	53
4.3.1 Le lancement du serveur Web WAMP SERVER.....	53
4.4 Conclusion partielle	58
CONCLUSION GENERALE.....	50
REFERENCE.....	52

AVANT-PROPOS

Le programme national des institutions supérieures techniques de notre pays, prévoit des défenses des travaux ou projets à la fin du premier cycle des études en informatique, et l'Ecole Supérieure d'Informatique Salama qui est régie par ce programme, prévois des défenses de ceux-ci. Par cette occasion s'inscrit ce présent travail de fin d'études en réseaux et télécommunications intitulé : «MISE EN PLACE D'UN SYSTEME AUTOMATIQUE DE GESTION DE RETRAIT DES ENFANTS DES ECOLES MATERNELLES AVEC LA TECHNOLOGIE NFC ».

On ne pourrait dire que notre travail est exempt d'erreurs ! Comme disait John KENNEDY : « une erreur ne devient faute que si l'on refuse de la corriger », c'est avec modestie que nous accepterons toutes les critiques et suggestions constructives pouvant nous permettre d'améliorer notre travail ultérieur.

La sécurité est importante dans notre société et nous avons besoin de remédié à toutes formes d'insécurité qui entourent la société

INTRODUCTION GENERALE

0.1 Présentation du sujet

La société actuelle est confrontée à plusieurs formes d'insécurité (banditisme sous plusieurs formes de maltraitance : viol, vol, kidnappage, et autres) et dans divers endroits dans les maisons, les écoles sur les rues et cela inquiète la population.

Nous, nous visons les écoles et précisément les écoles maternelles et les crèches, ou nous y trouvons des enfants qui n'ont pas encore cette conscience avérée et encore moins un sens de responsabilité accru pour se prendre en charge eux-mêmes, ces enfants sont faciles à manipuler et à tromper, ils sont accompagnés à l'école chaque matin par les parents ou par un membre de famille.

0.2 Problématique

Dans nos écoles l'inquiétude c'est au niveau du retrait des enfants parce que les enfants sont en charge de l'école dès leurs arrivés jusqu'à la sortie, les écoles utilisent un système manuel pour identifier l'enfant en donnant une carte papier qui contient les identités de l'enfant, mais les n'arrivent pas à gérer le retrait parce qu'ils délivrent les enfants à quiconque possède cette carte, la certitude de la personne qui doit prendre l'enfant est faible parce que une personne malintentionnée peut facilement se procurer une carte papier et se pointer à l'école pour récupérer l'enfant et les écoles peuvent facilement donner l'enfant sans même poser de question juste parce que la personne possède la carte contenant les identités de l'enfant.

Les écoles n'arrivent pas à gérer et à se justifier aussi en cas de perte d'enfants parce que la présence des enfants est faite à la sortie de classe, elles ne savent pas quel enfant était présent le matin et qui ne se retrouve pas en classe à la sortie. Pour remédier à ces problèmes nous allons proposer une solution pour renforcer la sécurité des enfants et aider les écoles à faire une bonne gestion et suivi de ses élèves, quelques questions sont posées pour une compréhension claire du problème.

Comment arriver à identifier la personne qui prend l'enfant et être certain que cette personne est habilitée à le faire ainsi que l'heure de retrait ?

Quel mécanisme mettre en place pour remplacer le système papier et renforcer la sécurité et la gestion des élèves ?

0.3 Hypothèse

La société a besoin des solutions pratique pour renforcer la sécurité nous essayerons de donner réponse aux questions posées ci-haut.

Pour une sécurité renforcée des enfants dans les écoles maternelles et crèches, nous allons mettre en place un système automatique de vérification des personnes qui prennent les enfants à l'aide d'une carte à puce difficile a falsifié qui remplacera le papier et cela permettra de faire la présence à l'arrivée de l'enfant, ce système consistera à donner aux parents des enfants une carte à puce qui contiendra un code identifiant un élève et cette carte sera lue que par le lecteur de cartes (lecteur NFC) que seul l'école possèdera, cela pour la sécurité des enfants et nous permettra d'identifier la personne qui a pris l'enfant, l'heure que l'on a pris l'enfant et avoir un suivi concernant les enfants qu'on prend avec retard, avec ce statistique l'école peut convoquer les parents pour le bien de l'enfant.

Ce système permettra à l'école de faire la présence question d'être sure quand on viendra récupérer l'enfant qu'il était bel et bien en classe, c'est la technologie NFC une technologie d'identification sans contact (technologie à zone rapprocher) qui nous permettra de réalisée le système.

0.4 Etat de la question

Pour notre travail nous avons été inspiré par les travaux de nos prédécesseurs et quelques innovations d'étudiants qui nous avons exploité leurs sujets dans des angles différent et de technologies différentes, nous avons lu les travaux de certains étudiants :

- Etude de la sécurité et de la localisation des élèves dans une école maternelle par un système de localisation RFID suivi d'un message vers un tuteur en 3G » défendu par

Dornit LONGWA 2015-2016

- KARUMB IRUNG Marianne, G3 télécom « radio identification des matériels de laboratoire, cas d'ESIS » année 2015-2016
- KILEPA MWEWA Arcel G3 Telecom « étude de mise en place pour la gestion des animaux, cas du zoo de LUBUMBASHI » année 2015-2016
- Signature automatique à l'aide de carte magnétique JPO 2017-2018

0.5 Etat de l'art

Dans ce monde du numérique ou notre pays est en train d'émergé nous avons voulu changer ce qui est manuelle [archaïque] à un système numérique [automatique], en touchant quelques points et une technologie que nos prédécesseurs n'ont pas touché et utiliser.

Faire une chose deux fois ne fera pas de notre recherche une innovation, c'est pourquoi nous avons voulu exploiter d'autre zones que nos prédécesseurs n'ont pas touché et apporte des innovations en utilisant une autre technologie.

0.6 Choix du sujet

Pour notre recherche on a opté pour le sujet intitulé : « Mise en place d'un système automatique de gestion de retrait des enfants des écoles maternelles avec la technologie NFC »

0.6.1 Contexte du projet

Notre sujet concerne un renforcement de la sécurité dans les écoles et les enfants seront plus ou moins bien gérer. Les écoles seront alaise dans la gestion de leurs élèves au lieu de faire recours chaque fois aux papiers.

Notre travail a les intérêts liés à la société et ceux de ma filière :

- Dans la société on aide les parents et les écoles, les parents ne seront plus très inquiets parce qu'avec ce système l'école pourra assurer la sécurité des enfants normalement.
- Par rapport à ma filière le travail me permet la prise en mains de différentes technologies d'identification et de localisation et certains de ces technologies

utilisent les notions de radio transmission, de transmission de données et cela nous a permis de bien assimilé certaines notions.

0.7 Délimitation du travail

Notre travail se focalise sur la technologie NFC qui est une technologie d'identification sans contact à champs proche et notre travail va se limiter sur l'identification de la personne qui prend l'enfant, faire la présence automatique de l'enfant, faire une gestion statistique des événements des enfants à l'école ainsi qu'identifier l'enfant en question et nous avons **pris** quelques échantillons des écoles de la ville de Lubumbashi et cela nous a poussé à généraliser notre travail pour toutes la ville de Lubumbashi.

0.8 Méthodes et technique

0.8.1 Méthodes

Comme tout travail scientifique digne de ce nom, la réalisation de ce travail passera par des méthodes et techniques qui sont :

- Top down design
qui nous permis de faire une analyse et spécification de besoin qui nous a amenés à faire une conception physique ainsi que logique en quittant le plus niveau d'abstraction vers le plus bas niveau et elle nous a permis de découper notre travail en module.
- Analytique
Cette méthode nous permettra de bien approfondir nôtre étude dans la localisation, l'identification avec NFC/RFID.
- L'implémentation
Cette méthode consiste à passer une série de test afin de vérifier et de tester l'hypothèse, en se basant sur l'expérience scientifique.
- L'interprétation
L'implémentation ainsi faite il s'agira ensuite d'être capable d'expliquer d'une manière concrète le résultat obtenu

- Comparative : celle-ci nous a permis de faire une étude de différentes technologies d'identifications, enfin de faire un choix pour celle qui sera jugé efficace selon le besoin et le cas d'application.

0.8.2 Techniques

- Documentation

La consultation des livres, manuels, tutoriels, forum possédant beaucoup des détails sur le sujet que nous traitons.

- L'interview

Nous ne sommes pas les premiers ni les derniers à traiter ce sujet, d'où cette méthode nous a permis à entrer en contact avec nos prédécesseurs, afin de rendre plus robuste notre travail.

0.9 SUBDIVISION DU TRAVAIL

Notre recherche repose sur quatre chapitre ainsi nous allons détailler chacun de ces chapitre

Chap. 1. ETUDES SECURITAIRES DANS LES ECOLES MATERNELLES ET DESCRIPTION DU SYSTEME EXISTANT

Dans ce chapitre il sera question de faire une étude approfondie de la sécurité des écoles, les menaces auxquelles les écoles font face ainsi que faire une étude descriptive du système existant dans les écoles.

Chap. 2. CONCEPTION LOGIQUE DE LA SOLUTION ET SPECIFICATION DE BESOIN

Le chapitre deux faire l'objet l'analyse de besoin ainsi que la conception d'une manière logique du système envisagé, nous allons donner tous les acteurs qui entrerons en contact avec le système.

Chap. 3. CONCEPTION PHYSIQUE DE LA SOLUTION

Dans ce chapitre nous parlerons de différente technologies d'identifications qui existent ainsi que leurs manières de fonctionner ensuite nous allons faire un choix sur une technologie qui va répondre à notre besoin.

Chap. 4. IMPLEMENTATION DE LA SOLUTION

Dans ce dernier chapitre nous allons implémentés la solution avec les guide d'utilisation

0.10 Outils logiciels et équipements utilises

0.10.1. Logiciels

- *Système d'exploitation 10 professionnel 64bits*
- *Microsoft Office Word 2016 : pour l'édition des textes et la gestion des références bibliographiques*
- *Star UML: pour la modélisation*
- *Edraw Network Diagram : Pour les différentes schémas et figures*

CHAPITRE 1 : ETUDES SECURITAIRES DANS LES ECOLES MATERNELLES ET DESCRIPTION DU SYSTEME EXISTANT

1.1 Introduction partielle

Les écoles en générale sont des endroits où plusieurs personnes fréquentent pour diverses raisons à des heures différentes, les écoles ne savent pas qui entre, quand et pourquoi et ce laissé aller peut être la base de plusieurs dégâts, alors nos écoles doivent mettre en place de mécanismes pratique pour les heures de fréquentation de gens qui accèdent dans les écoles pour renforcer la sécurité des élèves ainsi que de responsable de la dite école.

Etant donné notre travail vise à renforcer la sécurité et la gestion dans les écoles maternelles nous voulons donner l'aperçu de ce qui se passe réellement dans les écoles de la ville, la façon de faire la gestion générale des enfants et aussi comment l'école arrive à se libérer de la charge des enfants après le cours ainsi les statistiques de gestion de l'école.

Bien avant la description du système existant nous devrions d'abord faire une étude sur la sécurité dans les écoles ainsi que les risques auxquels les écoles sont confrontées.

1.2 Etude de la sécurité et menace dans les écoles

1.2.1 Définition

Selon le dictionnaire Larousse la sécurité est une situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration. Cette installation présente une sécurité totale.

Situation de quelqu'un qui se sent à l'abri du danger, qui est rassuré.

Absence ou limitation des risques dans un domaine précis : Ils recherchaient la sécurité matérielle.

Nous venons de comprendre la sécurité, la sécurité est différente dans chaque domaine, ce travail se basera dans le domaine de l'éducation, nous voulons étudier les mécanismes sécuritaires qui devraient être mise en place, étudier les menaces auxquelles les écoles peuvent faire face et propose de solution ainsi que de piste de solution pour garantir la sécurité des élèves et mettre beaucoup plus l'accent sur la sécurité des enfants des écoles maternelles dont l'intelligence n'est pas encore très développé.

1.3 Les types de menaces dans les écoles

Pour arriver à mettre une forme quelconques de sécurité nous devrions d'abord prendre conscience de menaces auxquelles les écoles font face puis prendre les mesures (préventives) les plus adéquates, il importe d'être conscient des risques existants. Il convient ici d'aboutir à un aperçu global de la situation et ne pas se borner uniquement aux menaces liées à la criminalité. Nous devons aussi analyser d'une manière détaillée les méthodes et mode opératoires mise en pratique par les personnes mal intentionnées pour accéder de manière illicite dans les écoles maternelles.

- Risques généraux
- Risques liés à la criminalité
- Manières dont une personne accède de manière illicite au milieu d'accueil

1.3.1 Risques généraux

1.3.1.1 Risque d'incendie et gestion d'accès.

Les statistiques nous montrent qu'il y a un chiffre vraiment élevé des bâtiments qui prennent feu ici chez nous en RDC, avec les conséquences dramatiques qu'on connaît: morts, traumatismes physiques et psychologiques, dégâts matériels et économiques considérables. Il faut donc rester vigilant vis-à-vis de ce risque. [1]

Un accès trop sécurisé risque d'empêcher l'évacuation adéquate du bâtiment en cas d'incendie. Toutefois, l'accueillante, l'accompagnateur ou la personne responsable doit pouvoir évacuer les enfants présents à tout moment de manière rapide et efficace. Il importe dès lors d'établir des politiques uniformisées en matière d'accès et de sécurisation.

1.3.1.2. Elèves qui s'enfuient sans être aperçus

Les enfants peuvent s'enfuir du milieu d'accueil ou de l'aire de jeux extérieure sans être aperçus, ou manquer à l'appel après une promenade. Si la disparition n'est pas constatée directement, les dégâts psychologiques et physiques peuvent être très importants.

1.3.2 Risques liés à la criminalité

1.3.2.1 Vol

Voler, c'est soustraire à une personne son bien. Comme le dit le proverbe, « l'occasion fait le larron ». Dans ce cas-là, des malfaiteurs remarquent par hasard un objet à voler et passent à l'action. Il n'y a pratiquement pas préméditation dans ce cas.

Les écoles maternelles ne contiennent généralement pas des sommes d'argent importantes ou des appareils de haute technologie. Pourtant, il arrive que des voiturettes d'enfants se trouvant à proximité de l'entrée du bâtiment soient volées, par exemple. Il existe également ce qu'on appelle les vols "ciblés". L'auteur sélectionne scrupuleusement une cible (lors d'une phase d'observation préalable) et détermine à l'avance ce qu'il souhaite dérober. [2]

1.3.2.2. Vandalisme

Le vandalisme consiste à endommager ou à détruire intentionnellement des biens qui sont la propriété d'autrui. D'un point de vue matériel, ces actes ne rapportent rien à leurs auteurs. Les vandales agissent généralement par ennui, par vengeance ou simplement par jeu, sans tenir compte des conséquences. Le vandalisme est presque toujours commis en groupe. Dans la plupart des cas, il s'agit de gamineries même si l'auteur peut également agir par malaise, voire en raison de troubles psychologiques plus graves. Qui prennent feu ici chez nous en RDC, avec les conséquences dramatiques qu'on connaît. [3]

1.3.2.3. Enlèvement

Dans le passé, il est déjà arrivé qu'un inconnu tente d'enlever un enfant de l'enceinte de l'école. Pour ce faire, la personne a toujours profité du moment d'affluence où les parents venaient chercher leurs enfants. L'école est aussi confrontée à des divorces conflictuels. Des parents se disputant la garde de leurs enfants n'hésitent parfois pas à tenter, par le biais de l'école, d'établir un contact avec leur enfant, voire de l'enlever. Dans les deux cas, l'aspect "accès" est primordial. Toutefois, dans la pratique, c'est généralement le flou qui règne parmi le personnel lorsqu'une personne autre que les personnes habituelles vient récupérer l'enfant. Il importe au plus haut point que l'accueillante ou l'accompagnateur soient informés des différentes personnes ayant l'autorisation du (des) parent(s) responsable(s) de venir récupérer l'enfant. L'accompagnateur non permanent du groupe d'enfants doit également disposer de ces informations. Aucune exception ne pourra dès lors être accordée aux accords conclus à ce niveau avec les parents. [3]

1.3.2.4. Agression

Les écoles maternelles n'échappent pas aux agressions verbales ou physiques. Ces deux formes d'agressions peuvent entraîner une douleur psychologique et/ou physique non négligeable. L'agresseur opère notamment pour les raisons suivantes :

- Il veut s'introduire dans le bâtiment afin d'y dérober un objet/d'enlever une personne ou d'occasionner des dégâts ;
- Il veut récupérer son enfant ou un autre enfant sous de vrais ou faux prétextes, mais sans en avoir reçu l'autorisation ; Il a plusieurs plaintes, frustrations au sujet de votre structure d'accueil (bâtiment, organisation, fonctionnement, ...) et veut pénétrer dans le bâtiment.

