

UNIVERSITE DE MAROUA

ECOLE NATIONALE SUPERIEURE
POLYTECHNIQUE DE MAROUA

DEPARTEMENT D'INFORMATIQUE ET DES
TELECOMMUNICATIONS



THE UNIVERSITY OF MAROUA

NATIONAL ADVANCED SCHOOL OF
ENGINEERING OF MAROUA

DEPARTMENT OF COMPUTER SCIENCE
AND THE TELECOMMUNICATIONS

INFORMATIQUE ET TÉLÉCOMMUNICATIONS

SÉCURISATION DE L'AÉROPORT INTERNATIONAL DE MAROUA-SALAK PAR UNE SOLUTION DE CONTRÔLE D'ACCÈS BIOMÉTRIQUE

Mémoire présenté et soutenu en vue de l'obtention du Diplôme d'INGENIEUR DE
CONCEPTION EN CRYPTOGRAPHIE ET SÉCURITÉ INFORMATIQUE

par

YOUNKAP NINA Duplex

Ingénieur des travaux en sécurité et administration réseau

Matricule: 13Z474S

Sous la direction du

Dr. OUMAROU MAMADOU BELLO

Chargé de cours

devant le jury composé de:

Président

Rapporteur

Examineur

Invité

Dr. OUMAROU MAMADOU BELLO

CDT EBANGA Frédéric

Année académique 2017/2018

REMERCIEMENTS

Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à toutes les personnes qui ont contribué de près ou de loin à l'édification de ce travail. Nos pensées vont particulièrement aux personnes suivantes :

- Le président de jury pour avoir accepté de présider le jury de ma soutenance ;
- L'examineur pour avoir accepté d'examiner le présent mémoire ;
- L'encadreur académique **Dr OUMAROU MAMADOU BELLO** pour sa disponibilité et son attention ;
- Le chef de département d'informatique et des télécommunications pour les encouragements et l'intérêt qu'il accorde à notre formation ;
- L'encadreur professionnel **CDT EBANGA Frédéric**, pour son soutien, sa disponibilité et ses conseils tout au long de notre stage ;
- **M. Terdam Valentin** pour son encadrement et sa disponibilité durant nos années de formation ;
- **M. GARBA BOUBA Raymond**, Chef Bureau AVSEC de l'Aéroport International de Maroua-Salak pour son soutien et ses suggestions ;
- L'ensemble du personnel de l'Aéroport International de Maroua-Salak particulièrement ceux de l'Autorité Aéronautique pour leur accompagnement ;
- Mes Camarades de classe pour leur soutien ;
- Ma maman **MBOUMI Jeannette** pour son accompagnement et soutien ;
- Ma très chère petite sœur **NGOPSEU Josephine Gaëlle** pour son soutien ;
- Tous mes collègues et camarades qui ont accepté de se salir les doigts pour nous donner leurs empreintes.

TABLES DES MATIÈRES

REMERCIEMENTS	i
TABLES DES MATIÈRES	v
LISTE DES SIGLES ET ABRÉVIATIONS	vi
RÉSUMÉ	viii
ABSTRACT	x
LISTE DES TABLEAUX	xii
LISTE DES FIGURES ET ILLUSTRATIONS	xiv
INTRODUCTION GÉNÉRALE	xv
1 CONTEXTE ET PROBLÉMATIQUE	2
1.1 Introduction	2
1.2 Présentation de l'Aéroport International de Maroua-Salak	2
1.2.1 Historique de l'aéroport	2
1.2.2 Les acteurs	3
1.3 Présentation du Commandement de l'Aéroport International de Maroua-Salak	4
1.3.1 Sa mission	4
1.3.2 Son organigramme	5
1.3.3 Son fonctionnement	5
1.4 Contexte et Problématique	6
1.5 Objectifs	7
1.5.1 Objectif Général	7
1.5.2 Objectifs Spécifiques	8
1.6 Méthodologie	8
1.7 Conclusion	11
2 GÉNÉRALITÉS	12
2.1 Introduction	12
2.2 Sûreté de l'aviation civile et contrôle d'accès des personnes	12
2.2.1 Définition et objectif de la sûreté de l'aviation	12

2.2.2	Dispositions réglementaires en matières du contrôle d'accès	13
2.2.3	Nature des menaces	14
2.2.4	Types d'agresseurs	14
2.2.5	Motivations	15
2.2.6	Les contre-mesures	15
2.2.7	Le contrôle d'accès des personnes	17
2.3	Généralités sur le contrôle d'accès	17
2.3.1	L'identification	17
2.3.2	L'authentification	18
2.3.3	L'autorisation	18
2.3.4	L'auditabilité	19
2.4	Le contrôle d'accès physique	19
2.4.1	L'authentification	19
2.4.2	Les technologies du contrôle d'accès physiques	19
2.5	Le contrôle d'accès biométrique	24
2.5.1	L'authentification biométrique	24
2.5.2	Les caractéristiques utilisées dans les application biométriques . . .	24
2.6	Les technologies d'authentification biométrique	31
2.6.1	Définition	31
2.6.2	L'architecture et fonctionnement	31
2.6.3	L'enrôlement	32
2.6.4	La vérification	33
2.6.5	L'identification	34
2.7	Spécification des données biométriques	34
2.8	La précision des système biométrique	35
2.9	Vulnérabilités des systèmes d'authentification biométriques	37
2.9.1	Limites de performance	37
2.9.2	Limites de qualité pendant la phase d'enrôlement	37
2.9.3	Mécanismes de protection des modèles biométriques	37
2.10	L'empreinte digitale	38
2.10.1	Caractéristiques des empreintes	38
2.10.2	Le traitement d'une empreinte digitale	39
2.11	Conclusion	44

3 ANALYSE, MODÉLISATION ET CONCEPTION 45

3.1	Introduction	45
-----	------------------------	----

3.2	Le cahier de charges	45
3.2.1	Étude de l'existant	45
3.2.2	Identification des zones sensibles	46
3.3	Évaluation de la sécurité	49
3.3.1	L'évaluation des ressources	49
3.3.2	Identification des menaces	49
3.3.3	Identification des vulnérabilités	50
3.4	Fonctionnalités attendues du nouveau système	50
3.4.1	Expression des besoins fonctionnels	50
3.4.2	Expression des besoins de sécurité	51
3.4.3	Expression des besoins non fonctionnels	51
3.5	Étude de faisabilité	51
3.5.1	Étude de faisabilité politique	52
3.5.2	Étude de faisabilité organisationnelle	52
3.5.3	Étude de faisabilité opérationnelle	53
3.5.4	Étude de faisabilité technique	53
3.5.5	Étude faisabilité économique	54
3.6	Planification des activités du projet	54
3.7	Étude comparative des technologies biométriques	55
3.8	Architecture de notre système	56
3.8.1	Architecture globale	56
3.8.2	Architecture fonctionnelle	57
3.8.3	Matrice de contrôle d'accès	58
3.9	Les opérations réalisées par notre système	60
3.9.1	L'enregistrement	60
3.9.2	L'enrôlement	61
3.9.3	L'authentification /La vérification	62
3.9.4	L'identification	63
3.10	Modélisation	64
3.10.1	Les acteurs du système et leur but	64
3.10.2	Cas d'utilisation que réalise chaque acteur	64
3.10.3	Les diagrammes de cas d'utilisation	65
3.10.4	Description des cas d'utilisation	69
3.10.5	Les diagrammes d'activité	73
3.10.6	Diagramme de classe	76
3.11	Conclusion	76

4	MISE EN ŒUVRE DE LA SOLUTION	77
4.1	Introduction	77
4.2	Technologies et outils de développement	77
4.2.1	Langage et outils de modélisation	77
4.2.2	Langage de programmation	78
4.2.3	Les outils de développement	81
4.2.4	Choix du lecteur biométrique	82
4.3	Conclusion	83
5	RÉSULTATS ET COMMENTAIRE	84
5.1	Introduction	84
5.2	Page d'accueil application	84
5.3	Phase d'enregistrement	86
5.3.1	Enregistrement d'un employé de groupe 1	87
5.3.2	le badge d'un employé	88
5.4	Phase d'enrôlement	88
5.4.1	Connection à la base de données et choix du lecteur biométrique	89
5.4.2	Enrôlement	89
5.5	Phase d'authentification	90
5.5.1	Authentification d'un utilisateur légitime	90
5.5.2	Tentative d'usurpation d'identité	91
5.6	Conclusion	92
	CONCLUSION ET PERSPECTIVES	93
	RÉFÉRENCES	97
	ANNEXE A : ÉVALUATION DE SÉCURITÉ DE L'AÉROPORT	98
	ANNEXE B : ENQUÊTE DE TERRAIN	107