1.3.3 Manières dont une personne parvient à accéder au sein de l'école sans autorisation

1.3.3.1 Occasion (opportunité)

Les cambrioleurs peuvent profiter de "l'occasion" ou de "l'opportunité" pour pénétrer dans votre milieu scolaire sans en avoir reçu l'autorisation. Si le milieu scolaire investit dans des dispositifs de sécurité, il est également tenu de les utiliser en conséquence. L'installation d'un vidéophone est inutile si la porte finit malgré tout par rester ouverte. En outre, une attention particulière est souvent accordée à la sécurisation et au contrôle de l'entrée principale, oubliant par là même les entrées latérales et celles situées à l'arrière du bâtiment. [4]

1.3.3.2 Tromperie

Les malfrats peuvent également user de la technique de la tromperie ou 'ingénierie sociale'. 'L'ingénierie sociale', également appelée 'l'art de la tromperie', utilise l'individu comme maillon faible. Voici quelques exemples de techniques fréquentes (seules ou en combinaison) d'accès non autorisé dans un milieu scolaire pour enfants :

- L'amabilité, la flatterie, l'intimidation ;
- La tactique du "namedropping", ou le malfrat utilise (abusivement) des noms d'organisations (ex. inspection par des instances compétentes, inspection de la police/des pompiers), de collaborateurs ou du jargon professionnel, etc ;
- L'utilisation (abusive) de documents formels à l'égard du personnel ;
- La tactique 'de l'urgence', où le malfrat crée une situation qui montre qu'une demande précise est urgente et qu'il doit y donner suite dans les plus brefs délais (ex. : inspection de la police/des pompiers, des services de sécurité de la chaîne alimentaire, ...) ;

- Une surcharge d'informations par laquelle le malfrat tente de vous dominer et un recours à l'autorité.

Aucune mesure architecturale ou électronique ne permet de contrer ces techniques.

La seule solution possible est la vigilance du personnel de la structure d'accueil et la prise de différentes mesures préventives organisationnelles. [5]

1.3.3.3 Accès non autorisé en suivant une autre personne

Un autre mode d'accès non autorisé auquel on doit prêter attention est le "tailgating" ou "piggybacking". Dans ce cas, le malfaiteur suit, sans contrôle, une autre personne à l'intérieur ou à l'extérieur. Cette tactique requiert également une vigilance de la part du personnel de l'école. [5]

1.3.3.4 Collaboration interne

Dans certains cas très graves, le cambrioleur bénéficie de la complicité d'un collaborateur interne du milieu d'accueil. A ce niveau, les mesures prises doivent être étroitement liées à la politique du personnel. Un contrôle minutieux du personnel lors du recrutement, entre autres, revêt ici une importance capitale. [5]

1.4 Le diagnostic de sécurité

La prévention et la sécurité constituent un travail sur mesure. Le contrôle des accès doit dès lors être élaboré progressivement et de manière logique : Dans ce point nous Analyserons d'une manière profonde la structure que doit prendre les écoles, sa situation dans l'environnement et l'accès aux espaces intérieurs et extérieurs ; ensuite, nous Identifierons les points problématiques en matière de sécurité et nous dresserons une liste des mesures à prendre ; pour enfin Evaluez et corrigez la situation. [4]

1.4.1 Le contrôle des accès

Dans les écoles les accès doivent être surveillés et il est important d'avoir une seule entrée principale par laquelle tous les mondes passent cela évitera les menaces extérieurs parce que la sentinelle ou l'agent de sécurité devra voir les gens qui veulent entrer et signaler toutes tentatives d'insécurité.

1.4.2 Mesures nécessaires

Si un cambrioleur ne parvient pas à accéder rapidement au bâtiment, il mettra vite fin à sa tentative. Il importe donc d'accorder une attention toute particulière aux mesures organisationnelles, architecturales, et électroniques, sans oublier la qualité du matériel utilisé.

1.4.3 Mesures organisationnelles

La sécurité commence par l'adoption de bonnes habitudes. Bien que souvent négligées, ces mesures sont peu coûteuses, simples et réalisables dans chaque milieu scolaire. Ces bonnes habitudes constituent dès lors la première étape essentielle dans le contrôle d'accès et pour la rédaction d'un plan de sécurité. Il s'agit ici tant de l'introduction de procédures, telles que le signalement des visiteurs, les procédures de fermeture des portes, que de la prise de responsabilités à tous les niveaux. [5]

1.4.4 Mesures architecturales et mécaniques

Les mesures de sécurisation architecturales et mécaniques constituent un obstacle supplémentaire pour les cambrioleurs. Ils réduisent les risques que ces derniers puissent accéder au bâtiment sans être vus ou entendus. Soulignons également que la sécurisation d'un bâtiment ne sera optimale que si l'on élimine tout maillon faible. Sécuriser uniquement l'entrée principale, mais pas l'entrée latérale, ne suffit donc pas. [5]

1.4.5 Politique relative aux portes

Dans une école maternelle, il est parfois indispensable que les portes restent fermées à tout moment. Les collaborateurs de l'école doivent être sensibilisés en ce sens. Dans les grandes structures tel qu'une école maternelle, il est possible, pour des raisons pratiques, de laisser l'entrée principale ouverte pendant les heures de grande affluence (entre 7 et 8h, par exemple). Dans ce cas, il importe de prévoir du personnel à la porte, chargé de vérifier qui pénètre dans le bâtiment.

1.4.6 Les mesures électroniques

Adopter des mesures organisationnelles et architecturales permet de limiter considérablement les risques d'incidents liés à l'accès de l'école. En optant pour des mesures électroniques, ces risques pourront être réduits davantage. La sécurisation électronique est complémentaire aux autres mesures et ne doit donc pas s'envisager seule.

Ces mesures ne permettent pas en soi d'empêcher l'accès non autorisé, mais produisent un effet de dissuasion et d'avertissement. C'est la raison pour laquelle les mesures électroniques ne peuvent être envisagées indépendamment de la sécurisation organisationnelle et physique. [4]

Par rapport aux menaces et aux mesures sécuritaires relevées ci-haut les écoles en RDC doivent mettre une politique commune dans la sécurisation des élèves ainsi que de personnes qui prennent soins de ses enfants.

1.5 Plan de sécurité des écoles maternelles

Ce plan concerne beaucoup plus les écoles maternelles ou nous y trouvons de jeunes enfants qui sont toujours accompagnés par un membre de famille le matin et retiré à la sortie par la même personne ou une personne de la famille.

Prendre soins de la sécurité des enfants commence de la maison les écoles doivent instruire les parents et les parents à leurs tours feront pareil avec leurs enfants cela évitera les dangers et va permettre un bon déroulement des activités aux seins des écoles.

Les plans à suivre pour écoles maternelles:

- Accueil des élèves par un adulte
- Dispositif de sécurité
- Affichage de consigne de sécurité
- Contrôle visuel de sac avant d'entrer dans l'établissement
- "Pas d'attroupement devant les établissements
- Vérification des identités de personnes extérieures

Après l'étude sur la sécurité ainsi que des menaces qui tournent au tour de nos écoles nous avons proposé un plan pour remédier à cela nous allons maintenant détailler les fonctionnements des systèmes actuels dans les écoles maternelles.

I.6 Description du système existant

1.6.1 Sources d'information

Pour arriver à décrire réellement les fonctionnements dans les écoles maternelles dans la ville de Lubumbashi nous avons eu à faire de visites dans différentes écoles pour s'acquérir de la situation, nous sommes passés dans quatre écoles dans différentes commune pour notre échantillons ; nous sommes passés dans les écoles suivantes :

- L'école Sacre Cœur commune de la RUASHI, L'école Saint Michel (Tuendelee) commune de LUBUMBASHI, L'école Maternelle Rafiki Commune de KATUBA, les Amis d'annuarite commune de KAMALONDO,

Nous avons essayé de mettre ensemble les informations reçues sur les fonctionnements dans la gestion des enfants nous avons constaté qu'il était presque identique mais avec quelques différence près selon les écoles mais complètement manuel.

1.6.2. Fonctionnement du système existant

1.6.2.1 Processus d'inscription

Le système qui existe actuellement dans les écoles visitées, le fonctionnement est manuel, les écoles procèdes de la manière suivante, pendant la période de campagne d'inscription, les écoles prennent les identités des enfants (nom, post nom, prénom, date de naissance, sa classe ainsi que sa photo) et quelques informations des parents (nom, post nom, prénom et le numéro), le numéro permettra à l'école d'entrer en contact avec les parents en cas de problème avec l'enfant (maladie, accident qui pourra survenir pendant que l'enfant est à la charge de l'école). Les informations de l'enfant qui l'école détiendra seront inscrites sur une carte papier (macaron) qui permettra d'identifier l'enfant pendant la période de cours.

1.6.2.2 Procédure de retrait des enfants

Pour récupérer un enfant, la manière de procéder est différentes d'une école à l'autre pour certaines écoles il y a un agent de sécurité qui se charge du contrôle des enfants ainsi que de retraits et dans d'autres écoles c'est la maitresse qui garde les enfants jusqu'à l'arrivée du tuteur ou parent des enfants.

➤ Cas d'un agent de sécurité

Dans les écoles ou c'est un agent de sécurité qui est chargé du retrait et du contrôle des enfants, à la sortie de classe tous les enfants (élèves) se dirige vers la salle d'attente commune accompagner par leurs maitresse respectifs. Les enfants doivent attendre leurs parents dans la salle d'attente sous la supervision de l'agent de sécurité et quand un parent, un tuteur ou une autre personne délégué par les responsable de l'enfant arrive à l'école il présente la carte (macaron) à l'agent qui identifie l'enfant et l'agent à son tour vérifie la

carte et appelle l'enfant en question et le met à la disposition de la personne qui est venu le chercher.

Pour les gens qui viennent souvent récupérer l'enfant même sans carte, si l'agent les reconnaît et donne l'enfant à la personne, dans le cas d'oubli l'agent fait la même chose pour les visages qui lui sont familiers et pour les autres qui oublient la carte et que l'agent ne les reconnaît il appelle les parents de l'enfant (élève) pour une vérification.

➤ Cas de maîtresse

Dans les écoles où c'est la maîtresse qui s'occupe de ses élèves la maîtresse est obligée de rester à l'école jusqu'à ce que le dernier élève de sa classe soit libéré, quand les responsables de l'enfant viennent le chercher la maîtresse vérifie la carte et libère l'enfant si c'est un parent ou un autre membre de famille avec l'habitude la maîtresse libère l'enfant. Souvent les maîtresses si elle est occupée ou indisponible elle laisse ses élèves dans une autre classe avec une autre maîtresse pour surveiller les enfants.

1.7 Menace

Nous avons plusieurs menaces liées à ce mode de fonctionnement comme la vérification est humaine l'agent peut se fatiguer de s'assurer du visage de la personne et ce qui va le préoccuper c'est juste avoir la carte et on donne l'enfant, cela est un problème sérieux dans le cas où la personne qui prend l'enfant n'est pas la bonne et nous sommes confrontés à plusieurs menaces :

1.7.1 Menaces liées au système

1.7.1.1 L'accès de personnes extérieures dans la cour de l'école

Manque de contrôle d'accès des personnes extérieures, à n'importe quelles heures les personnes extérieures peuvent entrer dans la cour de l'école, peuvent facilement tromper la vigilance de la sentinelle pour diverses raisons, les écoles doivent veiller sur cela.

1.7.1.2 Vérification des identités de personnes extérieures

Pour la vérification des identités des gens qui sont censés récupérer les enfants la certitude de la personne qui récupère l'enfant est faible à cause de diverses formes de mensonge :

- La personne qui falsifie la carte
- Une personne malintentionnée qui ment avoir perdu la carte
- La personne qui ramasse le macaron de l'enfant

La personne qui ramasse le macaron de l'enfant

Une personne qui n'est pas malintentionné peut ramasser la carte par hasard si la famille l'a égaré est faire du chantage aux parent en demandant de l'argent, de grande somme et il peut créer un mensonge pour convaincre les parents de l'enfant de son histoire fondée.

Ces personne arrivent à convaincre la sécurité de plusieurs manière, humains que nous sommes la sécurité peut accorder le bénéfice du doute à la personne et peut facilement donner l'enfant ; Les parents ne seront pas informer parce qu'il n'y a pas de mesure sécuritaire pour gérer ces genre de situation ou pour notifier les parents à chaque fois que l'enfant est retiré,

1.7.2 Menace du à l'indisponibilité de parents

Les parents avec leurs indisponibilités demande à quiconque qui passe vers l'école donne la carte pour retirer l'enfant, l'école avec cette confiance donne l'enfant mais on ne sait pas quand la personne mal intentionnée viendra.

1.7.3 Menaces liées aux perturbations de l'environnement

Trouble venant de l'extérieur pour les manifestations politiques par exemple les gens peuvent fuir et se cacher à l'endroit le plus proche et si c'est l'école les personnes mal intentionnées qui aurait occasionné cela peuvent profiter de l'occasion et faire leur coup.

1.8 Critique du système

Nous avons détaillé la manière dont les choses se passent actuellement dans les écoles, comme toute chose il y a de points négatifs et de points positifs le système existant relève beaucoup de points négatifs que positifs

1.8.1 Point fort

- Avec le système actuel les écoles n'ont pas besoins d'investir pour faire une gestion,
- fonctionnement est manuel et moins couteux
- Un système basé sur la confiance

1.8.2 Point faible

Nous allons ressortir quelques points négatifs du système actuel et cela qui nous a poussés à faire notre étude

- La certitude de celui qui prend l'enfant n'est pas garanti parce que quiconque a la carte peut venir prendre l'enfant l'école n'arrive pas à identifier les personnes qui récupère les enfants.
- L'habitude de donner les enfants même aux gens qui non pas de carte de fois l'agent ne mentionne même pas l'heure du retrait le nom de la personne étant humain il peut se fatiguer et oublier à cause de ça, les statistiques ne seront pas vrai et en cas de problème l'école ne saura pas se justifier parce que elle va manquer de preuve
- Pour les maitresses qui laissent leurs élèves chez d'autres maitresses l'heure du retrait n'est pas souvent mentionnée
- Le fait juste de reconnaître la personne même sans la carte l'enfant est libère cela cause un problème de gestion des enfants parce que nous ne savons pas qui a pris l'enfant à quelle heure a été pris cela pose de sérieux problème.
- parce que la reconnaissance de personnes se juste regarder la personne et puis s'imaginé si c'est la personne qui vient souvent prendre l'enfant dans cas contraire l'école appel les parents pour une vérification (si il y a une foule l'agent peut être débordé et donner l'enfant à n'importe qui a la carte (macaron) identifiant l'enfant) les enfants se cafouillent et certains des enfants se faufilent dans la foule et se trouvent à l'extérieur de la cour.

1.9 Orientation

En tant que concepteur, l'étude préalable conduit à mieux comprendre le problème, à partir des objectifs globaux fixés au départ de l'étude, et de prendre en compte le bilan critique de l'existant ainsi que les besoins exprimés par les utilisateurs dans le système d'information en place. Ces observations vont permettre de définir de nouvelles orientations pour la mise en place du système futur.

Cela amènera à dégager une solution de synthèse qui devra prendre en compte des contraintes organisationnelles, techniques, économiques, et traduire sous forme concrète les objectifs à atteindre.

a. Une solution manuelle

C'est une solution non informatisée qui est une amélioration de l'existant nous proposons :

- Celui qui prend l'enfant doit laisser ses identités et signer pour confirmer le retrait

Avantages

- Un système moins coûteux

Inconvénient

- Cette solution ne résout pas le problème de certitude de la personne qui récupère l'enfant parce que n'importe qui peut toujours passer et laisser ses identités, voir même laisser les fausses identités pour récupérer l'enfant, nous nous rendons compte que l'enfant est toujours en insécurité.
- Très manuelle pour faire les statistiques concernant la gestion des enfants

b. Une solution informatique

Pour répondre complètement à ces inquiétude nous pensons à un système d'identification automatique à l'aide de carte à puce pour permettre l'identification des personnes qui commencerons a passé à l'école pour récupérer l'enfant.

Ou nous aurons une carte à puce, un lecteur de carte avec une partie serveur pour le traitement cette solution permettra d'enlever l'incertitude de la personne qui récupère l'enfant.

1.10 Conclusion partielle

Dans ce chapitre il était question de faire une étude approfondie sur les aspects sécuritaires et risques auxquels les écoles font face ainsi que l'étude de l'existant, le fonctionnement dans les écoles concernant le retrait des enfants. Nous avons aussi fait une observation sur les pistes de solution qui pouvaient exister manuellement tant qu'information et nous avons opté pour une solution informatique qui présente beaucoup plus d'avantage.

Le chapitre précédent nous donne le squelette de notre travail d'une manière logique ce qui sera notre solution.

CHAPITRE 2 : SPECIFICATION DE BESOIN ET CONCEPTION LOGIQUE DE LA SOLUTION

2.1 Introduction partielle

Le chapitre précédant décrit le système existant, et ce dernier relève les différentes menaces auxquels les écoles sont confrontées, sur base de ces menaces nous allons ressortir les besoins fonctionnels ainsi que le besoins non fonctionnel, nous allons analyser ces besoins et après analyse nous allons ressortir les fonctionnalités du système envisagé ainsi que les mécanismes à mettre en place pour son fonctionnement.

Tout tourne autour de l'identification de la personne qui récupère l'enfant

Nous pensons que, il peut y avoir plusieurs solutions qui pourrons permettre la reconnaissance des personnes qui viennent prendre les enfants, cela pour renforcer la sécurité et améliorer la gestion des écoles,

Après l'étude et analyse du système existant, sur base de failles que présente le système actuel nous voulons généraliser notre travail sur toute l'étendue de la ville pour améliorer et renforcer la sécurité des enfants dans les écoles, nous avons pensé de mettre en place un système automatique dans la gestion des enfants pour ce qui concerne le retrait,

La mise en place de ce système est conditionné par : une inscription et une présence automatique, Le système va remplacer le macaron¹ par de carte à puce sur lesquelles nous allons inscrire les informations concernant les élèves.

¹ Macaron : les cartes papiers

2.2 Analyse et spécification de besoin

Nous allons faire une analyse des besoins des écoles par rapport aux menaces et risques auxquels les écoles sont confrontées citées dans le chapitre précédent et aussi pour améliorer certaines choses nous allons ressortir les besoins fonctionnels et non fonctionnels qui feront l'objet même de notre travail.

a. Définition

Nécessité ou désir éprouvé par un utilisateur (*norme NF X50-150*)

2.3 Formulation du besoin

Pour ce qui concerne l'analyse nous allons procéder par quelques questions pour pouvoir ressortir les besoins ainsi que les différents acteurs qui entreront en jeu pour l'utilisation du système²,

Les questions :

A qui sert notre solution ?

Nous avons à ce niveau deux catégories de personnes l'utilisateur et l'utilisateur pour notre cas l'utilisateur c'est les responsables de l'école nous citons le directeur, les agents de sécurité de l'école et l'utilisateur nous avons les personnes externes à l'école.

A quoi sert notre solution ?

Notre solution doit répondre aux inquiétudes des parents pour la sécurité de leurs enfants ainsi qu'aux problèmes de gestion pour les écoles, la solution doit :

- S'assurer de la personne qui prend l'enfant si elle est habilitée à le faire
- Faire les statuts de retrait des enfants nous voyant l'heure et la personne qui récupère l'enfant
- Faire une inscription des enfants (élèves)
- Faire une présence automatique des élèves pour faciliter le retrait

Le quoi nous permet de ressortir les **besoins fonctionnels** et nous avons ressorti les besoins principaux il s'agit de la sécurité des enfants et de la gestion d'élève à l'école.

² Système : solution

Quelles sont les contraintes de notre solution ?

Après les questions nous avons pu formuler les besoins des écoles

Le besoin existe à cause d'une mauvaise gestion et un manque d'attention lors de la sortie des enfants dans les écoles maternelles c'est pourquoi nous voulons palier à ces problèmes en renforçant la sécurité avec une solution qui permettra aux écoles de faire des statistiques des enfants, s'assurer des personnes qui passent prendre les enfants, bref une bonne gestion garantie pour les élèves, pour ça il y a quelques contraintes qu'il faudrait palier qui nous ressort les besoins non fonctionnels ou contraint

2.3.1 Besoin non fonctionnel

Pour une gestion réussie les écoles doivent veiller sur tous les détails possible. Les écoles doivent mettre en place certains mécanismes qui permettent un bon fonctionnement de notre système nous citons

- Mise en place d'un petit réseau
- L'école doit être en clôture et avoir une seule sortie pour les enfants
- Les écoles doivent disposer d'un nombre important d'agents de sécurité à la sortie des enfants

2.3.2 Besoin fonctionnel

Après analyse de besoin non fonctionnel nous pensons que, pour la réussite de notre système les mécanismes doivent être informatisés, nous allons ressortir les besoins fonctionnels, pour une bonne compréhension de notre travail nous allons procéder par la suite avec les diagrammes et schémas.

La solution envisagée nous donne 3 blocs importants pour sa réalisation :

- Inscrire les élèves
- Faire la présence automatiquement
- Faire le retrait de l'enfant moyennant la carte

2.4 Modélisation du système envisagé

Nous avons modélisé les grandes fonctionnalités de notre travail avec un diagramme UML³ de cas d'utilisation⁴ (CU) figure 2.1, ce diagramme nous montre l'interaction de personnes externes au système et le système en question, nous avons aussi les acteurs qui entrent en jeu avec pour l'utilisation de notre système.

³ UML Langage de Modélisation Unifié

⁴ CU cas d'utilisation

2.4.1 Diagramme de cas d'utilisation

Dans notre diagramme nous y trouvons 3 cas d'utilisation important nous citons :

- Inscrire enfant
- Faire la présence
- Signaler retrait

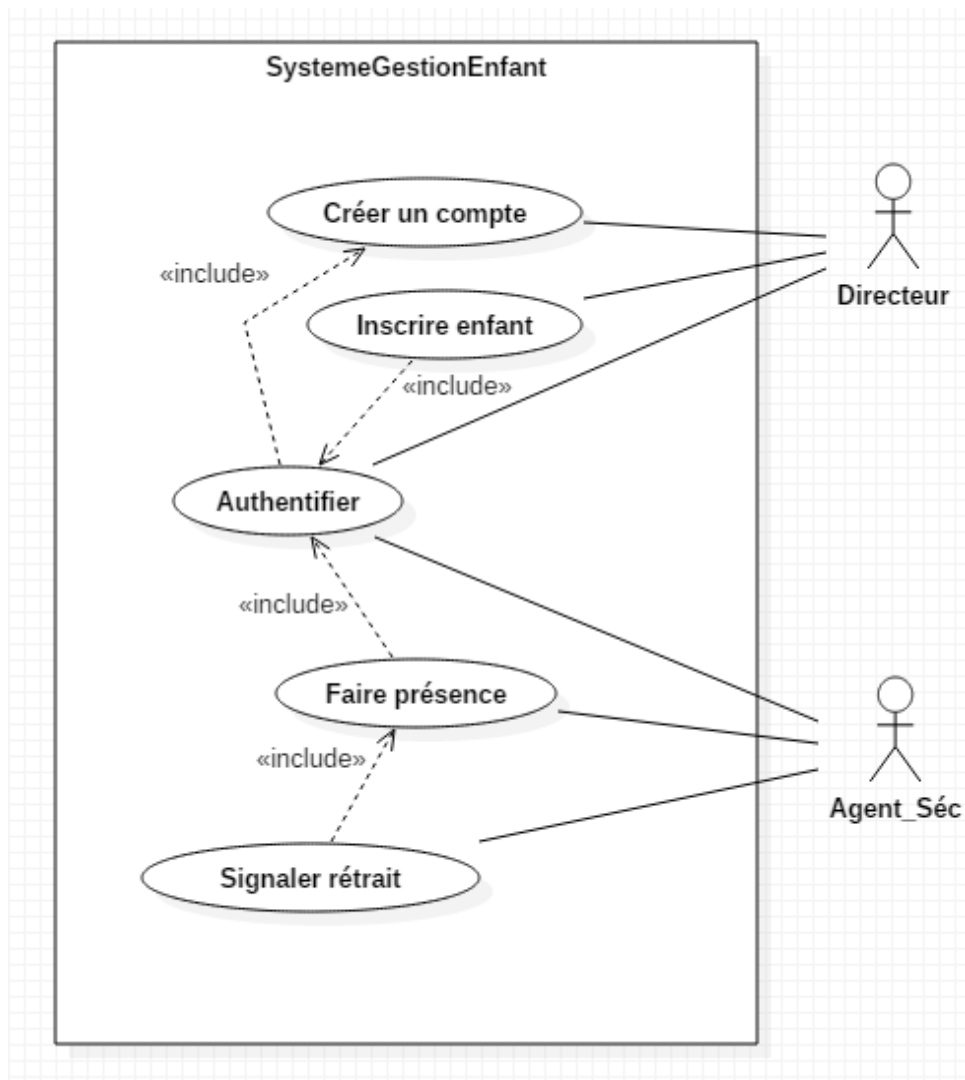


Figure 2. 1 Diagramme de cas d'utilisation du système envisagé

Dans notre diagramme chaque cas d'utilisation détermine une fonctionnalité qui sera détaillés dans la suite de notre travail.

2.4.2 Diagramme de séquence

L'objectif du diagramme de séquence est de représenter les interactions entre les objets en mettant l'accent sur la chronologie des échanges.

Nous allons modéliser toutes les séquences possibles de notre travail : création de compte, inscription, authentification, présence, retrait

2.4.2.1 Inscription

Pour ce qui concerne l'inscription ce n'est pas n'importe qui va commencer à le faire, alors nous avons pensé à mettre certaines restrictions au niveau de notre système seul le directeur de l'école peut faire l'inscription cela nous pousse à procéder de la manière suivante il faut d'abord avoir un compte administrateur donc nous aurons :

- La création des comptes et
- L'authentification

Les diagrammes de séquences suivantes nous montreront les processus possibles de la création de compte jusqu'à l'inscription des élèves.

2.4.2.2 Création d'un compte

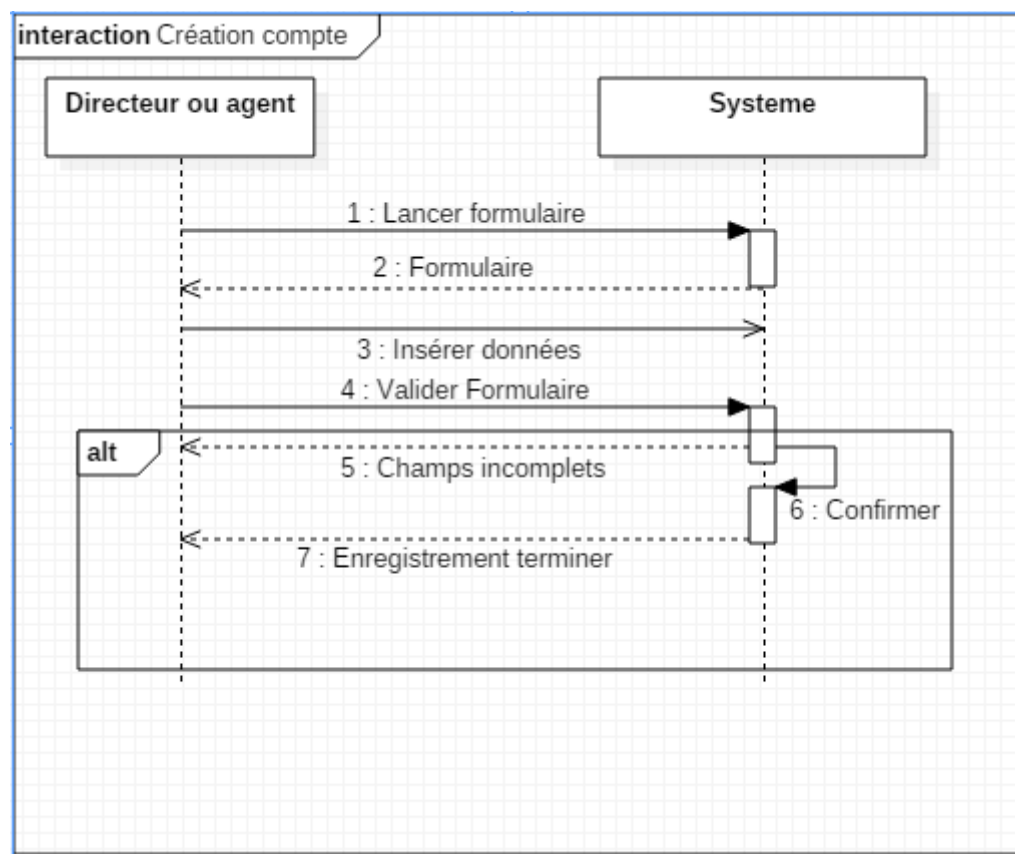


Figure 2. 2 Diagramme de séquence montrant le processus de création de compte

Le diagramme précédant nous montre les étapes possibles de création d'un compte, et pour accéder à un compte l'administrateur doit entrer son login et mot de passe pour s'authentifier, la séquence suivante nous montrera ce processus figure 2.3.

2.4.2.3 Authentification du directeur ou agent de sécurité

Le directeur ou l'agent de sécurité doivent s'authentifier pour avoir accès à leurs compte respectif avec de niveau de restriction différent seul le directeur peut avoir pouvoir d'agir sur le système entier.

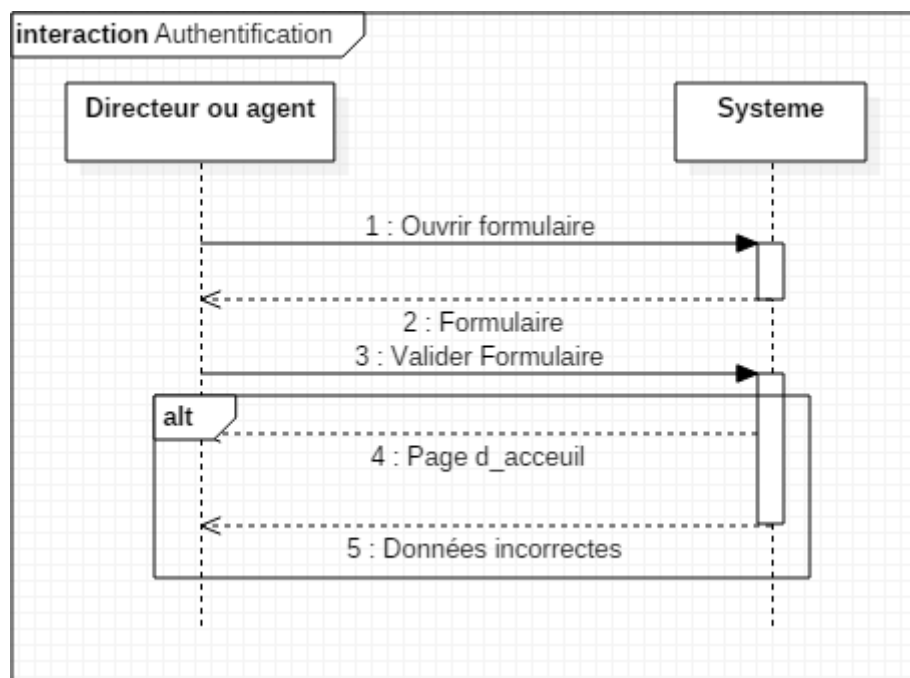


Figure 2. 3 processus d'authentification

2.4.2.4 Inscription de l'enfant

Pour inscrire un élève le directeur doit d'abord s'authentifier, la figure 2.4 montre le processus d'inscription.

Nous aurons un formulaire d'inscription qui permettra à l'administrateur (Directeur) d'inscrire les élèves, les processus normal : le directeur prend les identités des élèves fournies par le parent auxquelles on annexe une photo, les identités de parents ainsi que de personnes qui commenceront à passer prendre l'enfant en cas d'indisponibilité de parents.

À l'inscription un matricule est généré, il est constitué de chaque première lettre du nom, post nom et le prénom de l'élève on y ajoute l'année d'inscription et son numéro

sur la liste pour que ce matricule puisse identifier d'une manière unique un élève et ce dernier sera inscrit sur la carte à puce⁵.

La carte à puce sera utilisée pour les opérations de présence et retrait des élèves pendant la période de cours.