LISTE DES SIGLES ET ABRÉVIATIONS

ADC	Aéroport Du Cameroun
AIM	Aeronautical Information Management
APDU	Application Protocol Data Unit
AVSEC	Aviation Security
CCAA	Cameroon Civil Aviation Authority
CER	Cross Error Rate
CNI	Carte Nationale d'Identité
DME	Distance Measuring Equipment
EEPROM	Electrical Erasable Programmable Read Only Memory
FAR	False Acceptance Rate
FRR	False Reject Rate
GNSS	Global Navigation Satellite System
GP	Glide Path
HF	Heigh Frequency
IDE	Integrated Development Environment
ILS	Instrument Landing System
LLZ	Localizer
MABAC	Maroua-Salak Airport Biometric Access Control
MARAIC	Maroua-Salak Airport Restricted Aera Identification Card
MIRE	Maintenance des Infrastrutres Radio-électrique
NAVAID	Aide à la Navigation Aérienne
NDB	Non Directional Beacon
OACI	Organisation de l'Aviation Civile Internationale
PAPI	Path Approach Precision Indicator
PIN	Personnal Identification Number
PNC	Personnel Navigant Commercial
PNS	Programme National de Sûreté
PNT	Personnel Navigant Technique
PTS	Protocol Type Selection

RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read Only Memory
SDLC	System Development Life Cycle
SGBD	Système de Gestion de Base de Données
SLI	Sauvatage et Lutte contre Incendie
SQL	Structured Query Lnaguage
SecSDLC	Security System Development Life Cycle
UML	Unified Modeling Language
USAP	Universal Security Audit Program
VHF	Very Heigh Frequency
VIP	Very Important Person
VOR	VHF Omni-drectional Range

RÉSUMÉ

Le présent travail entre dans le cadre du mémoire de fin d'étude d'ingénieur de conception en sécurité informatique et cryptographie. Dans le cadre de la formation, le cursus scolaire prévoit un stage de fin d'études permettant d'apprendre à identifier et à utiliser efficacement les méthodes scientifiques acquises durant nos années d'étude à la résolution des problèmes de terrain. C'est dans cette optique que nous avons effectué notre stage de fin d'études à l'Aéroport International de Maroua-Salak , un environnement marqué par des exigences fortes et strictes en matière de sûreté et de sécurité, seul gage de l'émergence d'une aviation civile sûre et fiable.

Sur le terrain, nous avons constaté que l'identification des personnes désirant accéder aux zones réservées de l'aéroport se fait à travers la présentation d'une pièce d'identification (CNI, Badge, Passport). Cette méthode de contrôle d'accès a un problème évident car, le document présenté pour l'authentification peut être facilement volé, falsifié, dupliqué, copié, emprunté ou corrompu. Il s'agit d'un problème sérieux d'autant plus que l'identification des personnes désirant accéder à ces zones est une exigence de l'organisation mondiale de l'aviation civile éditée dans son Annexe 17.

Sur le plan scientifique, il est prouvé que la biométrie est aujourd'hui le moyen le plus fiable et efficace pour l'identification des personnes. Le présent mémoire vise à résoudre le problème sus-mentionné par une solution de contrôle d'accès biométrique.

Pour y arriver, nous nous proposons de concevoir et implémenter une méthode simple, efficace et efficiente pour la gestion des autorisations d'accès dans l'enceinte de l'Aéroport Internattional de Maroua-Salak à travers une solution de contrôle d'accès biométrique basée sur la vérification de l'empreinte digitale. Notre solution que nous appellerons MABAC : MAROUA-SALAK AIRPORT BIOMETRIC ACCESS CONTROL, comportent cinq opérations dont deux opérations clé : l'enrôlement et l'authentification. Durant la phase d'enrôlement, l'empreinte de la personne est capturée, les minuties sont extraites et stockées dans la base de données comme modèle de référence pour cette personne associée à son matricule. Pour l'authentification, l'empreinte de la personne est encore capturée et les minuties extraites. Le modèle de test ainsi obtenu est comparé avec le modèle de référence stocké dans la base de données ; s'il y a correspondance, la personne est

authentifiée.

Notre étude adopte une approche qualitative ; pour l'implémentation, le langage de programmation Java est utilisé avec Mysql en arrière plan pour stocker les modèles biométriques et le lecteur biométrique Digital Persona U.are.U 4500 est utilisé pour capturer l'image de l'empreinte.

Mots clés : biométrie, authentification, identification, enrôlement, sûreté, sécurité.

ABSTRACT

The present work is a part of Master of engineering course in computer security and cryptography. As part of the training, the school curriculum includes a final internship in which, we have to learn how to identify and effectively use the scientific tools acquired during our study to solve real world problems.

It is with this in mind that we did our end-of-studies internship at Maroua-Salak International Airport, a field marked by strong and strict requirements in terms of safety and security the guarantee of the emergence of a safe and reliable civil aviation. At the airport, we found that identification and authentication of people wishing to access the airport restricted area has been through the presentation of medium of authentication such as ID cards, badge or passport. This method of authenticating a person has an obvious problem such as presentation of fake clearance card, impersonation and so on. It is a serious safety and security issue since the identification of people wishing to access airport restricted area is a requirement of the International Civil Aviation Organization published in Annex 17.

From the scientific point of view, it is proven that biometric techniques have become a prominent option and secured means of authentication capable of sustaining the emerging ubiquitous computing.

The purpose of this memo is to solve the aforementioned problem with a biometric access control solution. To achieve this, we propose to design and implement a simple, effective, efficient and reliable method to manage airport access clearance at the Maroua-Salak International Airport enclosure through a fingerprint verification.

The proposed Maroua-Salak Airport Biometric Access Control (MABAC) uses fingerprint identification in Airport access control. It has five operations with two main operations called enrollment and authentication. During the enrollment stage, the person's fingerprint is captured, minutiae are extracted and stored in the database as a template for that person associated with his personnel number. For authentication, the person's fingerprint is captured again and minutiae extracted, the template thus obtained is compared with the template stored in the database; if there is a match, the person is authenticated.

The study adopted a qualitative research method. The model was implemented using java programming language and the back-end makes use of MySQL as the database as well as the template. Digital Persona U.are.U 4500 fingerprint scanner was used to capture live fingerprint image.

Key words : biometric, authentication, identification, enrollment, safety, security.

LISTE DES TABLEAUX

3.1	Identification des ressources à protéger	48
3.2	Menaces identifiées	50
3.3	Identification des vulnérabilités	50
3.4	Tableau comparatif des technologies biométriques	56
3.5	Matrice de contrôle d'accès	58
3.6	Matrice de contrôle d'accès réduite	59
3.7	Les acteurs du système et le but	64
3.8	Cas d'utilisation que réalise chaque acteur	64
3.9	Description du cas d'utilisation enregistrer employé	69
3.10	Description du cas d'utilisation enrôler employé	70
3.11	Description du cas d'utilisation enrôler employé	71
3.12	Description du cas d'utilisation identifier employé	72
3.13	Description du cas d'utilisation du sous système audit	73

LISTE DES FIGURES ET ILLUSTRATIONS

1.1	Organigramme du Commandement de l'Aéroport de Maroua-Salak	5
1.2	Méthodologie SecSDL	9
2.1	Architecture d'une carte à puce	20
2.2	Communication entre la carte et le lecteur	21
2.3	Les accessoires de la technologie RFID	23
2.4	Les caractéristiques biométriques	25
2.5	Reconnaissance faciale	26
2.6	L'empreinte digitale	26
2.7	La géométrie de la main	27
2.8	La rétine	28
2.9	L'iris	29
2.10	La voix	29
2.11	La signature manuscrite	30
2.12	La dynamique du clavier	31
2.13	Architecture d'un système de reconnaissance biométrique	32
2.14	Enrôlement d'un utilisateur	33
2.15	Vérification d'un utilisateur	33
2.16	L'identification d'un utilisateur	34
2.17	Le seuil d'efficacité	36
2.18	Caractéristiques d'une empreinte digitale	39
2.19	Phase de prétraitement	40
2.20	Phase de binarisation	41
2.21	Phase de squelettisation	42
2.22	Extraction des minuties	43
3.1	Représentation des zones sensibles	48
3.2	planification des tâches	55
3.3	Architecture globale	57
3.4	Architecture fonctionnelle	57

3.5	Matrice de contrôle d'accès	60
3.6	L'enrôlement	61
3.7	L'authentification /vérification	62
3.8	L'identification	63
3.9	Diagramme de cas d'utilisation du système global	65
3.10	Diagramme de cas d'utilisation du sous système enregistrement	66
3.11	Diagramme de cas d'utilisation du sous système enrôlement	66
3.12	Diagramme de cas d'utilisation du sous système authentification	67
3.13	Diagramme de cas d'utilisation du sous système identification	67
3.14	Diagramme de cas utilisation du sous système auditer	68
3.15	Diagramme d'activité du sous système enregistrement	73
3.16	Diagramme d'activité du sous système enrôlement	74
3.17	Diagramme d'activité du sous système authentification	74
3.18	Diagramme d'activité du sous système identification	75
3.19	Diagramme de classe système MABAC	76
4.1	Implémentation de la base de données	79
4.2	Visualisation des tables 1	80
4.3	Visualisation des tables 2	81
4.4	Lecteur biométrique	83
5.1	Page de login à l'application	85
5.2	Page d'accueil de l'application	86
5.3	Enregistrement d'un employé de groupe 1	87
5.4	Architecture d'un système de reconnaissance biométrique	88
5.5	Connexion à la base de données et choix du lecteur	89
5.6	Enrôlement d'un employé	90
5.7	Authentification d'un utilisateur légitime	91
5.8	Tentative d'usurpation d'identité	92

INTRODUCTION GÉNÉRALE

Les tragiques événements du 11 Septembre 2001 ont choqué le monde entier en général et la communauté aéronautique en particulier. Dès lors, le débat se pose sur le niveau de sécurité assuré dans les aéroports, l'efficacité des mesures de sûreté mises en œuvre et leur capacité à faire face aux menaces que pèsent le terrorisme et d'autres formes de violence sur les activités aéronautiques. Plusieurs mesures ont été prises afin d'atténuer les risques d'une attaque terroriste sur l'industrie aéronautique. On peut citer entre autres l'élargissement de la zone de sûreté en faisant passer certaines zones publiques à accès libre comme une zone de sûreté à accès réglementé ou encore le verrouillage à l'intérieur du cockpit d'un avion de ligne.

L'on remarque dès lors que l'ensemble de ces mesures concerne pratiquement les visiteurs et les passagers. Très peu de mesures sont relatives aux personnes qui travaillent au sein de l'aéroport, pourtant il s'agit d'un environnement hétérogène où plusieurs institutions travaillent en collaboration. Cependant chaque institution a ses propres critères de recrutement et sa propre politique de sécurité. Dès que des agents sont amenés à travailler de façon continue ou temporaire au sein de l'Aéroport International de Maroua-Salak, ils utilisent généralement un badge d'identification délivré par leur institution ou toute autre pièce d'identification reconnu et valide pour être autorisé à accéder à l'enceinte aéroportuaire.

L'absence d'un mécanisme sûr, efficace et fiable d'identification des employés autorisés à accéder aux zones réservées de l'aéroport est une brèche dans le système de sécurité et de sûreté de l'aéroport. L'expérience qui nous vient du domaine de la sécurité informatique nous enseigne que la sécurité globale d'un système d'information est celle de son maillon le plus faible ; il semble évident qu'une faille dans le dispositif de contrôle d'accès physique du personnel est une menace sérieuse qui peut compromettre l'ensemble des mesures de sécurité et de sûreté mises en œuvre.

L'Aéroport International de Maroua-Salak est comme tous les aéroports du Cameroun un espace public à forte densité de personnes. Ce pendant l'environnement aéroportuaire est confronté à un challenge majeur ; il s'agit en effet de concilier la sûreté et la facilitation. C'est-à-dire la capacité à mettre en œuvre des mesures visant à

protéger les personnes, leurs biens, les bâtiments, les avions, et les installations contre les actes d'interventions illicites, tout en assurant une facilité d'accès et de circulation au sein de l'enceinte aéroportuaire. L'authentification et l'identification des personnes désirant accéder aux zones réservées d'un aéroport est une exigence de l'Organisation Mondiale de l'Aviation Civile (OACI) dans sont annexe 17 : "*Chaque État contractant veillera à ce que des systèmes d'identification de personnes et de véhicules soient mis en place pour empêcher les accès non autorisé aux zones côté piste et aux zones de sûreté à accès réglementé. L'identité sera vérifiée aux points de contrôle d'accès désigné avant d'autoriser l'accès à ces zones*".[26]

L'identification et l'authentification des personnes se font manuellement à travers un badge d'identification délivré par l'institution qui emploi cette personne. Ce système n'est pas à l'abri de la fraude, de la contrefaçon et en plus il est difficile de garder un enregistrement fiable du mouvement des personnes au sein de l'aéroport. Le besoin d'un moyen d'authentification plus fiable et efficient apparait et la biométrie semble être la meilleur solution à cette préoccupation. C'est dans cet optique qu'il nous a été demandé d'axer nos études sur le thème « **Sécurisation de l'Aéroport International de Maroua-Salak par une solution de contrôle d'accès biométrique.** »

Notre solution que nous appellerons MABAC: Maroua-Salak Airport Biometric Access Control vise à concevoir et implémenter une solution contrôle d'accès biométrique pour l'authentification des personnes désirant accéder aux zones réservées de l'aéroport.

Le présent travail est structuré autour de cinq chapitres ; dans le premier chapitre, il sera question de présenter de manière brève l'environnement du stage, de situer le sujet dans son contexte et de dégager la problématique qui en ressort. Le deuxième chapitre portera sur les généralités liées à notre sujet , c'est-à-dire que nous présenterons de manière sommaire la problématique de sécurité et sûreté dans l'aviation civile, le contrôle d'accès et l'authentification biométrique. Dans le troisième chapitre, nous décrirons l'architecture et le fonctionnement de notre solution MABAC ainsi que les fonctionnalités attendues de notre système. La quatrième partie sera consacrée à l'implémentation notre solution, tout en passant en revu les outils de développement et le matériel utilisé. Et pour terminer le cinquième chapitre sera consacré à l'analyse des résultats obtenus.

CONTEXTE ET PROBLÉMATIQUE

1.1 Introduction

Dans ce chapitre, il sera question pour nous de décrire le contexte dans lequel a été réalisé notre travail. Nous présenterons l'Aéroport International de Maroua-Salak, les différents acteurs qui concourent à son fonctionnement, leur rôle et la structure qui nous a accueillis. Puis nous présenterons la problématique liée à notre sujet ainsi que les objectifs visés par notre travail. Enfin nous définirons la méthodologie utilisée tout au long de notre travail.

1.2 Présentation de l'Aéroport International de Maroua-Salak

L'Aéroport International de Maroua-Salak est, après les Aéroports de Douala, Yaoundé et Garoua le quatrième aéroport international du Cameroun. Il est situé à 18 Km au Sud-Est de la ville de Maroua, chef lieu département du Diamaré dans la Région de l'Extrême-Nord Cameroun et au lieu-dit Salak. Il s'agit d'un aéroport moderne (sur le plan des installations et services de la navigation aérienne) et ouvert à la circulation aérienne publique.

1.2.1 Historique de l'aéroport

1950 : Construction de l'Aéroport de Maroua-Salak sous la gestion de l'Etat.

05/07/1952 : Ouverture de l'Aéroport de Maroua-Salak à la circulation aérienne public.

1974 : La gestion de l'Aéroport est confiée à l'ASECNA.

12/08/1994 : Signature de la Convention de concession entre l'État et les A.D.C pour la gestion des Aéroports du Cameroun.

01/10/1994 : Démarrage des activités des A.D.C.

28/11/1994 : Signature du Contrat de Sous-traitance de la partie technique des Aéroports de l'Ex. Article 10 entre A.D.C. S.A et ASECNA.

31/12/2003 : Résiliation du Contrat de Sous-traitance.

2003 - 2007 : Réhabilitation de la Piste d'atterrissage.

01/10/2008 : Début de la fourniture des services de la navigation aérienne à l'Aéroport de Maroua-Salak par la CCAA.

2011 : Installation d'un balisage lumineux haute intensité.

2013 : Acquisition des équipements modernes de sécurité incendie et installation d'un VOR Conventionnel couplé à un DME

16/04/2014 : Signature de l'arrêté portant transformation de l'aéroport à l'international.

Installation d'une nouvelle centrale électrique.

Installation d'un Système l'atterrissage aux Instruments (ILS Cat II).

Installation d'une station météo automatique.

2015 : Renouvellement de la convention Etat-ADC de concession de l'aéroport à ADC.