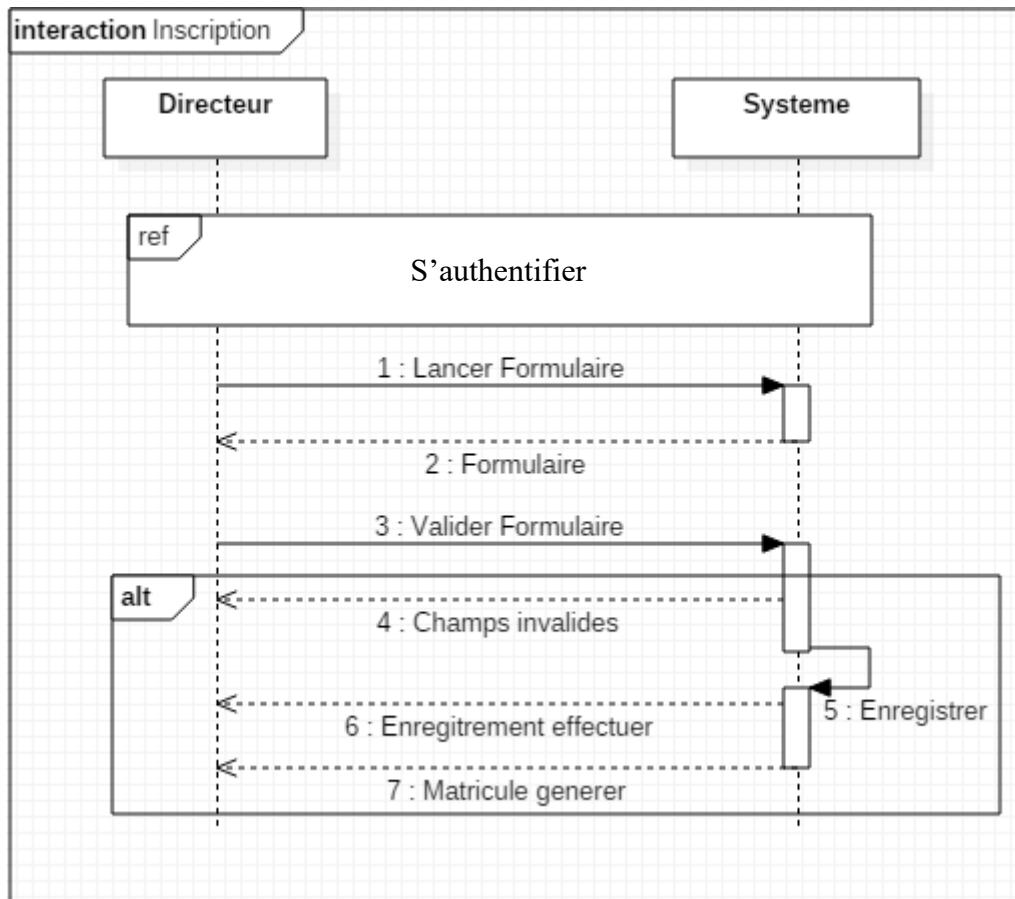


Figure 2. 4 Diagramme de séquence pour l'inscription d'un élève

2.4.2.5 Présence de l'enfant

Le matin le parent arrive à l'école avec l'enfant avant que l'enfant n'entre dans la cour de l'école, l'agent de sécurité doit faire une présence, il scanne la carte à l'aide d'un lecteur de carte à puce et ce dernier permet de récupérer les informations de la carte identifiant l'enfant et les envoyées du côté serveur pour un traitement informatique et la présence sera faite après la comparaison des informations issues de la carte et ceux enregistrés dans notre système de gestion de base de données reçues à l'inscription.

Avec notre système de gestion de base de données (SGBD)⁶ qui contient toutes les identités des élèves. Avec notre carte à puce sur laquelle l'on a inscrit le matricule de l'élève, qui sera lu par un lecteur de carte à puce qui sera géré par les dirigeants la figure 2.5 détaille cela.

⁵ Carte à puce : une carte qui permettra l'identification de l'enfant ...

⁶ SGBD : système de gestion de base de données

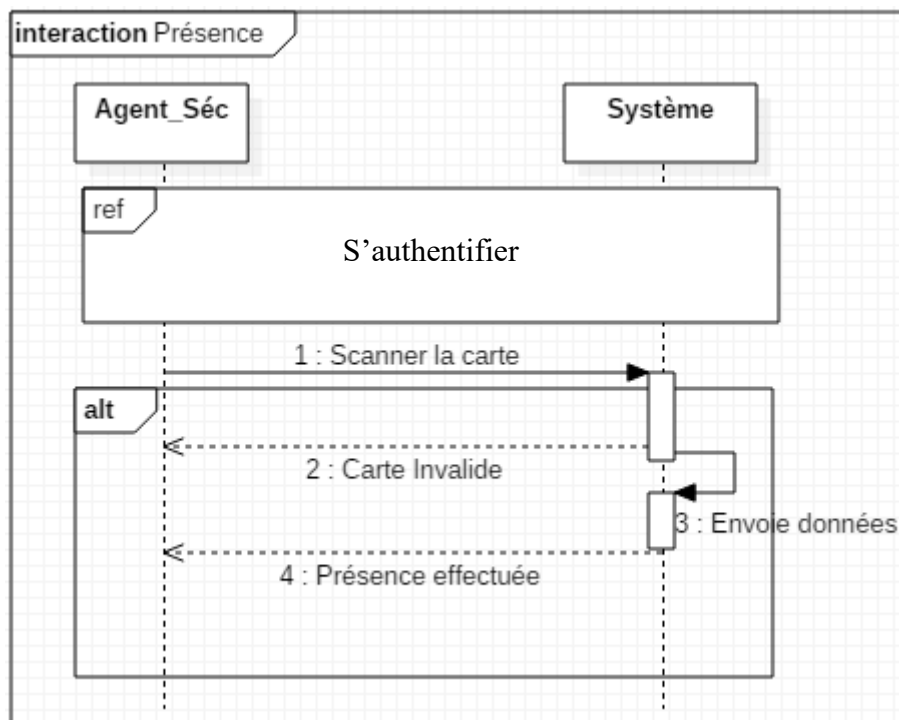


Figure 2. 5 Diagramme de séquence pour la présence des élèves

2.4.2.6 Retrait de l'enfant

Pour ce qui concerne le retrait, à ce stade l'école devra être vigilante parce que l'enfant est à sa charge la présence effectué le matin justifie que l'école à bien reçu l'enfant.

Nous avons fait la présence c'est-à-dire que l'enfant est bel et bien dans la cour de l'école, et maintenant elle devra veiller sur les personnes qui viennent prendre les enfants et aussi veiller aux mouvements des enfants pendant la sortie qui cherchent à tout prix sortir pour rentrer à la maison, dans le cafouillage que les enfants ne sortent pas de la cour sans être aperçu, pour éviter les problèmes avec les parents en cas de disparition d'un enfant.

Le retrait des enfants se passera de la manière suivante figure 2.6 nous montres les étapes possible concernant le retrait d'un élève,

Le parent ou un autre membre de la famille qui passera à l'école pour récupérer l'enfant, il doit se munir d'une carte en plastique sur laquelle sera collé notre puce qui contient le matricule de l'enfant pour l'identifier, la carte est donnée à la personne chargée de livrer les enfants (l'agent de sécurité), il va scanner cette carte avec le lecteur de carte de l'école, après lecture de la carte le lecteur va prendre les informations qui se trouve sur la carte et les envoyées via une connexion câblée au ou sans fil du côté serveur pour un traitement et cela consistera à rechercher une correspondance entre les informations de la carte et celle de la base de données une fois qu'il y a correspondance d'informations

une page sera renvoyer à l'interface utilisateur qui contiendra les identités de l'enfant et des personnes habilités à prendre l'enfant ainsi l'agent doit confirmer la personne et valider le retrait après validation du retrait les parents seront notifier du retrait de leur enfant soit par le réseau cellulaire avec un message ou soit par un système de messagerie.

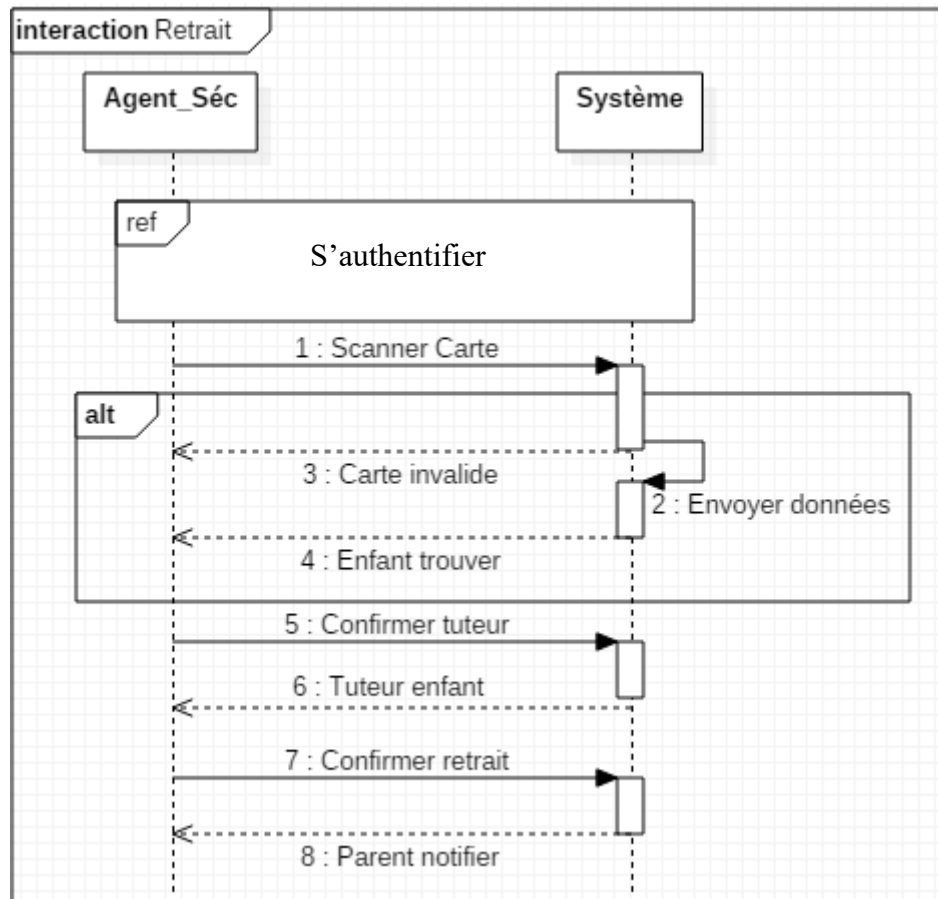


Figure 2. 6 Diagramme de séquence pour le retrait d'un élève

Après tous les processus cités précédemment on se rend compte que après inscription nous aurons les informations des enfants ainsi que de personnes qui commencerons à passer pour prendre l'enfant, bien que nous aurons les informations de parents ou tuteurs nous sommes appelé à vérifier cela en posant quelques questions de sécurité à la personne qui passera pour être sûr à 100% que l'enfant est parti dans des bonnes mains.

Après toutes ces séquences nous allons donner un diagramme qui montre d'une manière explicite le fonctionnement global du système ainsi que tous les acteurs qui entre en jeu.

2.4.5 Diagramme d'activé

Le diagramme d'activité décrit le déroulement des activités d'une catégorie d'objet. Il décrit le déroulement d'un cas d'utilisation.

2.4.5.1 De l'inscription à la présence

Les figures 2.7 et 2.8 décrivent les cas d'utilisation d'une manière détaillée avec tous les acteurs qui entre dans l'interaction avec le système

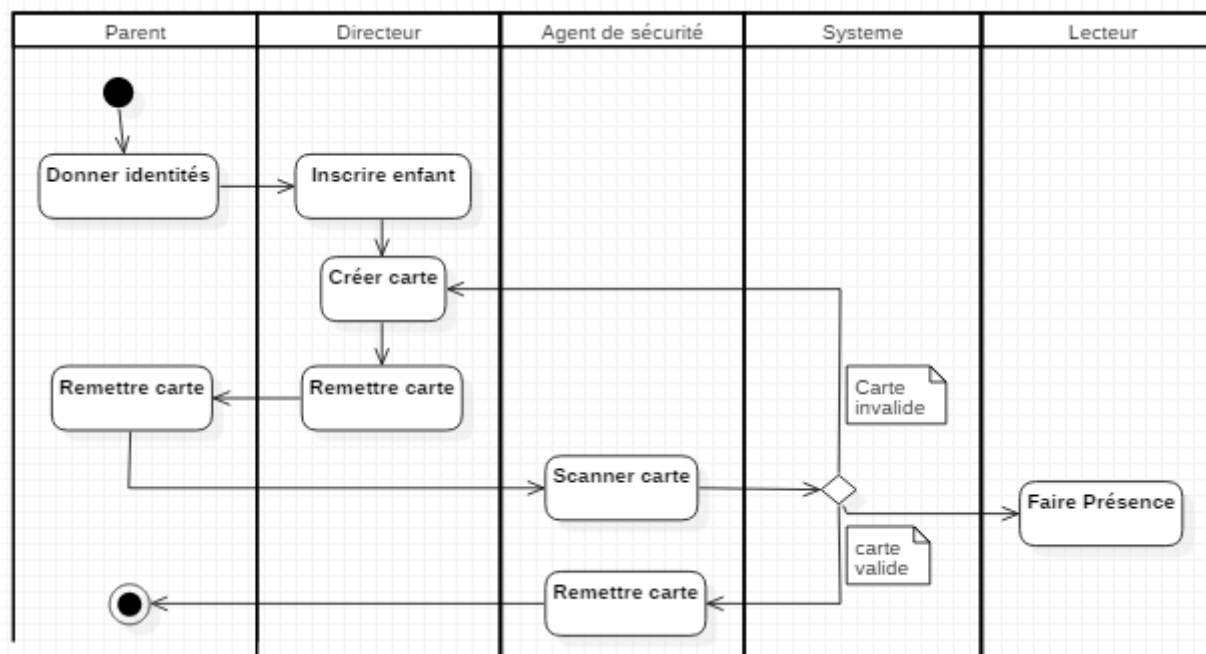


Figure 2. 7 Diagramme d'activité de l'inscription à la présence

2.4.5.2 Le retrait de l'enfant

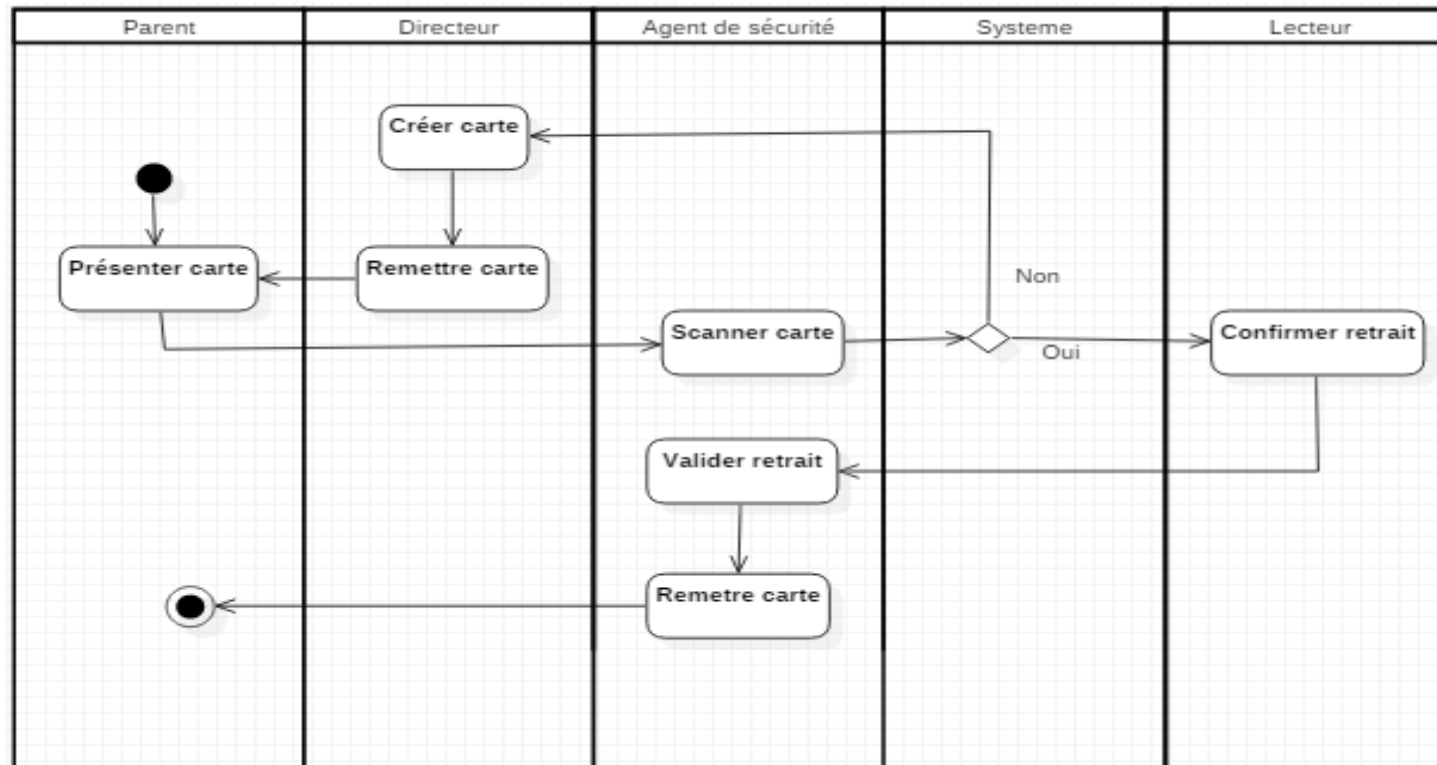


Figure 2. 8. Diagramme d'activité pour le retrait

2.5 Conception du système de gestion de base de données

Nous allons donner un modèle de base de données avec différentes tables et montrés la façon dont les tables communiquent.

2.5.1 Model logique de données

Nous avons 3 tables principales :

➤ Enfant

Dans cette table nous y trouvons les identités des enfants, tous identifié de manière unique avec un matricule.

➤ Tuteur

Cette table contient les identités de tous les tuteurs et ils sont relire à leurs enfant par le matricule.

➤ Statistique

La table statistique montre les activités des enfants et des tuteurs

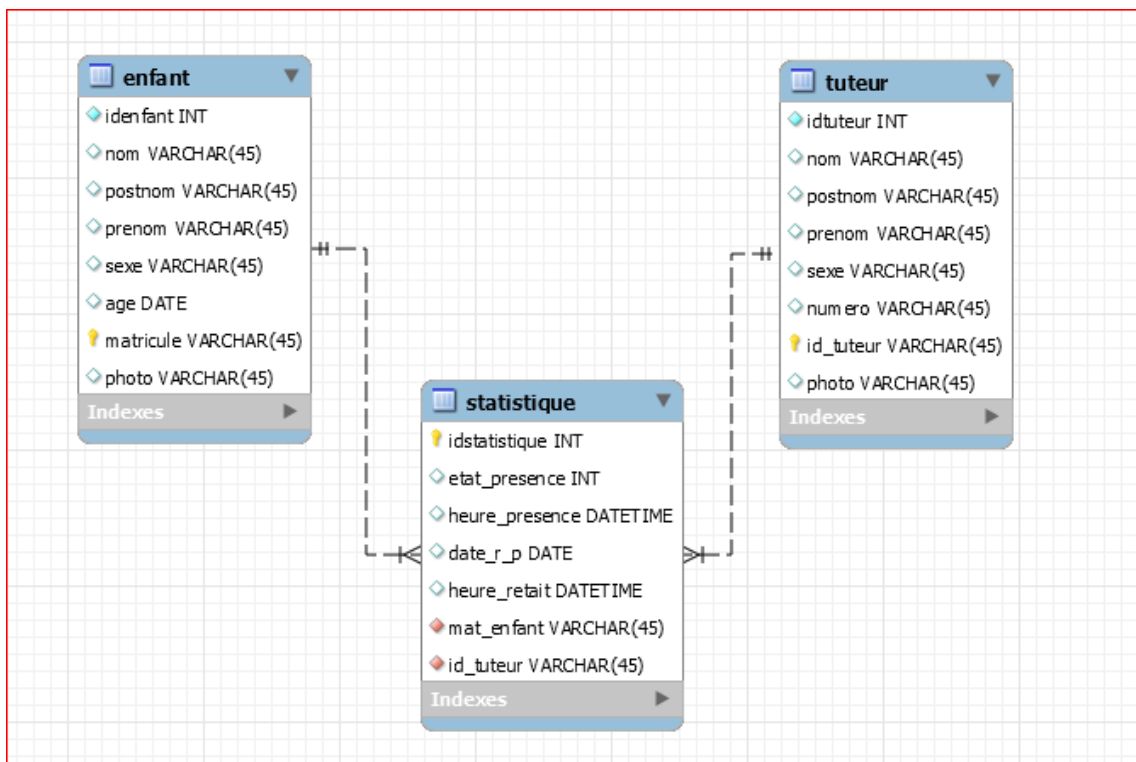


Figure 2. 9 model logique de données

Conclusion partielle

Dans ce chapitre il était question de faire l'analyse et spécification de besoin sur base de quels nous avons pu ressortir le vrai problème et les difficultés des écoles, afin de pouvoir donner une solution nous avons pensé à une solution d'identification numérique et nous avons modélisé la solution pour une bonne compréhension et les parties suivantes seront là pour mettre l'accent sur la conception dite logique du présent chapitre.

Chapitre 3 : ETUDE TECHNOLOGIQUE ET CONCEPTION PHYSIQUE DE LA SOLUTION

3.1 Introduction partielle

Par rapport aux besoins fonctionnels et non fonctionnels ressortis dans notre conception logique, cela nous pousse à faire une étude approfondie sur les différentes technologies d'identification, les outils matériels ainsi que logiciel qui vont interagir avec la technologie d'identification qui sera choisie.

Nous voulons identifier une personne une question se pose :

Comment arriver à identifier de manière unique une personne ?

Nous aurons besoins d'une technologie d'identification adaptée à notre problème qui est d'identifier la personne qui vient récupérer l'enfant, plusieurs technologies d'identification s'offre à nous, voilà pourquoi nous allons faire la découverte de différentes technologies et nous allons ressortir leurs points forts ainsi que leurs points faible et qui nous permettrons de faire un choix pour une technologie qui sera adapter à notre problème.

Une fois la technologie choix nous aurons besoin des outils informatiques pour faire le traitement et la communication avec notre technologie choisie.

3.2 Raison de s'authentifier

Pour ce qui concerne l'authentification ou l'identification, nous avons trois niveaux de preuve à savoir

- Ce que l'on possède (carte, badge, document) ;
- Ce que l'on sait (un nom, un mot de passe) ;
- Ce que l'on est (empreinte digitales, main, visage)

Les trois niveaux de preuve sont exploités avec différentes technologie

3.3 Les technologies d'identification

Nous avons plusieurs technologies d'identification chacune avec de particularités sur lesquelles nous sommes appelé à faire un choix, nous les distinguons par leur manière d'identifier les personnes ou les choses :

- Par la biométrie
- Par les codes

3.4 Identification par la biométrie

3.3.1 Contexte d'utilisation de la biométrie

La biométrie est utilisée pour différentes raisons :

- Supprimer le doute sur l'identification
- Supprimer les mots de passe
- Sécuriser les données confidentielles et les stations de travail

Le but de la biométrie dans le contrôle d'accès est de gérer les accès physiques ou logiques afin d'accroître la sécurisation des accès à des locaux de tous types mais aussi sécuriser l'accès à des stations informatiques et aux dossiers et fichiers présents sur ces dernières. La biométrie commence à être utilisée également afin d'authentifier un utilisateur lors de transactions bancaires pour sécuriser les paiements via des terminaux physiques ou encore pour des paiements en ligne.

3.3.2. Famille de système de biométrie

Il existe de nombreux systèmes biométriques pour le contrôle d'accès que nous pouvons séparer en deux grandes familles : Avec contact et sans contact physique.

3.3.2.1. La biométrie avec contact

La biométrie avec contact physique est très répandue. Elle comprend la reconnaissance de l'empreinte digitale, de la morphologie de la main ou encore en mode multimodal avec analyse combinée et simultanée de l'empreinte digitale et du réseau veineux du doigt. [6]

Dans le monde, l'une des technologies les plus utilisées est la biométrie via l'empreinte digitale. Autant au niveau du contrôle des individus (passeport, carte d'identité et permis de conduire biométriques), qu'au niveau du contrôle d'accès.

a. Empreinte digitale

Une empreinte digitale est le dessin formé par les lignes de la peau des doigts, des paumes des mains, des orteils ou de la plante des pieds. Ce dessin se forme durant la période fœtale. Il existe deux types d'empreintes : l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (saleté, sueur ou autre résidu déposé sur un objet).

Elles sont uniques et immuables, elles ne se modifient donc pas au cours du temps (sauf par accident comme une brûlure par exemple). La probabilité de trouver deux empreintes digitales similaires est de 1 sur 10 puissances 24. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches mais pas identiques.

Elles sont composées, de façon rudimentaire, de terminaisons en crêtes, soit le point où la crête s'arrête, et de bifurcations, soit le point où la crête se divise en deux. Le noyau est le point intérieur, situé en général au milieu de l'empreinte. Il sert souvent de point de repère pour situer les autres minuties. [6]

b. Dynamique des frappes au clavier (*keystroke-scan*)

Pour identifier une personne grâce à son style de frappe, la frappologie mesure des paramètres comme le temps de pression sur chaque touche, le temps de relâchement, le temps de vol entre deux touches ou encore le nombre de doigts utilisés, selon Christophe Rosenberger, professeur à l'ENSICAEN et introducteur de cette discipline en France.

Les frappes au clavier sont influencées par plusieurs choses ; tout d'abord, selon le texte que l'on tape et, de manière plus générale selon sa nature, on aura tendance à modifier sa façon de taper au clavier. C'est d'ailleurs un des moyens utilisés par certaines attaques (*timing attacks*) pour essayer d'inférer le contenu ou la nature du texte tapé de façon à remonter jusqu'à un mot de passe par exemple. Cette technique de frappologie est assez satisfaisante mais reste néanmoins statistiques. [6]

c. Dynamique des signatures (*signature-scan*)

Ce type de biométrie est à l'heure actuelle peu utilisé mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents électroniques, rapports, contrats...). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc. Bref tout ce qui peut permettre d'identifier une personne de la façon la plus sûre possible quand on utilise une donnée aussi changeante que la signature. [6]

3.3.2.2. La biométrie sans contact

Au niveau des technologies sans contact, il existe des systèmes à reconnaissance faciale, de l'iris et du réseau veineux de la paume de la main. Également depuis 2009, il existe une technologie capable de capturer et de traiter les empreintes digitales des 4 doigts (hors pouce) sans contact, seulement d'un mouvement

a. Reconnaissance de l'iris

L'utilisateur doit fixer l'objectif d'une caméra numérique qui balaie l'iris d'une personne d'une distance de 30 à 60 cm, et acquiert directement son dessin. Elle le compare ensuite à un fichier informatisé d'identification personnelle (les systèmes de comparaison en usage aujourd'hui sont en mesure de fouiller une banque de données à la vitesse de plusieurs millions de codes iridiens par seconde).

Or, l'iris est un organe sensible, sa taille est petite et il est obscurci par les cils, les paupières ou les lentilles de contacts. De plus, elle est variable et les utilisateurs ont tendance à bouger. Il est donc assez difficile d'avoir une bonne image de l'iris, il faut que ce soit rapide, précis et qu'il n'y ait pas de lumière pouvant se refléter sur l'œil.

Pour le traitement numérique, la méthode employée est celle de John Daugman : après la numérisation de l'image de l'œil, le logiciel détermine le centre de la pupille et le contour de l'iris. Puis sur ces deux données le logiciel établit des bandes de tailles égales (la taille varie selon la dilatation de la pupille) pour former un fichier « gabarit »,

à partir de l'analyse de la texture de l'iris. Le fichier formé est un code iridien accompli grâce à l'algorithme de Daugman. [6]

b. Reconnaissance de visage

On peut identifier un individu en fonction de ses caractéristiques faciales en effectuant des mesures : écartement des yeux, arêtes du nez, commissures des lèvres, oreilles, menton. Ces différentes caractéristiques sont analysées par les systèmes de reconnaissance faciale et comparées à une base de données existante. Cette méthode permet d'identifier une personne ou de vérifier une identité.

Le système évolue et l'on peut maintenant reconnaître des visages en mouvement, vu de profil et on peut aussi désormais vieillir un visage. [6]

c. Reconnaissance vocale (*voice-scan*)

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. Ils ne sont en général pas imitables. [6]

3.5 Indentification par les codes

Nous avons plusieurs technologies qui utilisent le code pour identifier une personne ou quelque chose :

- Le code-barres
- La RFID
- Le smart Card

3.5.1 Le code-barres

Code-barres, ou code à barre (CAB), est la représentation d'une donnée numérique ou alphanumérique sous forme d'un symbole constitué de barres et d'espaces dont l'épaisseur varie en fonction de la symbologie utilisée et des données ainsi codées. Il existe des milliers de codes-barres différents ; ceux-ci sont destinés à une lecture automatisée par un capteur électronique, le lecteur de code-barres. [7]

Pour l'impression des codes-barres, les technologies les plus utilisées sont l'impression laser et le transfert thermique.

Identifier des objets simplement à travers l'utilisation de code a toujours été un vrai besoin. Par exemple dans une bibliothèque, un livre comporte un numéro qui lui est unique, le code ISBN, qui permet de l'identifier. Ce code vient en complément du nom de l'auteur, du livre lui-même et de l'éditeur, et est la clé unique permettant d'indexer le livre. Cela permet ainsi de le retrouver facilement et rapidement dans un catalogue.

3.5.1.1. Type de code-barres [8]

On distingue deux types généraux de codes-barres :

- Unidimensionnel (1D) : ces codes sont ceux représentés par une série de lignes parallèles d'épaisseur variable. Leur lecture est unidimensionnelle. Selon la technologie de lecture utilisée, le décodage pourra se faire de façon unidirectionnelle ou bidirectionnelle afin de confirmer le premier décodage.



Figure 3. 1 code barre

- Bidimensionnel (2D) : ces codes utilisent une variété de symboles (rectangles, points, hexagones et autres formes géométriques). Cette forme matricielle permet d'enregistrer davantage d'informations.



Figure 3. 2 code QR

On distingue deux familles de codes 2D :

- Les codes empilés

Il s'agit de codes 1D empilés (Code 16k, PDF417, etc.). Ces codes peuvent aussi être lus par les lecteurs 1D en faisant un balayage du code.

- Les codes bidimensionnels

Il s'agit de codes dont les motifs constituent une forme souvent rectangulaire ou carrée qui ne peuvent être lus que par des technologies de prise de photos.

3.5.1.2. Quelques types de codes-barres unidimensionnels (1D) :

- les codes-barres EAN : EAN 8, EAN 13, Code Universel des Produits (CUP)
- le Code 128
- le 2 parmi 5

3.5.1.3. Quelques types de codes-barres bidimensionnels (2D) :

- le PDF-417 : Portable Data File, code avec une grande capacité de stockage
- le Code 1 : de domaine public, utilisé pour les étiquettes médicales et l'industrie du recyclage
- le Flashcode : spécification issue de DataMatrix

- le MaxiCode : de domaine public, utilisé par United Parcel Service
- le Code QR : Quick Response, conçu pour être décodé rapidement, stocker une grande quantité d'informations et être lu par plusieurs types d'appareils

3.5.1.4 Lecture des codes-barres [8]

Pour décoder un code-barres, il faut un lecteur relié à un ordinateur. Les premières technologies utilisaient le port RS-232, puis l'USB s'est imposé. La lecture se fait le plus souvent grâce à un rayon laser qui permet le déchiffrement des zones claires et sombres, et ainsi de l'information codée.

On appelle *zone de silence* les marges situées autour du code et qui permettent au lecteur de trouver le début et la fin du code.

Il existe 3 types différents de lecteurs de code-barres : les douchettes code-barres, les lecteurs portables de code-barres et les terminaux code-barres autonomes. Chacun d'entre eux correspond à un besoin et à un domaine d'activité spécifique.

- Les douchettes code-barres : sont utilisées principalement dans le domaine médical ainsi que par les petites et grandes surfaces commerciales. Appréciables pour leur rapidité et leur simplicité d'utilisation, les douchettes autotrigger sont connectées à un ordinateur et peuvent lire aussi bien les codes 1D (code-barres linéaires) que 2D (codes plus élaborés tels que les QR code).
- Les lecteurs de code-barres portables sont utilisés régulièrement pour les inventaires en entrepôt et magasin, ou encore les services de poste. Ils sont parfaits pour une utilisation extérieure grâce à leur maniabilité et leur simplicité d'utilisation. Ces lecteurs portatifs peuvent aussi lire aussi bien les codes 2D que 1D.
- Les terminaux code-barres autonomes sont les plus élaborés, en plus de scanner les codes 1D et 2D, ils analysent les données et les transmettent en réseau comme un mini-ordinateur le ferait. Parfaitement adaptés pour l'inventaire, l'audit et contrôle de prix ainsi que le merchandising, ces terminaux laser correspondent aux besoins des commerciaux en magasins, aux gestionnaires de stocks ainsi que les transporteurs.

À l'exception de quelques codes-barres spéciaux (par exemple les codes-barres "presse" de la norme EAN 13), l'information relative au prix d'un produit n'est généralement pas codée directement dans le code-barres. Le prix est en effet stocké dans le fichier interne du magasin. La lecture du code-barres sur une borne-prix est reçue par le terminal du magasin qui en retour renvoie l'information correspondante.

3.5.2. La RFID

RFID fait partie des technologies d'identification automatique, au même titre que la reconnaissance optique de caractères ou de codes barre. Cette technologie permet d'identifier un objet ou une personne, d'en suivre le cheminement et d'en connaître les caractéristiques à distance grâce à une étiquette émettant des ondes radio, attachée ou incorporée à l'objet ou à la personne.