1.2.2 Les acteurs

Plusieurs acteurs participent aux activités qui font vivre l'Aéroport International de Maroua-Salak. Parmi ces différents acteurs, trois principaux groupes sont à retenir :

L'État du Cameroun

C'est lui le propriétaire de l'aéroport ; il est le principal responsable de l'aéroport et agit dans les domaines de la sûreté et de la supervision de l'ensemble des activités aéroportuaires. Il s'appuie sur plusieurs institutions étatiques pour atteindre ses objectifs notamment :

L'Autorité Aéronautique du Cameroun(CCAA) qui est responsable des activités de supervision de la sécurité de la navigation arienne et de la sûreté de l'aviation civile.

La police qui assure les fonctions relatives à la sûreté (le contrôle de sûreté des passagers, du personnel et des bagages).

La gendarmerie qui est responsable de la sécurité des personnes et des installations situées du côté piste.

La douane qui s'occupe des question relatives aux entrées et sorties des biens.

Autres : il s'agit des services du tourisme, de la poste, phytosanitaire et de santé publique.

.

Le gestionnaire de l'aéroport (ADCSA)

Il est responsable des questions liées à la viabilisation de l'aéroport, il s'occupe du confort des passagers et de l'assistance aux compagnies aériennes. Il est également responsable de la promotion de l'image de l'aéroport, de son développement et s'occupe en général de la supervision de toutes les activités à caractères commerciales exercées à l'aéroport.

L'affectataire (CCAA)

C'est elle qui est responsable de la fourniture des services de la navigation aérienne et de l'assistance météorologique à la navigation aérienne.

A coté de ces trois acteurs majeurs, on note la présence d'autres acteurs notamment, les compagnies aériennes, les commerçants, les agences de location de voitures et les hôtels.

1.3 Présentation du Commandement de l'Aéroport International de Maroua-Salak

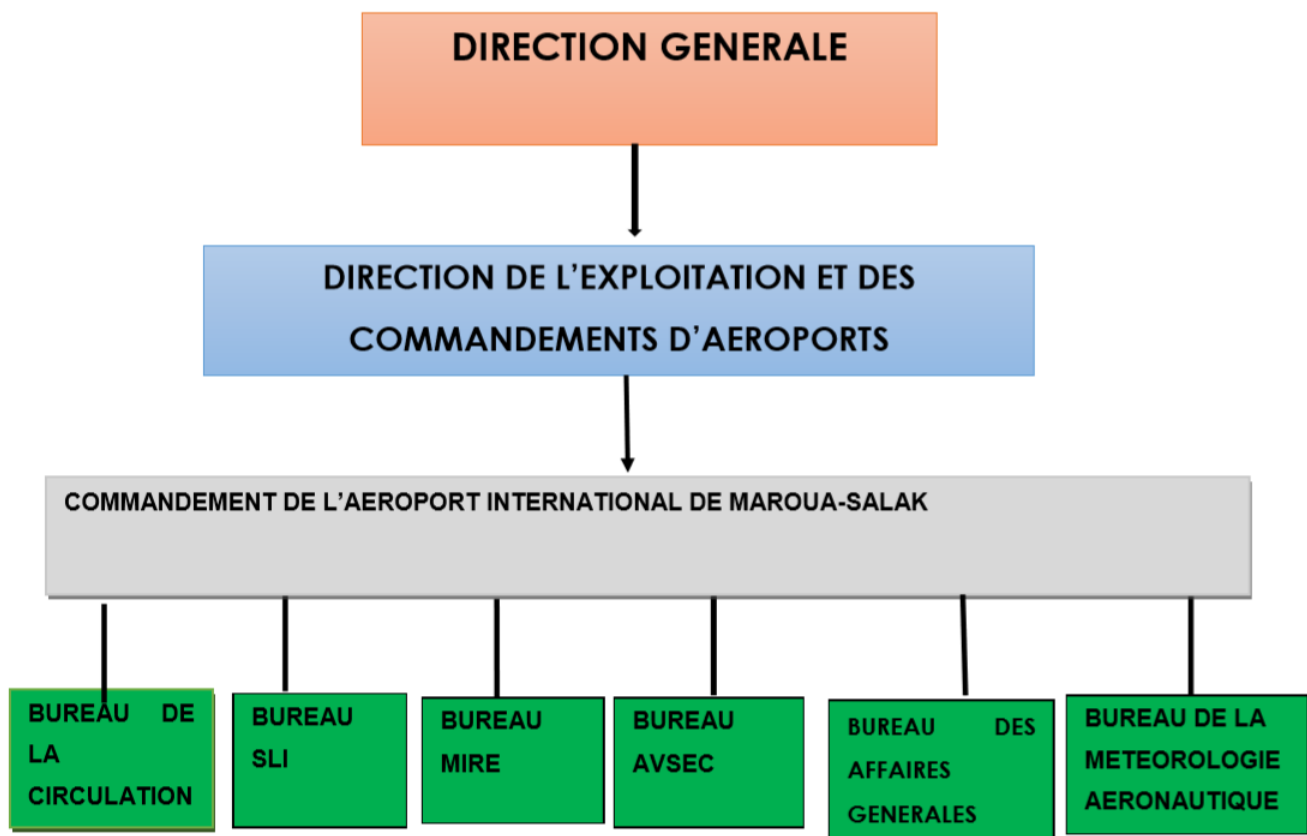
Il est la représentation de l'Autorité Aéronatique du Cameroun dans la Région de l'Extrême Nord. C'est au sein de cette institution que nous avons effectué notre stage de fin d'études.

1.3.1 Sa mission

D'après le plan d'organisation de l'Autorité Aéronautique, le Commandement de l'Aéroport est chargé entre autres :

- De la fourniture des services de la navigation aérienne ;
- De la gestion de l'aéroport ;
- Des questions relatives à la sûreté de l'aviation civile, à la facilitation aéroportuaire et à la sécurité des vols.

1.3.2 Son organigramme



Source: Manuel d'exploitation du Bureau circulation aérienne

FIGURE 1.1 – Organigramme du Commandement de l'Aéroport de Maroua-Salak

1.3.3 Son fonctionnement

Placé sous l'Autorité du Commandant d'Aéroport, l'Aéroport International de Maroua-Salak est ouvrable tous les jours de la semaine de 08h à 18h. Sur le plan fonctionnel et administratif le Commandement de l'Aéroport de Maroua-Salak comporte sept (07) Bureaux à savoir :

1. le Bureau de la circulation aérienne (CA) ;
2. le Bureau de la gestion de l'information aéronautique (AIM) ;
3. le Bureau de Maintenance des Infrastructures Radioélectriques (MIRE) ;
4. le Bureau de l'assistance météorologique (METEO) ;
5. le Bureau de sauvetage et de lutte incendie (SLI) ;
6. le Bureau de la sûreté de l'aviation civile (AVSEC) ;
7. le Bureau des Affaires Générales.

1.4 Contexte et Problématique

L'Aéroport International de Maruoa Salak est un aéroport ouvert à la circulation aérienne publique ; par conséquent est sous réserve du respect des contraintes liées à la longueur et à la structure physique de sa piste d'atterrissage capable d'accueillir tout type d'avion quelque soit l'opérateur qui l'exploite. Il est depuis plusieurs années engagé dans un processus de modernisation ayant conduit à l'acquisition et l'installation des aides à la navigation aérienne permettant des atterrissages de précision, la conception des nouvelles procédures de vol exploitant les possibilités de navigation offerte par la GNSS, ce qui a considérablement amélioré son accessibilité en permettant des atterrissages de nuit et par mauvaise visibilité. En cette période même où se déroule notre stage, les travaux de construction d'un poste d'inspection filtrage moderne est en cours et doit à terme permettre de renforcer le dispositif de sûreté en place pour le contrôle des passagers et leurs bagages. Par contre le dispositif de contrôle d'accès physique du personnel est un système manuel, basé sur l'identification des personnes via des documents tels que le badge d'identification, la CNI, le passeport ou toutes autres pièces d'identification. Dans cet environnement hétérogène, ou plusieurs organisations aux activités et objectifs différents se côtoient et participent par leurs activités au fonctionnement de l'aéroport. Ce dispositif semble être peu fiable, d'autant plus que les systèmes d'authentification par carte, les numéros PIN, les clés ou autres informations d'identification permettant à quiconque les possède d'y accéder , ne peuvent pas être contrôlés efficacement parce qu'ils sont si facilement perdus, volés, empruntés, copiés ou compromis . Ces problèmes inhérents pourraient éventuellement être exploités par un criminel, y compris un terroriste, qui souhaitent avoir accès aux installations et équipements sensibles de l'aéroport. Bien que le contrôle d'accès puisse être le principal facteur contribuant à

sa vulnérabilité, le contexte sécuritaire que connaît la région oblige les autorités aéroportuaires à accorder une attention particulière à cette menace. Une brèche dans le système de contrôle d'accès de l'aéroport pourrait compromettre l'ensemble des mesures de sécurité suscitées et avoir des conséquences graves sur la sécurité des installations, des équipements, des aéronefs, des personnes et de leurs biens. Il faut donc empêcher les accès non autorisés à l'enceinte aéroportuaire par une méthode d'authentification fiable et efficace. Le besoin d'un meilleur système qui protège les zones réservées contre les accès non autorisés semble être justifié et nous amène à nous poser les questions suivantes :

- Quel est la solution adéquate à mettre en place pour authentifier les personnes qui accèdent aux équipements et installations sensibles de l'aéroport ?
- Comment mettre en place un mécanisme simple et efficace permettant de s'assurer que seuls les employés auxquels des privilèges d'accès ont été accordés à des "zones sensibles" en conformité avec leur "zones de travail" respectives peuvent accéder à ces zones ?
- Comment renforcer le dispositif de contrôle d'accès physique des personnes et surveiller la circulation des personnes dans les différentes zones réservées de l'aéroport ?