La technologie RFID permet la lecture des étiquettes même sans ligne de vue directe et peut traverser de fines couches de matériaux (peinture, neige, etc.).

3.5.2.1 Principe de fonctionnement de la RFID

Le système d'identification comprend une base et une étiquette (tag, transpondeur) [7]

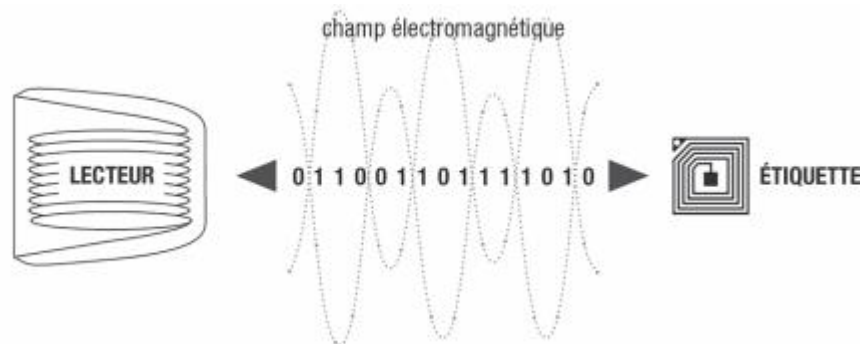


Figure 3. 3 Principe de fonctionnement de la RFID

Tableau 3. 1 Description du processus de fonctionnement de la RFID

1	2	3	4
Le lecteur génère un champ électromagnétique	L'énergie de ce champ est captée par l'antenne de l'étiquette	Cette énergie permet d'activer la puce de l'étiquette	Et la transmission de données en retour vers le lecteur

3.5.2.2 Composants et fonctionnement du système

Une solution complète de la RFID comprend les étiquettes, les lecteurs et un encodeur et l'intergiciel (middleware). Ce dernier permet d'intégrer le flux des données dans le système d'information.

➤ Le tag (étiquette)

Une des méthodes d'identification les plus utilisées est d'abriter un numéro de série ou une suite de données dans une puce (chip) et de relier cette dernière à une petite antenne. Ce couple (puce silicium + antenne) est alors encapsulé dans un support (RFID Tag ou RFID Label). Ces "tag" peuvent alors être incorporés dans des objets ou être collés sur des produits.

Le tout est alors imprimé sur un support pliable, souvent adhésif. Le format des données inscrites sur les étiquettes est standardisé à l'initiative d'EPC Global (Electronic Product Code). [9]

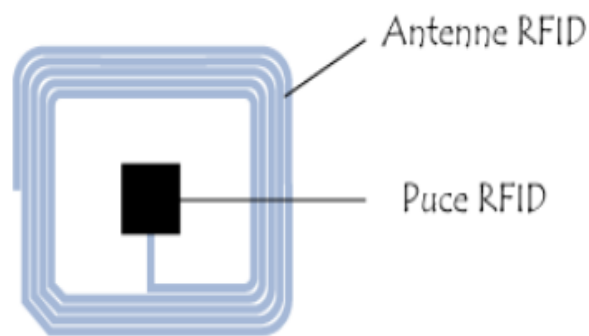


Figure 3. 4 Une étiquette RFID

➤ Le lecteur

Le lecteur/enregistreur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et d'une électronique qui reçoit et décode les informations envoyées par le transpondeur et les envoie au dispositif de collecte des données.

Il ne permet pas seulement de lire les étiquettes RFID, il est à même d'écrire leur contenu. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence et de la transmission des informations qu'elles contiennent (code EPC ou autre, informations d'état, clé cryptographique...) vers le niveau suivant du système (middleware). Cette communication entre le lecteur et l'étiquette s'effectue en quatre temps :

- Le lecteur transmet par radio l'énergie nécessaire à l'activation du tag ;
- Il lance alors une requête interrogeant les étiquettes à proximité ;
- Il écoute les réponses et élimine les doublons ou les collisions entre réponses ;
- Enfin, il transmet les résultats obtenus aux applications concernées.

Il y a une diversité de lecteur de carte RFID cela est fonction de la distance et le besoin, chaque lecteur est adapter à un besoin bien déterminer. [10]

3.5.2.3 Fonctionnement du système RFID

La communication entre le lecteur et l'étiquette s'effectue via les antennes qui équipent l'un et l'autre, ces éléments étant responsables du rayonnement radiofréquence. Les antennes dont dispose le lecteur sont plus ou moins standardisées, mais offrent les mêmes différences que les haut-parleurs d'une chaîne stéréo d'un modèle à l'autre.

La puissance du lecteur est donc à combiner avec l'antenne adéquate, ceci permettant de déterminer la portée optimale de la lecture. Généralement, on distingue quatre modalités :

- Lecture de proximité : entre 10 et 25 cm ;
- Lecture de voisinage : jusqu'à 1 mètre ;
- Lecture à moyenne distance : de 1 à 9 mètres ;
- Lecture longue portée : jusqu'à plusieurs centaines de mètres. [11]

Par ailleurs, le terme de lecteur RFID est en fait une impropriété, puisque ce dernier est également capable d'écrire des informations sur l'étiquette.

Car, si bon nombre d'étiquettes sont en lecture seule (le code qu'elles contiennent ayant été « imprimé » en même temps que l'étiquette elle-même, d'autres contiennent, au-delà du code de base, une zone mémoire pouvant contenir des données variables.

C'est pourquoi des fonctionnalités sont intégrées dans les contrôleurs pour pallier ce problème de collision. On dispose ainsi notamment d'un variateur de puissance qui corrige et ajuste la puissance des antennes et dans le cadre de la HF, d'un ASIC de couplage inductif donnant un peu plus d'intelligence au contrôleur. C'est d'ailleurs au niveau de cette intelligence que se fait toute la différence entre produits. Certains disposent en effet de fonctions middleware intégrées qui leur permettent d'expédier directement des données assimilables par l'ERP de l'entreprise. D'autres sont seulement programmables en langage machine, tandis que d'autres encore disposent d'un système d'exploitation dédié. Au niveau le plus bas, on peut opérer la classification suivante à propos de la lecture de l'étiquette : [9]

- lecture seule : le lecteur prélève le code du tag émettant le signal le plus fort
- lecture multiple : le lecteur explore le champ de lecture pour prélever les codes de toutes les étiquettes en émission RF En ce qui concerne en revanche le fonctionnement du lecteur:

- Autonome: le lecteur active le signal RF après avoir reçu une entrée ou une commande du logiciel ;
- Interactif : le lecteur lit lorsqu'il reçoit une requête d'une autre application à un autre niveau.

3.5.2.4 Les différents types de tags et leurs spécificités techniques

Pour exploiter les informations contenues dans ces étiquettes, il faut impérativement disposer du lecteur approprié. Celui-ci émet des ondes radios en direction de la capsule ce qui permet de l'alimenter en énergie (alimentation par induction électromagnétique), en d'autres termes de l'activer (la puce renvoie alors des données), pour en extraire les informations qu'elle renferme. [10]

Ces puces ne sont pas capables d'effectuer des traitements dynamiques mais seulement de renvoyer des données statiques.

- Tags passifs (sans batterie)

Les tags passifs ne disposant d'aucune alimentation externe, ils dépendent de l'effet électromagnétique de réception d'un signal émis par le lecteur. C'est ce courant qui leur permet d'alimenter leurs microcircuits. Ils sont peu coûteux à produire et sont généralement réservés à des productions en volume. Ce sont eux que l'on trouve plus particulièrement dans la logistique et le transport. Ils utilisent différentes bandes de fréquences radio selon leur capacité à transmettre à distance plus ou moins importante et au travers de substances différentes (air, eau, métal). La distance de lecture est inférieure à un mètre. Les basses et hautes fréquences sont normalisées au niveau mondial.

Ces puces sont collées sur les produits pour un suivi allant jusqu'aux inventaires. Elles sont jetables ou réutilisables suivant les cas. Les puces avec une antenne de type "papillon" ont une portée courante de 1 à 6 mètres. Ces puces UHF (Ultra Haute Fréquence) sont utilisées pour la traçabilité des palettes dans les entrepôts. Par contre, la tolérance aux obstacles est moyenne. Pour les très hautes fréquences (UHF), l'Europe, l'Asie et les Etats-Unis se distinguent par des fréquences et des réglementations différentes

- Tags semi-passifs

Ces tags sont similaires aux cartes d'identification passive. Ils emploient des technologies proches, mais avec quelques différences importantes. Ils disposent en effet eux aussi d'une petite batterie qui fonctionne en permanence, ce qui libère l'antenne pour d'autres tâches, dont 9 notamment la réception de signaux de retour. Ces tags sont plus robustes et plus rapides en lecture et en transmission que les tags passifs, mais ils sont aussi plus chers.

➤ Tags actifs

Les étiquettes actives sont les plus chères car elles sont plus complexes à produire et assurent, outre des fonctions de transmission, des fonctions soit de captage soit de traitement de l'information captée, soit les deux. De ce fait, elles ont besoin d'une alimentation embarquée et sont donc caractérisées par la durée de vie de celle-ci. Si le prix est un facteur discriminatif, il faut savoir que ces étiquettes s'avèrent particulièrement bien adaptées à certaines fonctions, dont notamment la création de systèmes d'authentification, de sécurisation, d'antivol, etc. Bref, elles sont idéales pour tout ce qui concerne le déclenchement d'une alerte ou d'une alarme. Elles émettent à plusieurs centaines de mètres. Le dernier cri est le tag «insensible à l'orientation du produit».

3.5.2.5 Les fréquences d'utilisation

Les systèmes RFID génèrent et réfléchissent des ondes électromagnétiques. Les systèmes RFID doivent notamment veiller à ne pas perturber le fonctionnement des autres systèmes radio. On ne peut, en principe, utiliser que les plages de fréquences spécifiquement réservées aux applications industrielles, scientifiques ou médicales. Ces plages de fréquences sont appelées ISM (Industriel – Scientifique – Médical). Les principales plages de fréquences utilisées par les systèmes RFID sont les basses fréquences (125 et 134.5 kHz) et les fréquences ISM : 6.78 MHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz (pas en Europe), 2.45 GHz, 5.8 GHz et 24.125 GHz. La plage de fréquences la plus utilisée est de loin 13.56 MHz (haute fréquence). [10]

Tableau 3. 2 Les fréquences d'utilisation

ISO 18000-2	ISO 18000-3	ISO 18000-7 4	ISO 18000-6	ISO 18000-4
LF	HF		UHF	
125.5 KHz 134.2 KHz	13.56 MHz	433 MHz	850/950 MHz	2.5 GHz
	NFC		RFID	

3.5.3 La NFC

La communication en champ proche est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm. Cette technologie est une extension de la norme ISO/CEI 14443 standardisant les cartes de proximité utilisant l'identification

par radiofréquence, qui combinent l'interface d'une carte à puce et un lecteur au sein d'un seul périphérique.

Un périphérique NFC est capable de communiquer avec le matériel ISO/CEI 14443 existant, avec un autre périphérique NFC ou avec certaines infrastructures sans-contact existantes comme les validateurs des transports en commun ou les terminaux de paiement chez les commerçants. La NFC équipe aujourd'hui des cartes utilisées dans les transports, dans le commerce ou pour l'accès à certains services publics et de plus en plus de terminaux mobiles.

En 2011, la NFC équipait en effet 50 millions de tablettes tactiles ou téléphones mobiles. Dotés d'un écran, d'un clavier et d'une connexion Internet, ces terminaux NFC ont un fort potentiel d'usages en favorisant les interactions entre les machines.

Au contraire d'autres techniques de radio-identification ou du bluetooth dont la portée est d'une dizaine de mètres, la technique NFC n'est utilisable que sur de très courtes distances (quelques centimètres). Elle suppose une démarche volontaire de l'utilisateur et normalement ne peut pas être utilisée à son insu. Mais cela n'exclut pas la collecte des données NFC par le système lui-même, qui reste capable d'historiser les usages de l'utilisateur avec cette technique de communication. [12]

En mai 2010, à l'occasion d'une visite des services sans contacts déployés à Nice, la CNIL³ a du reste énoncé les grands principes pour que les services sans contact

L'invention et les premiers brevets autour des cartes à puce avec contact datent des années 1970. Les premières cartes sans contact datent de la fin des années 1980 même si leur déploiement a vraiment pris son essor début des années 2000 : la carte de transport francilienne Navigo a plus de douze ans par exemple. Nous utilisons des cartes à puce avec ou sans contact tous les jours : les cartes de paiement que l'on glisse dans un distributeur automatique de billets (DAB) pour retirer de l'argent ou dans un terminal de paiement électronique (TPE) pour payer un achat chez un commerçant par exemple.

De nombreuses clés d'entrée d'immeubles ressemblent plus à des porteclés (avec une technologie spécifique) ; d'autres services vont utiliser des clés USB, des bracelets, des bagues... Toutes ces cartes et objets sont sans contact mais tous ne sont pas NFC. Ces cartes sans contact comportent un processeur, de la mémoire mais, pas de batterie. La communication vers les lecteurs de carte se passe par radiofréquence/RFID et non par lecture d'une piste magnétique ou contact direct dans un lecteur. Tout comme les applications RFID vues précédemment, elles vont être utilisées pour permettre l'identification, l'authentification et/ou l'autorisation et donc un paiement, un voyage en métro ou l'utilisation d'un vélo partagé. En revanche, ce n'est plus l'objet que l'on

identifie mais son porteur, le consommateur dans le cas des cartes de crédit, l'utilisateur des transports publics, le citoyen des services publics de la ville et de la région.

3.5.3.1 Le fonctionnement de NFC/RFID

Une application d'identification automatique radio fréquence se compose donc d'un lecteur qui transmet un signal selon une fréquence déterminée vers une ou plusieurs étiquettes radio situées dans son champ de lecture. Celles-ci transmettent en retour un signal. Lorsque les étiquettes sont "réveillées" par le lecteur, un dialogue s'établit selon un protocole de communication prédéfini et les données sont échangées. [7]

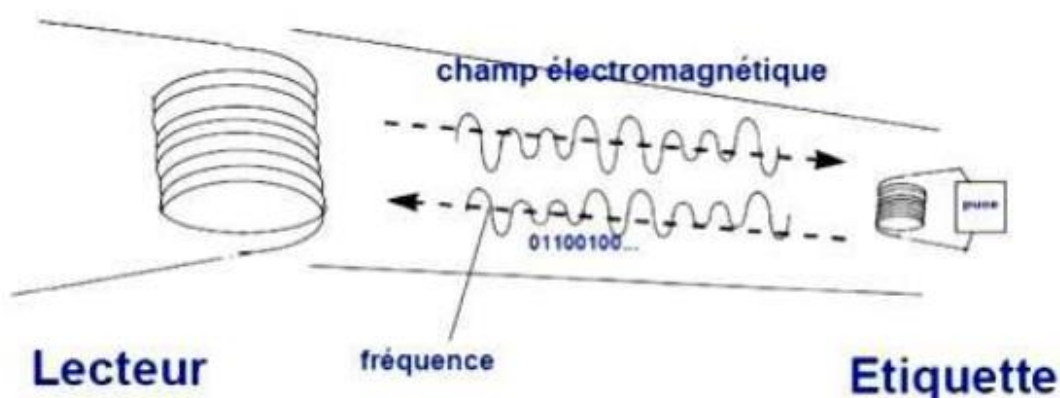


Figure 3. 5 le fonctionnement NFC/RFID

La technologie sans fil NFC est dite sans contact car elle nécessite une courte distance pour fonctionner de l'ordre d'une dizaine de centimètre maximum (aucune norme n'est définie à ce jour concernant les distances d'utilisation). Les débits de communications vont de 106 à 848 kbits/s sur une gamme de fréquence de 13,56 MHz.

La très courte portée suppose une démarche volontaire des utilisateurs et donc une résistance aux écoutes à leur insu. L'induction magnétique est le principe physique exploité par les solutions NFC/RFID:

3.5.1.2 le principe physique exploité par les solutions NFC/RFID

Un lecteur émet un faible courant électrique qui crée un champ magnétique entre les deux appareils.

L'acteur démarrant la connexion est appelé initiateur.

- Un client reçoit le champ et le transforme en impulsion électrique qu'il peut traduire en bits de données. Cet acteur est appelé la cible.
- La manière dont la réponse est envoyée dépend du mode de fonctionnement. Par défaut, tous les appareils compatibles NFC sont des clients potentiels et sont à

l'écoute de champ magnétique. Avant d'initier une connexion, et dans le but de ne pas perturber d'autres communications NFC (collision avoidance), l'initiateur écoute systématiquement le médium avant de commencer l'émission. Le temps d'écoute est défini aléatoirement.