1.5 Objectifs

1.5.1 Objectif Général

Notre travail vise à concevoir et implémenter une solution de contrôle d'accès simple, efficace et fiable pour l'authentification des personnes, la gestion des autorisations d'accès dans les zones réservées de l'aéroport et le contrôle du mouvement des personnes dans les zones sensibles de l'aéroport en conformité avec leurs zones de travail respectives. La mise en œuvre de notre solution aboutira à deux livrables. La première, le MABAC (Maroua-Salak Airport Biometric Access control) est une application qui permet l'identification, et l'authentification des personnes basées sur la vérification de l'empreinte digitale et la seconde, le MARAIC (Maroua-Salak Airport Restricted Area Identification Card) est un badge d'identification équipé de la technologie RFID et qui précise les différentes zones de l'aéroport auxquelles une personne particulière est autorisée à accéder. Notre travail se limite au contrôle d'accès du personnel de l'aéroport c'est-à-dire des personnes qui sont amenées à exercer de manière temporaire ou permanente, une fonction spécifique aux sein de l'aéroport. Les passagers, quant à eux, sont pris en

compte dans une procédure sûre conformément aux exigences réglementaires. Les visiteurs et les accompagnateurs ne sont pas autorisés à accéder aux zones réservées de l'aéroport ; sauf en cas de nécessité, ils doivent être accompagnés.

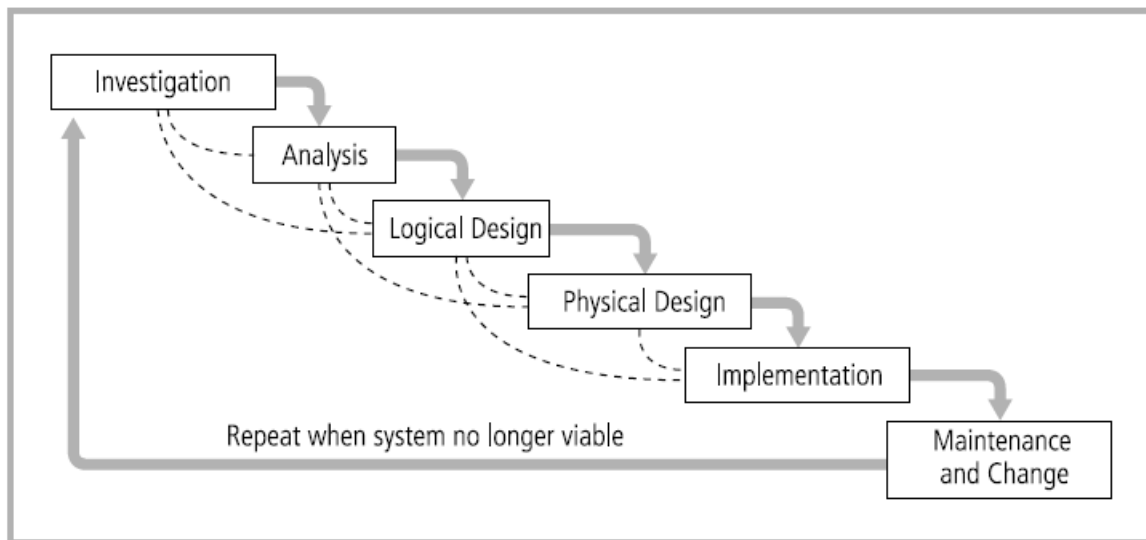
1.5.2 Objectifs Spécifiques

Sur un plan sécuritaire la mise en œuvre de notre solution permettra d'atteindre les objectifs suivants :

- Fournir une méthode d'authentification et d'identification des personnes basée sur la vérification de l'empreinte digitale.
- Informatiser et sécuriser la gestion des badges d'identification par la mise sur pieds d'un badge unique (MARAIC).
- Fournir une matrice de contrôle d'accès basée sur le rôle que joue chaque employé au sein de l'aéroport.
- Améliorer l'accessibilité de l'aéroport par la réduction du temps de contrôle d'accès.
- Renforcer le dispositif global de sécurité et de sûreté de l'aéroport.

1.6 Méthodologie

Afin d'apporter une solution nous permettant d'atteindre les objectifs sus-cités et d'obtenir les résultats escomptés, nous utiliserons la méthodologie Security System Development Life Cycle (SecSDLC). Cette méthodologie est une adaptation de la méthodologie System Development Life Cycle utilisée pour la conception et l'implémentation des systèmes d'information. Elle tire avantage de la SDLC traditionnelle par la mise en œuvre de la sécurité de l'information dans chaque activité, ce qui implique l'identification des menaces et la création des contrôles spécifiques pour contrer ces menaces. Cette méthodologie très adaptée pour la conception des systèmes de sécurité s'inspire de la norme ISO 27003 :2010 "Information security management system implementation guidance" et utilise un modèle en cascade constitué de plusieurs activités exécutées de façon séquentielles partant de l'investigation à la maintenance.



Source: Cangage course technologie

FIGURE 1.2 – Méthodologie SecSDL

L'adaptation de cette méthodologie à notre travail nous permet d'identifier les principales étapes suivantes pour la réalisation de nos objectifs :

Investigation

Étape 1 : Étude de la méthode de contrôle d'accès existante.

Étape 2 : Évaluation des ressources existantes.

Étape 3 : Description de la portée et des objectifs de notre projet.

Analyse

Étape 4 : Identification des zones sensibles de l'aéroport.

Étape 5 : Identification des actifs à protéger.

Étape 6 : Identification des menaces.

Étape 5 : Identification des vulnérabilités de la méthode de contrôle d'accès existante.

Étape 6 : Étude du risque.

Conception logique

Étape 7 : Expression des besoins de sécurité.

Étape 8 : Expression des besoins fonctionnels.

Étape 9 : Expression des besoins non fonctionnels.

Étape 10 : Revue des différentes solutions possibles.

Étape 11 : Étude de faisabilité.

Conception physique

Étape 12 : Étude comparative des différentes technologies biométriques

Étape 13 : Choix des meilleures technologies adaptées à nos besoins.

Étape 14 : Conception de notre solution.

Étape 15 : Évaluation de notre solution au regard des besoins exprimés aux étapes 7, 8 et 9.

Implémentation

Étape 16 : Choix des cartes à puce et lecteurs de carte.

Étape 17 : Choix du lecteur biométrique.

Étape 18 : Choix des technologies et outils de développement.

Étape 19 : Choix du langage de programmation.

Étape 20 : Développement et codage de l'application

Étape 21 : Test de notre solution et présentation aux acteurs.

Maintenance et changement

Étape 22 : Mise en place d'une procédure de contrôle de performance.

1.7 Conclusion

Ce chapitre nous a permis de définir le contexte ainsi que la problématique dégagée par notre sujet. Il nous a permis de ressortir quelques objectifs claires qui une fois à terme permettra de renforcer la sécurité de l'aéroport, ceci en optant pour une solution d'authentification biométrique basée sur la vérification de l'empreinte digitale.

GÉNÉRALITÉS

2.1 Introduction

Le présent chapitre aborde les généralités liées à notre sujet. Il sera question pour nous de présenter l'ensemble des éléments nécessaires à la compréhension des notions abordées dans notre travail. Nous y passerons en revue, les notions sur la sûreté et la sécurité de l'aviation civile, les technologies d'authentification et de contrôle d'accès, la biométrie et les technologies d'authentification biométrique.

2.2 Sûreté de l'aviation civile et contrôle d'accès des personnes

L'aviation civile est aujourd'hui le moyen de transport le plus sûr au monde. Pourtant, à première vue, elle semble être l'une des activités civiles la plus dangereuse. Elle a pu maintenir un très bon niveau de sécurité et gagner la confiance des utilisateurs en s'appuyant sur des normes de sécurité très strictes et en investissant d'énormes moyens dans les technologies innovantes.

2.2.1 Définition et objectif de la sûreté de l'aviation

La sûreté de l'aviation civile est une combinaison de mesures et ressources humaines et matérielles destinées à protéger l'aviation civile contre les actes d'intervention illicite. Elle a pour principal objectif, d'assurer la protection et la sécurité des passagers, des membres d'équipage, du personnel au sol, du public, des aéronefs et des installations aéroportuaires servant à l'aviation civile, contre les actes d'interventions illicites perpétrés au sol ou en vol. [26] La mise en œuvre des mesures de sûreté doit être compatible avec les normes de l'Organisation Mondiale de l'Aviation Civile.

Norme : toute spécification portant sur les caractéristiques physiques, la configuration,

le matériel, les performances, le personnel, et les procédures, dont l'application est uniforme est nécessaire à la sécurité ou à la régularité de la navigation aérienne internationale et à laquelle les États contractants sont tenus de se conformer en application des dispositions de la convention. [26] Elle révèle un caractère obligatoire auquel chaque État contractant est tenu de s'y conformer à moins de publier une différence.

Pratique recommandée : toute spécification portant sur les caractéristiques physiques, la configuration, le matériel, les performances, le personnel, et les procédures, dont l'application est uniforme est reconnu souhaitable dans l'intérêt de la sécurité, la régularité ou de l'efficacité de la navigation aérienne internationale et à laquelle les États contractants s'efforceront de se conformer en application des dispositions de la convention. [26]

2.2.2 Dispositions réglementaires en matières du contrôle d'accès

Les dispositions réglementaires relative au contrôle d'accès des personnes dans les zones de sûreté à accès réglementé de l'aéroport sont décrites dans la section 4.2 de l'Annexe 17. Il s'agit d'un ensemble de normes et recommandations édictées par l'Organisation Mondiale de l'Aviation Civile que nous reprenons ici :

Norme 4.2.1 : chaque État contractant veillera à ce que l'accès aux zones coté piste dans les aéroports servant à l'aviation civile soit contrôlé afin d'empêcher les entrées non autorisées.[26]

Norme 4.2.2 : chaque État contractant veillera à ce que soient établies à chaque aéroport des zones de sûreté à accès réglementé désignées par l'État sur la base d'une évaluation des risques de sûreté effectuée par les autorités nationales pertinentes.[26]

Norme 4.2.3 : chaque État contractant veillera à ce que des systèmes d'identification de personnes et de véhicules soient mis en place pour empêcher les accès non autorisés aux zones côté piste et aux zones de sûreté à accès réglementé. L'identité sera vérifiée aux points de contrôle désignés avant d'autoriser l'accès à ces zones.[26]

Norme 4.2.4 : chaque État contractant veillera à ce que les personnes autres que les passagers auxquelles est accordé un accès non accompagné aux zones de sûreté à accès réglementé de l'aéroport fassent préalablement l'objet d'une vérification de leurs antécédents.[26]

Norme 4.2.5 : chaque État contractant veillera à ce que les mouvements de personnes et de véhicules autour des aéronefs fassent l'objet de surveillance dans les zones de

sûreté à accès réglementé, afin d'empêcher l'accès des aéronefs aux personnes non autorisées.[26]

Norme 4.2.6 : chaque État contractant veillera à ce que les personnes autres que les passagers, de même que les articles qu'elles transportent, avant leur entrée dans les zones de sûreté à accès réglementé des aéroports servant à l'aviation civile internationale, fassent l'objet de mesures d'inspection/filtrage et de contrôles de sûreté. [26]

Norme 4.2.7 : chaque État contractant veillera à ce que les véhicules autorisés à pénétrer dans des zones de sûreté à accès réglementé, de même que les objets qu'ils transportent, fassent l'objet d'une inspection/filtrage ou d'autres contrôles de sûreté appropriés, en fonction de l'évaluation des risques réalisée par les autorités nationales compétentes.

Recommandation 4.2.9 : il est recommandé que chaque État contractant veille à ce que les vérifications spécifiées au 4.2.4 soient répétées de façon régulière pour toutes les personnes auxquelles est accordé un accès non accompagné aux zones de sûreté à accès réglementé. [26]

2.2.3 Nature des menaces

Les menaces qui pèsent sur l'aviation civile peuvent être de sources diverses, on peut citer entre autres :

- Sabotages d'aéronefs ;
- Sabotages d'aéroports ;
- Détournement d'aéronef au sol ou en vol et ;
- Attaque armée au sein des installations aéroportuaires et hors de l'aéroport.[25]

2.2.4 Types d'agresseurs

- Personnes mentalement instables ;
- Personnes cherchant à se venger ;
- Anciens employés mécontents ;

- Terroriste (individus et groupes).

2.2.5 Motivations

Motivations terroristes

- Réactions vives des gouvernements, des organisations et des compagnies aériennes affectées ;
- Les compagnies aériennes sont souvent le symbole de leur Etat, et l'attaque est en réalité dirigée contre le pays ou le gouvernement ;
- Très grandes publicités pour leur cause auprès des médias ;
- Chercher à attirer l'attention de la communauté internationale sur leur cause, et en faire une publicité ;
- Cibler des individus précis à bord de l'aéronef, tels que diplomates ou personnalités importantes ;
- Semer la peur de prendre l'avion chez le public et interrompre la vie de tous les jours ;
- Obtenir la libération des prisonniers appartenant peut-être à leur groupe.

Motivations criminelles

- Appât du lucre ;
- Extorsion ;
- Motifs personnels ;
- Imprévisibles.

2.2.6 Les contre-mesures

Les contre-mesures peuvent être législatives, techniques et physiques[25].

Les contre-mesures législatives

Il s'agit d'un cadre réglementaire tel :

- La convention sur l'Aviation Civile Internationale, signé à Chicago le 7 Décembre 1944 ;
- La convention relative aux infractions et à certains autres actes survenant à bord des aéronefs, signée à Tokyo le 14 Septembre 1963 ;
- la convention sur la répression de la capture illicite d'aéronefs, signés à la Haye le 16 Octobre 1970 ;
- La convention sur la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, signée à Montréal le 23 Septembre 1971 ;
- La convention sur la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, signée à Montréal le 23 Septembre 1971 ;
- Le protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, complémentaire à la convention sur la répression d'actes illicites dirigés contre la sécurité de l'aviation civile, signée à Montréal le 23 Septembre 1971 ;
- Convention de Montréal sur le marquage des explosifs plastiques et en feuilles aux fins de détection, signée à Montréal le 1er Mars 1971 ;
- La convention de Beijing sur la répression des actes illicites dirigés contre l'aviation civile internationale signée le 10 Septembre 2010 à Beijing.

Les contre-mesures techniques

Il s'agit d'un arsenal de 19 annexes à la Convention de l'Aviation Civile Internationale dont l'Annexe 17 qui décrit les Normes et Pratiques recommandées visant à protéger l'Aviation Civile Internationale contre les actes d'interventions illicites.

Les contre-mesures physiques

- L'inspection du personnel ;
- L'inspection des membres d'équipage et du personnel au sol
- L'inspection des bagages, du fret et de la poste ;

- Protection de l'aéronef;
- Protection de l'aéroport et des installations destinées à la navigation aérienne.

2.2.7 Le contrôle d'accès des personnes

L'ensemble du personnel de l'aéroport est dans l'obligation d'utiliser les points de contrôle d'accès désignés lorsqu'il entre dans les zones à accès réglementé de l'aéroport (ceci s'applique également aux membres d'équipage des aéronefs). [26]

Zone de sûreté à accès réglementé : zone coté piste d'un aéroport dont l'accès est contrôlé pour garantir la sûreté de l'aviation civile. En règle générale, ces zones correspondent, notamment, toutes les zones de départ des passagers entre les postes de filtrage et les aéronefs, l'aire de trafic, les zones de tri de bagages, les entrepôts de fret, les centres de courriers, les zones de services de restauration cotés piste et les aires de nettoyages des aéronefs. [26]

Système des permis de l'aéroport : système de cartes, ou autres documents délivrés aux personnes employés dans l'aéroport ou qui ont, pour des raisons, besoins d'être autorisées à pénétrer dans l'aéroport, du coté piste ou dans la zone de sûreté à accès réglementé. Il a pour objet d'identifier la personne et de faciliter l'accès. [26]

2.3 Généralités sur le contrôle d'accès

Le contrôle d'accès est la méthode par laquelle les systèmes déterminent les conditions d'admission d'un utilisateur dans une zone de confiance de l'organisation ; c'est-à-dire du système d'information, les salles informatiques et l'ensemble des emplacements physiques. Il s'agit d'une fonction de sécurité qui contribue à satisfaire les exigences de sécurité exprimées en termes de disponibilité, d'intégrité, de confidentialité, d'authenticité et de non répudiation. [30] Il est réalisé au moyen d'une combinaison de politique, de programmes et de technologies et peut être obligatoire, discrétionnaire ou non discrétionnaire. En général, toutes les méthodes de contrôle d'accès s'appuient sur les mécanismes suivants : l'identification, l'authentification, l'autorisation et l'auditabilité.