3.5.2.3 Mode de communication [12]

➤ Mode passif

La méthode de communication passif est utilisée par les tags NFC ou les systèmes devant économiser un maximum d'énergie. En effet, cette méthode permet à la cible de n'utiliser aucune source d'alimentation pour la transmission d'information. La seule action qu'elle effectue est la modulation du champ pour transmettre des données prédéfinies, opération qui nécessite peu d'énergie comparé à l'émission d'un courant électrique. La cible utilise par ailleurs ce champ pour tirer l'énergie dont elle a besoin pour le moduler, la rendant totalement autonome d'un point de vue énergie, mais lui permettant de transmettre un nombre limité d'informations. La technologie NFC utilise les communications passives pour deux modes de fonctionnement :

➤ Le mode émulation de carte

Permet à l'appareil de se comporter comme un tag RFID et de répondre ainsi aux lecteurs éventuels. NFC est ainsi compatible avec la norme RFID.

- Le mode lecteur permet de lire les tags RFID.

➤ Mode actif

Avec cette méthode de communication les deux appareils génèrent des champs magnétiques. Ils le font de manière alternative en désactivant la génération lors de l'attente. Les deux appareils nécessitent une source d'énergie qui leur est propre. Le mode de fonctionnement associé à cette méthode de communication est appelé pair à pair (peer to peer). Deux appareils échangent de l'information qui n'est pas prédéfinies (carte de visite, photos, ...). Jusqu'à récemment, le mode passif était le plus répandu, mais l'utilisation du mode actif avec les smartphones tend à se diffuser. Les fabricants de ces appareils font une promotion acharnée de cette nouvelle fonctionnalité dont l'objectif est d'étendre les possibilités de partage de données.

3.5.3.4 Les caractéristiques principales [12]

Un système RFID permet donc d'écrire, de stocker et d'effacer de l'information sur la puce électronique du tag. En plus du transfert de données sans contact, la communication via l'antenne, permet également, des transferts sans visibilité entre le lecteur et l'étiquette au travers de matériaux opaques à la lumière, cette lecture pouvant

s'effectuer simultanément sur plusieurs étiquettes. Les différents systèmes RFID sont caractérisés principalement par leur fréquence de communication.

Cependant, outre cette fréquence porteuse, d'autres caractéristiques définissent également les étiquettes RFID et constituent la base de leurs spécifications :

- l'origine et la nature de l'énergie ;
- la distance de lecture ;
- programmable ;
- la forme physique ;
- la taille mémoire ;
- les propriétés du packaging (matériau) ;
- le nombre de tags lus simultanément (anticollision) ;
- et bien sur le coût.

Tableau 3. 3 caractéristiques de la NFC

Débits de communication	106, 212 ou 424 kbit/s
Gamme de fréquence (classique)	135 KHz ; 13,56 MHz ;
Distance de communication	: maximum 10 cm
Mode de communication	half-duplex ou full-duplex

A noter que le débit 848 kbit/s n'est pas compatible avec la norme NFCIP-1

3.6. Critères de choix de la technologie

Nous avons fait un tour de l'horizon pour comprendre les technologies d'identification et nous avons constaté qu'il y a 2 manières de faire l'identification :

- Par les technologies de codes
- Par la technologie biométrique

Pour notre système nous avons opté pour les technologies d'identification par code,

Lorsqu'on a fait le choix d'une identification par badge, vient ensuite le choix de la technologie de badge pour laquelle opter. Qu'il soit avec ou sans contact, à piste magnétique, carte à puce, code à barre ou RFID... le choix de la technologie se fait en fonction de différents critères :

- Le niveau de sureté (copiable, falsifiable, critères ANSSI)
- Les conditions d'utilisation (intérieur, extérieur, température...)
- Les usages (occasionnel, trafic élevé...)
- La distance de lecture
- La fragilité,

Notre choix de la NFC se justifie par le fait que la NFC utilise les mobiles qui est à notre disposition chaque jour, son utilisation suppose une démarche volontaire de l'utilisateur et normalement ne peut pas être utilisée à son insu.

3.7 Conclusion partielle

Dans ce chapitre nous avons parlé des différentes technologies d'identification ou nous avons relevé les deux manière principale d'identification par les codes avec ses différents moyens ainsi que par la biométrie avec ses différents processus et cette étude nous a poussé à faire une manière d'identifier et une technologie adapter à notre problèmes selon un certains notre de critère que nous avons mise en place et la technologie choisie à nécessité des outils pour un bon fonctionnement de la solution.

CHAPITRE 4 : IMPLEMENTATION DE LA SOLUTION

4.1 Introduction partielle

Nous voici à la partie finale de notre travail ou devrons mettre en application toutes les théories démontrées dans les chapitres précédant, nous avons fait une étude de la sécurité, nous avons conçu notre système et nous avons fait un choix technologie et outils pour la réalisation de notre système.

Pour l'implémentation de la présente application, l'architecture du système a 4 couches: une application Android, navigateur de Web, serveur de Web et serveur de la base de données, a été prise en compte (Figure 4.1).

L'agent de sécurité après authentification, il prend le navigateur de web pour accéder au système en local en mettant l'adresse IP. Le protocole de communication entre le navigateur et le serveur est HTTP. Le mécanisme du système est très simple: d'abord, le navigateur envoie son requête au serveur, et puis, le serveur accède directement au serveur de la base de données, en suit, il envoie au navigateur les données.

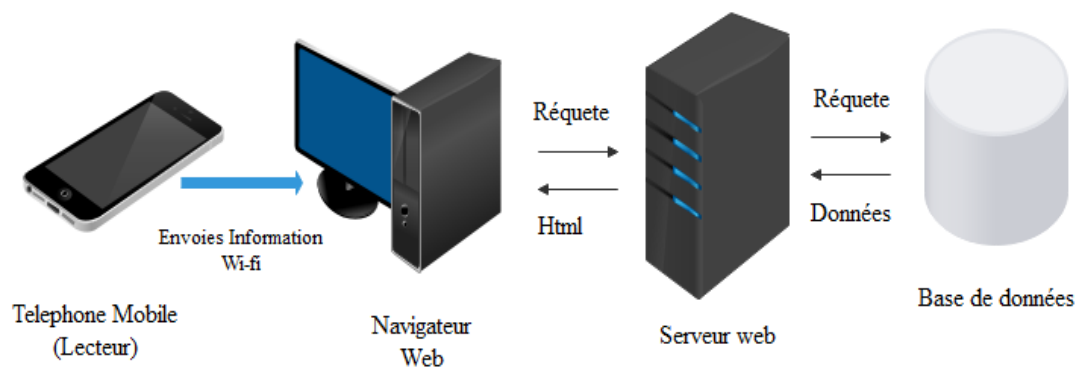


Figure 4. 1 Fonctionnement de la solution

4.2 Environnement de travail

Dans cette section, nous présenterons les environnements matériel et logiciel de notre travail pour la réalisation de cette application.

4.2.1 Environnement matériel

Afin de mener à bien concevoir ce projet de mémoire, il a été mis à notre disposition un ensemble de matériels dont les caractéristiques sont les suivantes :

- Un ordinateur LENOVO avec les caractéristiques suivantes :
 - Processeur : Intel® Celeron® CPU N3060 1.60GHz
 - RAM : 4.00 Go
 - Disque Dur : 500 Go
 - OS : Microsoft Windows 10 professionnel 64bits

Lecteur RFID/NFC ACR122U compatible libnfc

Ce lecteur ACR122U permet de bien démarrer dans le monde du RFID/NFC et compatible avec la suite d'outils NFC Tools et plus particulièrement libnfc. Combiné à ces outils, par exemple au travers de la distribution Kali Linux, il permet de lire, écrire et dupliquer les puces NFC fonctionnant à 13,56Mhz comme celles contenus dans les badges d'immeuble.



Figure 4. 2 lecteur de carte NFC

Pour notre travail nous avons développé une application Android qui nous permettra faire la lecture et de l'écriture de cartes NFC ainsi que d'envoyer les informations au serveur via une connexion Wi-Fi.

4.2.2. Outils de développement de l'application

Pour notre travail nous avons eu recours à un langage de programme PHP qui nous a permis de faire le traitement ainsi qu'une base de données MySQL qui tourne en local sur le serveur Apache et nous avons utilisé comme gestionnaire de serveur en local WampServer.

Un autre langage de programmation utiliser c'est le langage java pour le développement d'une application Android.

4.2.2.1. Le langage PHP [13]

PHP a une définition récursive: PHP: HyperText Processor. Mais, en réalité, son premier nom est: Personal Home Page Tools. PHP est un langage de script côté serveur inclus dans HTML.

- Pourquoi l'utilisation de PHP ?

Les raisons qui font que PHP soit plus utilisé sont que PHP ne coûte rien pendant la durée de la vie de l'application. Le développement, le serveur, la gestion de la base de données, le support, tous sont gratuits. La syntaxe de PHP est simple, PHP est donc facile à apprendre. Pourtant, on ne peut pas utiliser les outils pour générer le code source de PHP, ils sont écrits à la main.

Il vient s'incorporer dans HTML et son incorporation dans HTML a plusieurs conséquences utiles comme: PHP peut être rapidement ajouté à du code produit par un éditeur HTML graphique; PHP se prête de lui-même à une division du travail entre concepteurs graphiques et développeur de scripts; PHP peut réduire les coûts de développement et améliorer son efficacité.

PHP n'a pas besoin de compilation: C'est un point fort du type de langage de script, il n'est pas nécessaire d'une compilation en code binaire avant de tester ou de déployer une application. Il suffit de l'écrire et de la lancer. PHP est disponible sur plusieurs plates-formes: PHP est disponible en natif pour Unix et pour Windows (la plupart des serveurs HTTP fonctionne sous l'un de ces types de système d'exploitation). PHP est aussi compatible avec les serveurs Web populaires: Apache HTTP Server, Microsoft Internet Information Server et Netscape Enterprise Server. PHP de plus en plus populaire: PHP devient rapidement l'une des solutions de développement dite «à deux étage» (Web et données). Les deux figures au-dessus illustrent la croissance de PHP.

En résumé, PHP n'est pas la panacée à tous les problèmes de développement Web, mais il a de nombreux avantages. Il est fait par des développeurs Web et pour des développeurs Web.

4.2.2.2 MySQL [14]

MySQL est une base de données utilisant le SQL qui est un langage des requêtes structurées et qui permet l'utilisateur d'interagir avec la base de données.

MySQL est devenue la base de données open source la plus populaire au monde grâce à sa performance, sa haute fiabilité et sa simplicité d'utilisation. On la trouve dans plus de 8 millions d'installations, dans les grandes entreprises transnationales comme au sein d'applications embarquées spécialisées, sur tous les continents de la planète.

Non seulement MySQL est la base de données open source la plus populaire au monde, mais elle est également devenue le choix de prédilection de toute une nouvelle génération d'applications.

En outre, la fiabilité et la facilité d'administration de MySQL permettent aux administrateurs de base de données de ne plus perdre leur temps à régler des problèmes de performance ou d'interruptions de fonctionnement, pour pouvoir au contraire se concentrer sur des tâches plus stratégiques.

4.3 Présentation de l'application

4.3.1 Le lancement du serveur Web WAMP SERVER

Pour que le site WEB puisse faire connaissance de la base de données se trouvant sur le serveur.

4.3.1.1 Apache

Le logiciel libre Apache HTTP Server (Apache) est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web. Il est distribué selon les termes de la licence Apache.

4.3.1.2 Wamp

WampServer est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l'aide du serveur Apache2, du langage de scripts PHP et d'une base de données MySQL. Il possède également PhpMyAdmin pour gérer plus facilement vos bases de données.

WampServer s'affichera une fois que l'utilisateur aura cliqué sur Local host, et donnera ainsi l'opportunité de choisir notre base des données. Une fois que la base de données n'est pas créée l'opportunité de la créer lui sera proposé en cliquant sur

phpMyAdmin en donnant le nom de la base et ainsi créer table par table selon le besoin de l'utilisateur.

La même procédure est d'application dans le cas de la vérification des contenues de la base des données.