2.3.1 L'identification

L'identification est un mécanisme par lequel une entité non vérifiée appelée utilisateur qui cherche à accéder à une ressource propose une étiquette par laquelle il est connu du

système. L'étiquette appliquée à l'utilisateur (ou fournie par celui-ci) est appelée identifiant (ID) et doit correspondre à une seule et unique entité dans le domaine de sécurité. [33]

2.3.2 L'authentification

L'authentification est le critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et de s'assurer que l'identité fournie correspond à l'identité de cette personne préalablement enregistrée.[10] Il est donc le processus de validation de l'identité présumée d'un utilisateur. Il existe trois mécanismes d'authentification largement utilisés :[33]

Ce que connaît l'utilisateur : ce facteur d'authentification repose sur ce que l'utilisateur sait et peut rappeler, par exemple, un mot de passe, une phrase secrète ou tout autre un code d'authentification, tel qu'un numéro d'identification personnel (PIN).

Ce que détient l'utilisateur : ce facteur d'authentification repose sur quelque chose que l'utilisateur possède ou peut produire si nécessaire. Tels que les cartes d'identité ou cartes avec bandes magnétiques contenant le PIN.

Ce qu'est l'utilisateur : ce facteur d'authentification repose sur des caractéristiques individuelles, telles que les empreintes digitales, les empreintes palmaires, la topographie de la main, la géométrie de la main, ou de la rétine et l'iris, ou encore quelque chose qu'un utilisateur peut produire à la demande comme la voix, la signature manuscrite ou des mesures cinétiques au clavier.

2.3.3 L'autorisation

L'autorisation est la mise en correspondance d'une entité authentifiée avec une liste de ressources, d'information et les niveaux d'accès correspondants. Cette liste est généralement une liste de contrôle d'accès ou une matrice de contrôle d'accès. Elle est généralement gérée d'une des trois façons suivantes :

Autorisation pour chaque utilisateur authentifié, dans laquelle le système effectue un processus d'authentification pour vérifier chaque entité, puis accorde l'accès aux ressources pour cette seule entité. Cela devient rapidement un processus complexe et gourmand en ressources dans un système informatique.

Autorisation pour les membres d'un groupe, dans laquelle le système correspond à authentifier les entités à une liste d'appartenance à un groupe, puis accorde l'accès aux

ressources en fonction des droits d'accès du groupe. C'est la méthode d'autorisation la plus courante.

Autorisation sur plusieurs systèmes, dans laquelle un système authentification centrale vérifie l'identité de l'entité et lui accorde un ensemble d'informations d'identification. Dans ce système, le ticket émis par le serveur d'authentification centrale est accepté par plusieurs systèmes appartenant au même domaine. [33]

2.3.4 L'auditabilité

La reddition de comptes, également appelée l'auditabilité, garantit que toutes les actions sur un système autorisées ou non autorisées peuvent être attribuées à une identité authentifiée. Cet audit peut être mis en œuvre pour diagnostiquer ou vérifier l'état de la sécurité d'un système ou encore pour déterminer s'il y a eu ou non violation de la politique de sécurité et, éventuellement quelles sont les ressources compromises. C'est également la fonction destinée à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité d'un environnement. Il est le plus souvent accompli au moyen de journaux systèmes, de journaux de bases de données et l'audit de ses enregistrements. [33]

2.4 Le contrôle d'accès physique

Le contrôle d'accès physique décide qui a accès à quelles ressources physiques, pour quelle période et sous quelles conditions. Les systèmes de contrôle d'accès physique utilisent plusieurs technologies de contrôle d'accès telles que les cartes à puce et la biométrie permettant d'authentifier un utilisateur et un certain nombre de techniques de contrôle d'accès afin de gérer les autorisations.

2.4.1 L'authentification

L'authentification dans un contrôle d'accès physique implique de vérifier l'identité d'un utilisateur par rapport aux données logiques stockées dans une base de donnée.

2.4.2 Les technologies du contrôle d'accès physiques

Les technologies de contrôle d'accès sont utilisées pour permettre l'authentification et la gestion des accès dans les systèmes de sécurité.

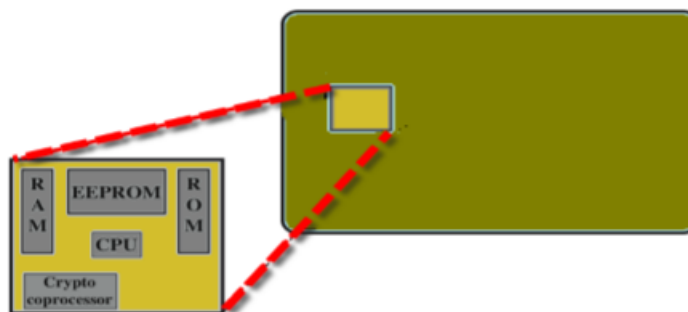
Les cartes à puces

Une carte à puce est un rectangle en plastique d'une épaisseur d'un millimètre environ qui porte un circuit intégré capable de mémoriser de façon sécurisée une série d'informations. Elle est généralement destinée à des fins d'authentification ou de paiement. Pour l'authentification des utilisateurs, la carte à puce sans contact est la plus utilisée ; elle s'apparente à une carte de crédit. Une carte à puce contient en son sein un microprocesseur entier, y compris un processeur, une mémoire et les ports d'entrées/sorties. Certaines versions intègrent un circuit de traitement spécial des opérations cryptographiques pour accélérer les tâches de codage et de décodage des messages ou pour générer signatures numériques et valider les informations transférées. Dans certaines cartes, les ports d'entrées/sorties sont directement accessibles par un lecteur compatible au moyen d'interface électrique pour les cartes à contact. Les cartes sans contact s'appuient plutôt sur une antenne intégrée pour la communication sans fil avec le lecteur. Une carte à puce typique comprend trois types de mémoire :

La mémoire en lecture seule (ROM) : stocke les données qui ne change pas pendant la vie de la carte, telles que le numéro de la carte et le nom du titulaire de la carte.

La ROM programmable effaçable électriquement (EEPROM) : contient des données et des programmes d'application, tels que les protocoles de communications. Il contient également des données qui peuvent varier avec le temps par exemple, un numéro de téléphone.

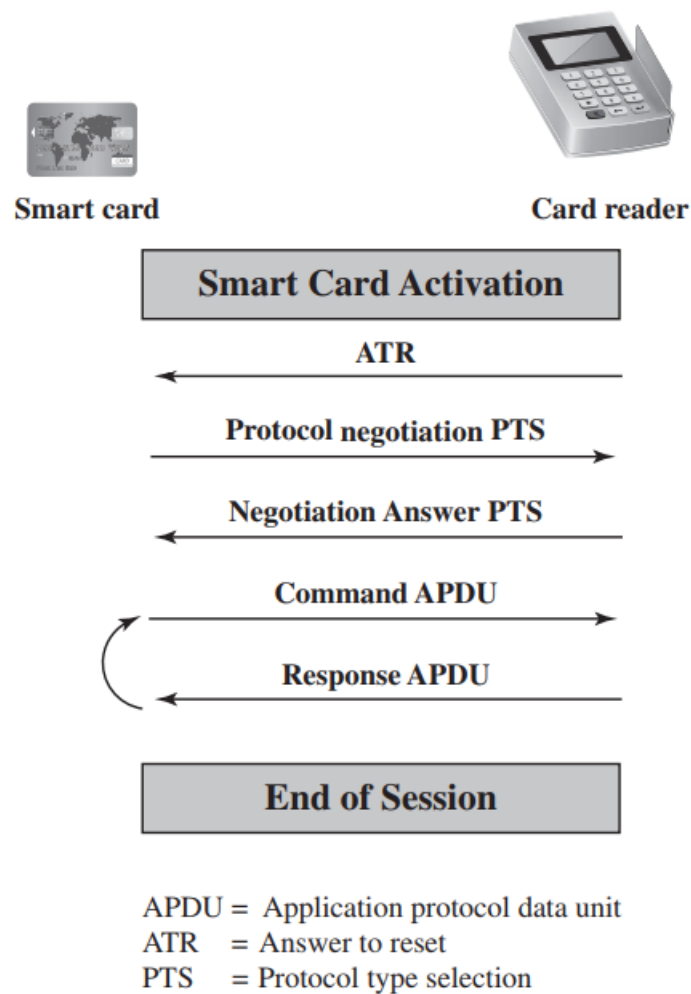
La mémoire (RAM) : contient des données temporaires générées lors de l'exécution des applications.