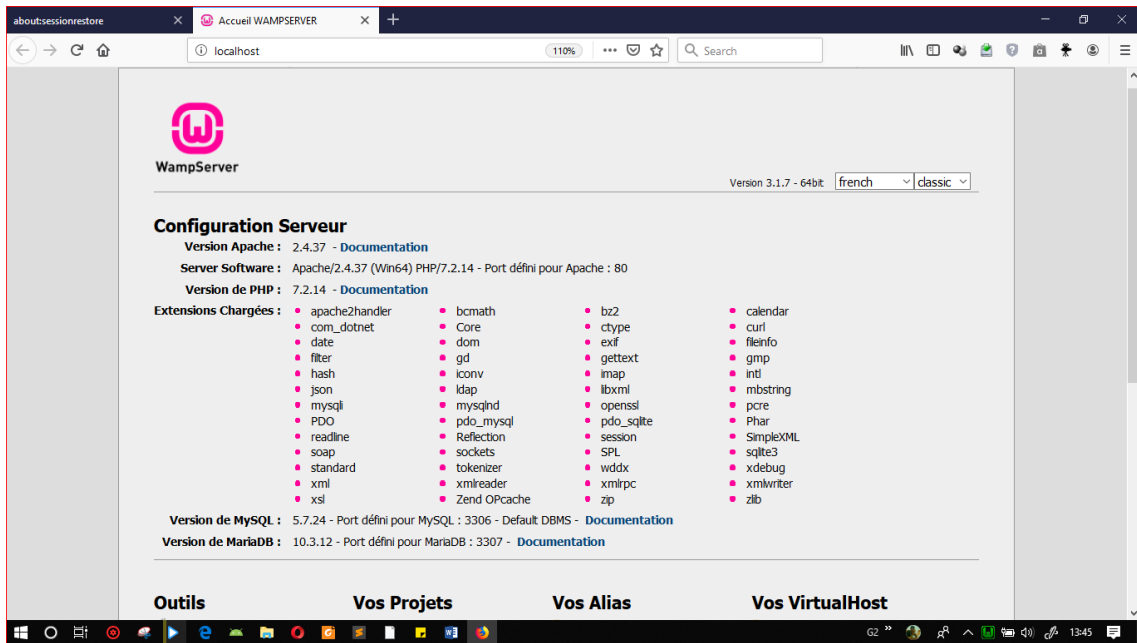


Figure 4. 3 Présentation de WampServer

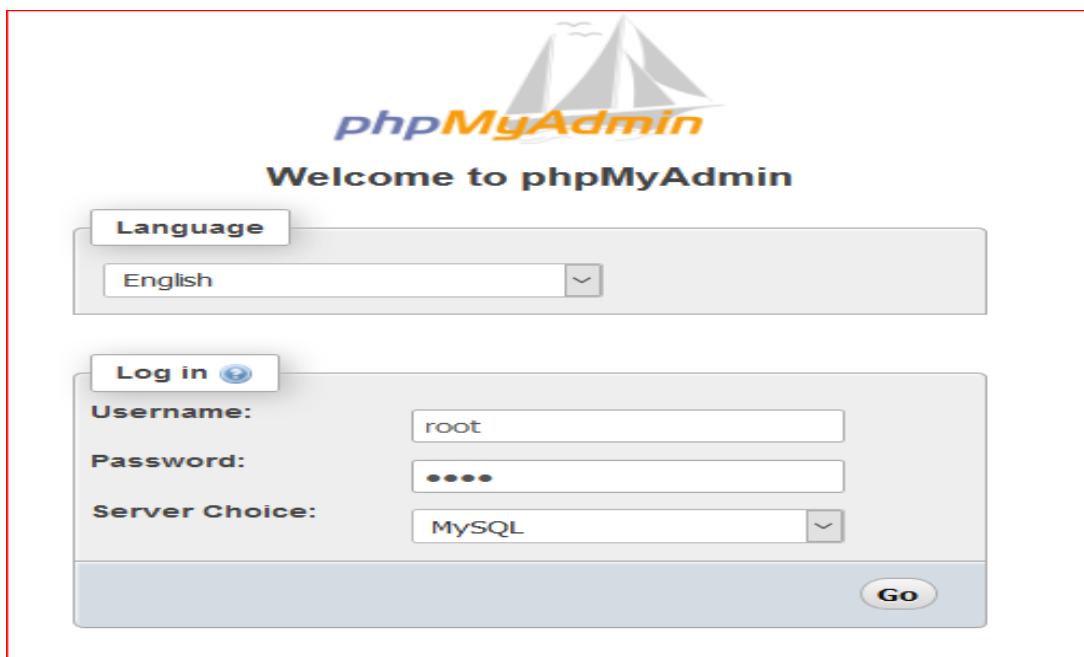


Figure 4. 4 Connexion à la base de données

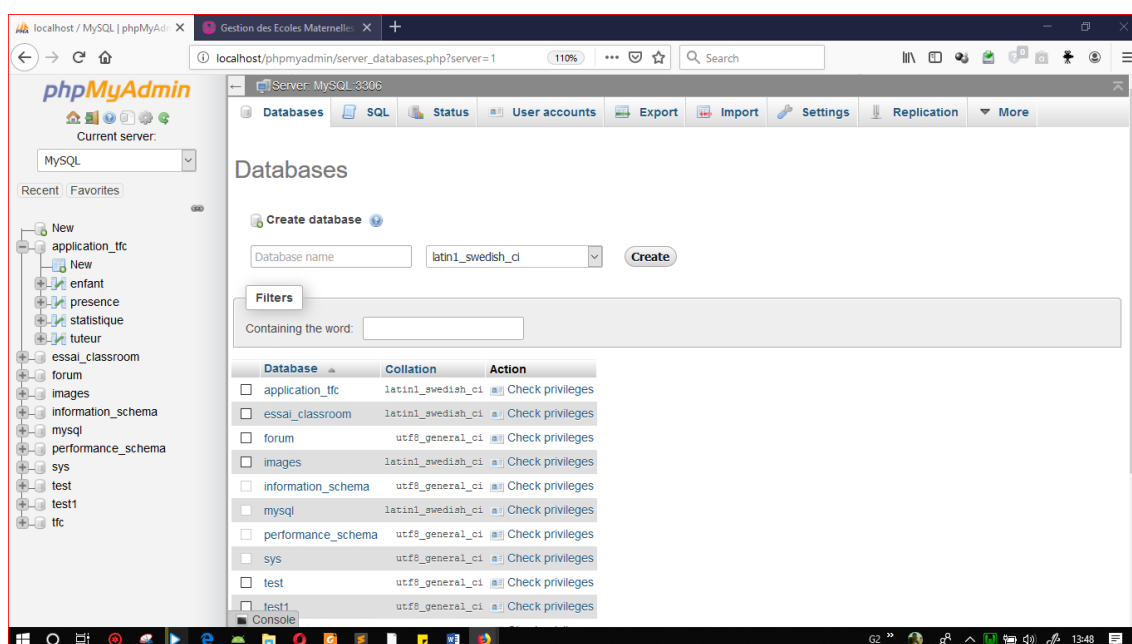


Figure 4. 5 Création d'une nouvelle base de données et des tables

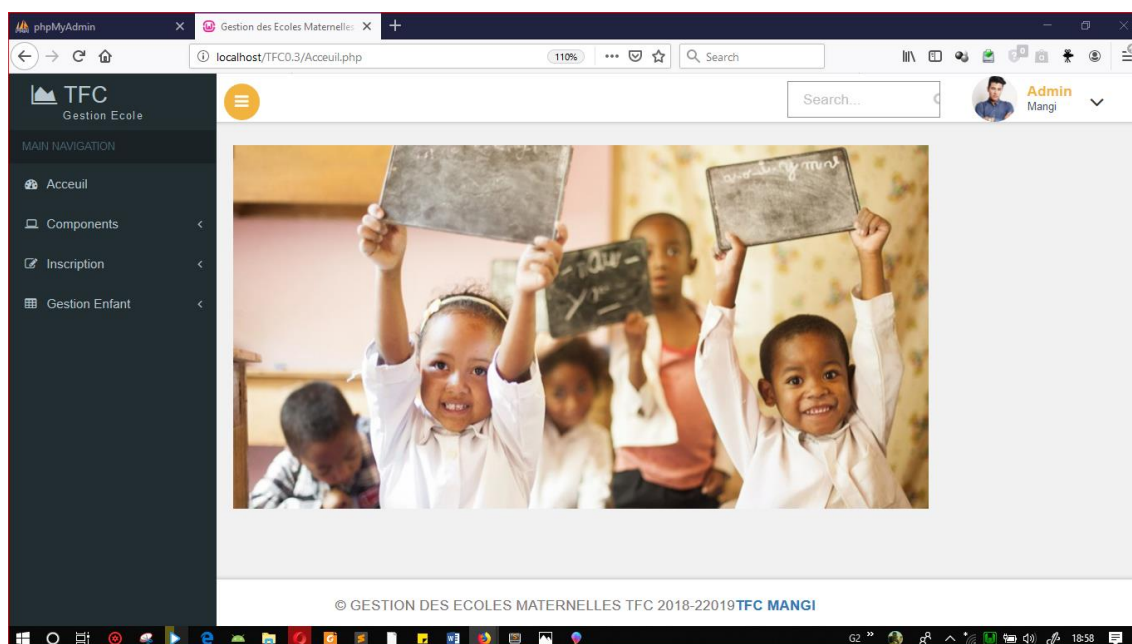



Figure 4. 6 Page d'accueil de l'application



INSCRIPTION ELEVE

Nom

Postnom

Prenom

Age

Photo No file selected.

Genre

Classe

Figure 4. 7 Formulaire d'inscription

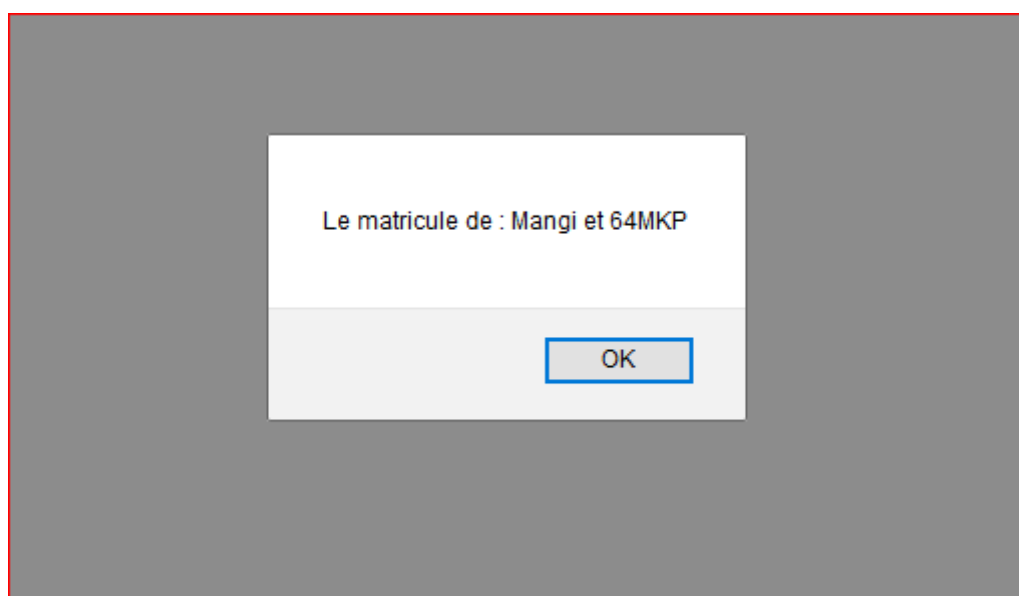


Figure 4. 8 Le matricule de l'élève

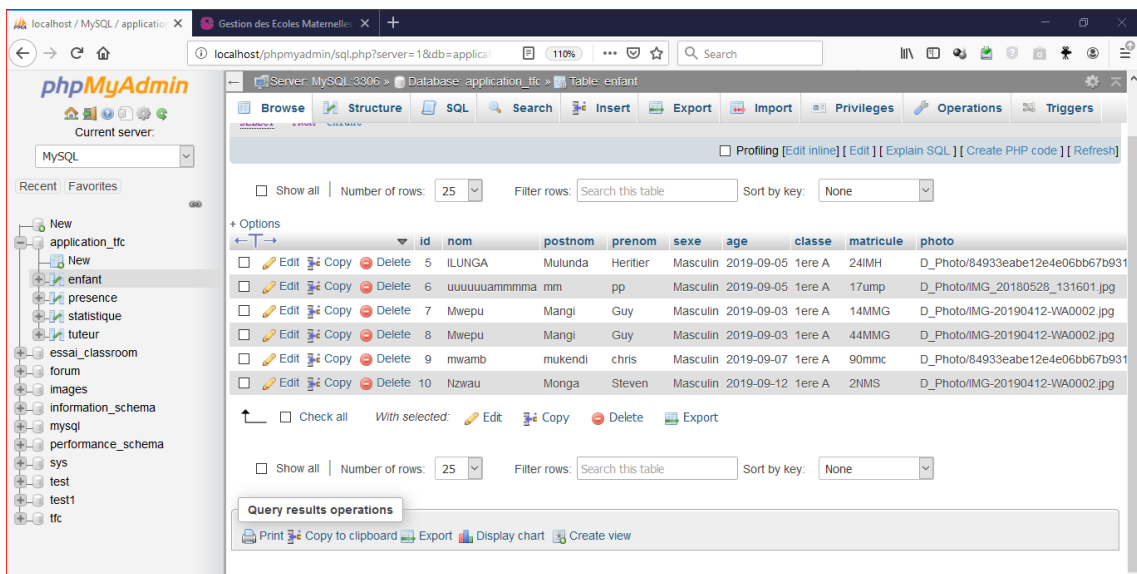


Figure 4. 9 les élèves inscrits à l'école

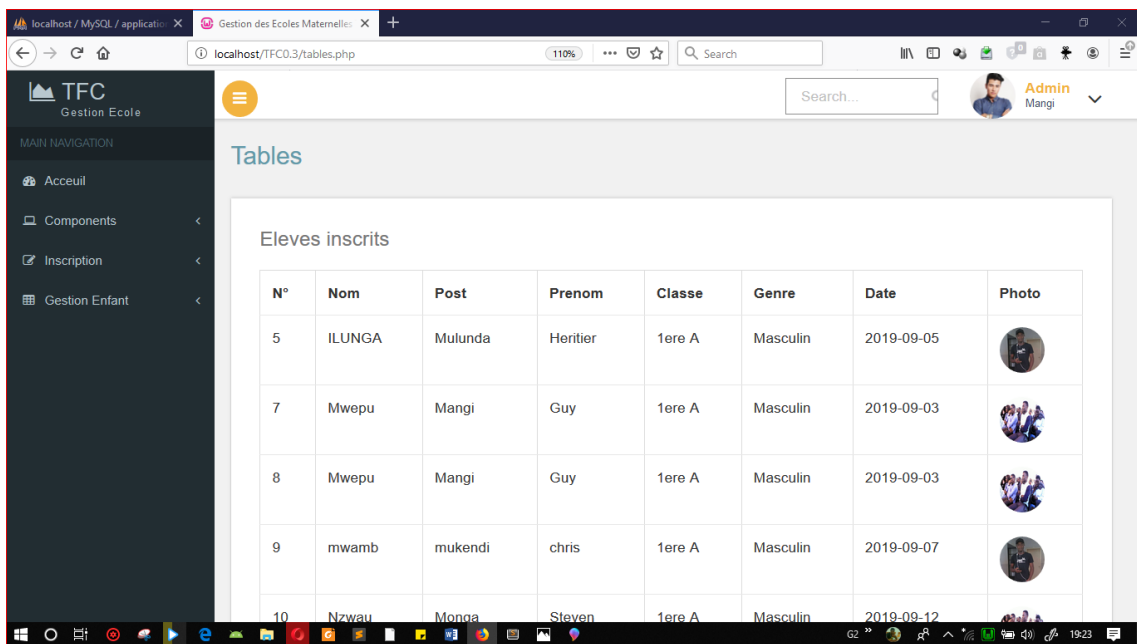


Figure 4. 10 Affichage des élèves inscrits

4.4 Evaluation des coûts de mise en place du système

Pour la mise en place de notre système, nous aurons besoins de matériaux suivants : Ordinateur, puce NFC, carte plastique, un lecteur de carte,

Le nombre de lecteur et de puce NFC dépend de l'organisation et du nombre des enfants nous allons représenter une quantité **n**.

Tableau 4. 1 estimation de couts de la solution

Matériaux	Quantités	Cout Unitaire	Cout total
Ordinateur	3	350\$	1050\$
Lecteurs	n	30\$	N*30\$
Puce NFC	n	1.5\$	N*1.5\$

4.4 Conclusion partielle

En définitive nous dirons que ce chapitre à constituer un atout pour notre système car il constitue tous les moyens nécessaires pour sa mise en place. L'installation des outils nécessaires permettent à une évolution pour tous les usagers de ces derniers. Au départ ce travail n'était qu'un projet abstrait mais cela venait d'être réalisé au troisième chapitre intitulé : « Mise en place d'un système automatique de gestion de retrait des enfants des écoles maternelles avec la technologie NFC » dans lequel nous avons misent en place toutes les connaissances théoriques pour parvenir à sa réalisation.

CONCLUSION GENERALE

Nous voici arrivé au terme du présent travail inhérent qui a consisté à la : « Mise en place d'un système automatique de gestion de retrait des enfants des écoles maternelles avec la technologie NFC » cas des écoles de la ville de Lubumbashi.

En effet, notre objectif était de mettre, à la disposition de la ville de Lubumbashi une application informatique qui servirait à la sécurité et gestion des écoles maternelles. A travers de cette application, il fallait aussi répondre à la problématique de l'insécurité dans les écoles. Outre l'introduction et la conclusion, ce travail était articulé sur quatre chapitres qui sont les suivants :

Dans le premier chapitre il était question de faire une étude approfondie de la sécurité des écoles, les menaces auxquelles les écoles font face ainsi que faire une étude descriptive du système existant dans les écoles.

Le chapitre deux a fait objet de l'analyse de besoin ainsi que la conception d'une manière logique du système envisagé, nous avons donnés tous les acteurs qui entrent en contact avec le système.

Dans ce chapitre nous avons parlé de différentes technologies d'identifications qui existent ainsi que leurs manières de fonctionner ensuite nous avons fait un choix sur une technologie qui va répondre à notre besoin.

Au quatrième chapitre nous avons parlé du déploiement de l'application et de la configuration technologique. Il étale par la même occasion la procédure du déploiement de l'application et la configuration technologique. Il s'agit de déployer l'application sur un serveur web (Apache-MySQL) et la configuration de l'architecture réseau dans le but d'interconnecter les différents bureaux de l'école.

Au terme de cette étude, nous affirmons l'hypothèse en disant que la mise en place et l'utilisation correcte de cette application informatique apporterait beaucoup d'améliorations dans la gestion des enfants des écoles maternelles ainsi que une bonne sécurité de ces enfants.

A ceci s'ajoute la connaissance sans ambiguïté les élèves ainsi que les tuteurs des enfants qui s'enregistrent à l'école.

Comme tout travail scientifique quelques imperfections ne manquent jamais, raison pour laquelle nous sollicitons l'indulgence de tous pour nos failles éventuelles ; ainsi dit, nous mettons à la disposition de toute personne capable d'enrichir davantage ce travail ou de le compléter à l'occasion des prochaines recherches avec le concours de notre vie professionnelle.

REFERENCE

- [1] Daudet, «« Les enlèvements en RDC, crime de l'est »,» 2009.
- [2] M. Christiane, «Prévention des risques à l'école maternelle et élémentaire, Moquet,» Paris, 2010.
- [3] P. tourel, «« Histoires sur les enlèvements »,», 2015.
- [4] Pouillet, « « Education et accueil des jeunes enfants », thèse, Montelieu, Montelieu,,» 2003.
- [5] Albert, «« contrôle d'accès pour l'école des enfants », Etude, Montpellier.».
- [6] «<https://fr.wikipedia.org/wiki/Biométrie>,» [En ligne]. Available: <https://fr.wikipedia.org/wiki/Biométrie>. [Accès le juin 2019].
- [7] «<https://www.boutique.afnor.org/resources/cf195160-5165-47bc-872c-9962baacd403.pdf>,» juillet 2019. [En ligne].
- [8] «<https://fr.wikipedia.org/wiki/Code-barres>,» juillet 2019. [En ligne].
- [9] Michaël MADEGARD, «http://www-igm.univ-mlv.fr/~dr/XPOSE2007/mmadegar_rfid/,» 2008.
- [10] M. S. A. Mr YAHIAOUI Billal, «Technologie RFID : Étude et application,» 2015.
- [11] B. Youssef, «PROJET RFID Projet de fin d'étude (option RSM),» 2015.
- [12] C. INGENIEURS, «NFC Near Field Communication,» 2012.
- [13] «<https://www.php.net/docs.php>,» juillet 2019. [En ligne].
- [14] «<https://www.mysql.com/fr/>,» [En ligne]. [Accès le juillet 2019].
- [15] B. S. B. O. J. G. BACHOTI Youssef, «PROJET RFID, projet de fin d'etude,» Algerie, Le 25 janvier 2011.
- [16] K. ALAIN, «« Projet de construction d'un bâtiment scolaire »».