[11]

FIGURE 2.1 – Architecture d'une carte à puce

La communication entre la carte et le terminal se fait pas l'échange des APDU. C'est toujours la carte qui initie la conversation. En effet, chaque fois que la carte est insérée dans un lecteur, une reinitialisation est lancée par le lecteur pour initialiser des paramètres tels que la valeur d'horloge. Après que la fonction de réinitialisation soit effectuée, la carte répond avec le message de réponse à la réinitialisation (ATR). Ce message définit les paramètres et les protocoles que la carte peut utiliser et les fonctions qu'elle peut effectuer. Le terminal peut être en mesure de changer le protocole utilisé et d'autres paramètres via une commande de sélection de type de protocole (PTS). La réponse PTS des cartes confirme les protocoles et les paramètres à utiliser. Le terminal et la carte peuvent maintenant exécuter le protocole pour effectuer l'application souhaitée.[31]



[31]

Source: Stallings and Brown, Computer Security, 3rd Ed., Pearson 2015, p93

FIGURE 2.2 – Communication entre la carte et le lecteur

La RFID

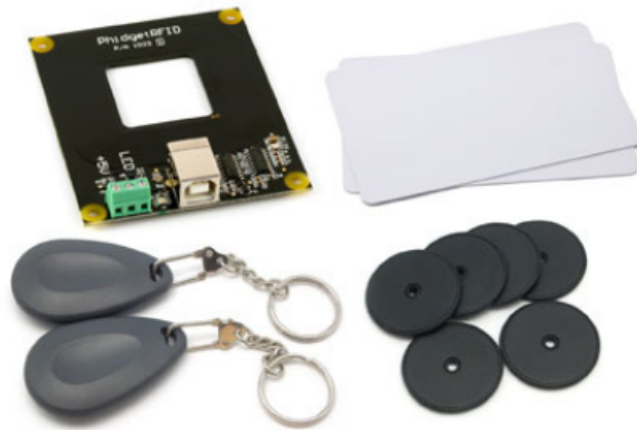
[17]

L'identification par radiofréquence (RFID) est une méthode d'identification automatique, basée sur le stockage et la récupération à distance des données à l'aide de dispositifs appelés transpondeurs. Un système typique consiste en un transpondeur avec un identifiant unique et intégré pour l'objet et des lecteurs conçus pour décoder les données sur le transpondeur et un système ou serveur hôte qui traite et gère les informations recueillies. Le transpondeur RFID est composé d'une antenne, d'une petite puce de silicium qui contient un récepteur radio, d'un modulateur radio pour envoyer une réponse au lecteur, d'un microprocesseur, d'une mémoire et d'un système d'alimentation. Différents types de transpondeurs RFID sont disponibles sur le marché : les transpondeurs actifs, les transpondeurs passifs et les transpondeurs semi-passifs.

Les Transpondeurs actifs : ils sont alimentés par batterie, et sont capables de diffuser à un lecteur sur des distances supérieures à 100 pieds.

Les transpondeurs passifs : ils ne sont pas alimentés par une batterie, mais tirent leur énergie d'un signal radio de faible puissance à travers son antenne. Le principal inconvénient avec ces transpondeurs est qu'ils ne peuvent transmettre que sur une courte distance, mais leur coût bon marché constitue leur principal avantage. Ils offrent également moins de possibilité en terme de cryptage et sont laissés ouverts aux attaques.

Les transpondeurs semi-passifs : ils tirent l'avantages des transpondeurs actifs et passifs pour offrir plus de sécurité. Comme les transpondeurs actifs , ils dispose d'une batterie, mais captent toujours leur énergie du lecteur pour transmettre un message. Ils ont donc la fiabilité en lecture d'un transpondeur actif mais la plage de lecture d'un transpondeur passif.



[17]

Source: Jing-Chiou Liou and Sujith Bhashyam, A Sophisticated RFID Application on Multi-Factor Authentication, Department of Computer Science Kean University, p 4

FIGURE 2.3 – Les accessoires de la technologie RFID

Les RFID viennent également dans plusieurs gammes de fréquences avec différents usages appropriés :

Basse fréquence (125 / 134KHz) : plus souvent utilisée pour le contrôle d'accès et le suivi des actifs.

Moyenne fréquence (13,56 MHz) : utilisée lorsque le débit de données moyen et les plages de lecture sont requis.

Ultra haute fréquence (850 MHz à 950 MHz et 2,4 GHz à 2,5 GHz) : offrent les plus longues plages de lecture et vitesses de lecture élevées

La biométrie

L'authentification biométrique est basée sur l'utilisation de certaines caractéristiques humaines mesurables pour authentifier un utilisateur . Il repose sur la reconnaissance, la même chose sur laquelle nous comptons pour identifier nos proches et connaissances. L'utilisation de l'authentification biométrique devrait avoir un impact significatif dans les domaines de la sécurité des systèmes d'information et de la protection de données dans les prochaines années

2.5 Le contrôle d'accès biométrique

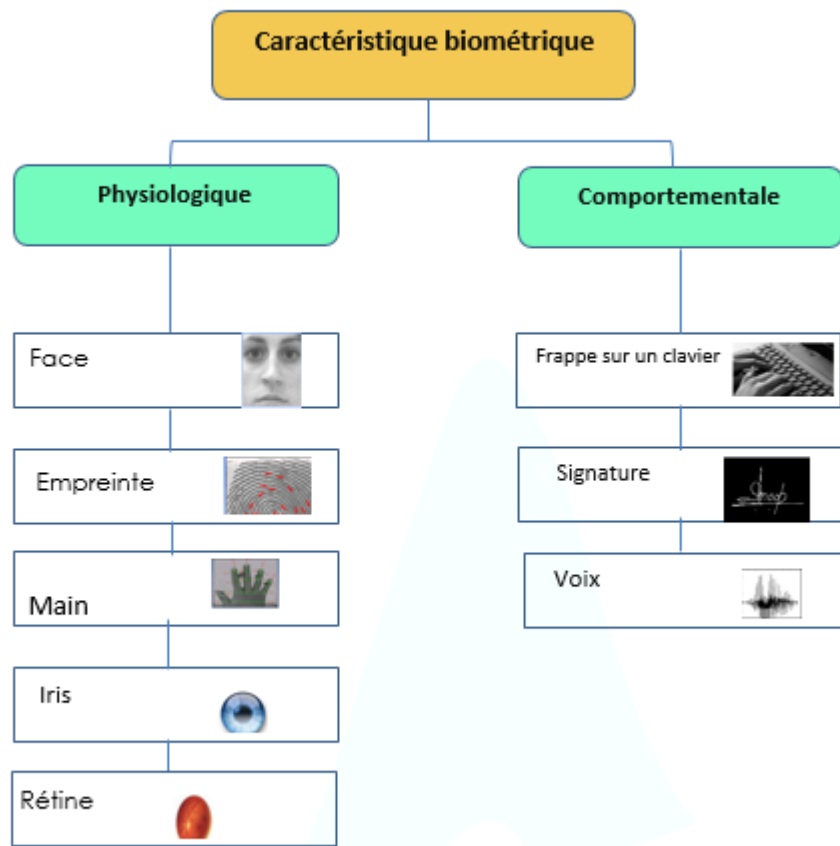
2.5.1 L'authentification biométrique

Une biométrie est une caractéristique physiologique ou comportementale d'un être humain qui permet de distinguer une personne d'une autre et qui peut théoriquement être utilisée pour l'identification ou vérification de l'identité. L'authentification est la propriété qui assure que seules les entités autorisées ont accès au système ; la biométrie fait référence à une authentification automatique d'une personne en fonction de ses caractéristiques physiologiques et / ou comportementales. Ceux-ci incluent des caractéristiques statiques : l'empreinte digitale, la géométrie de la main, les caractéristiques faciales, les motifs de la rétine et de l'iris ; et les caractéristiques dynamiques : l'empreinte vocale et la signature manuscrite, la dynamique du clavier.

En substance, la biométrie est basée sur la reconnaissance de formes. Comparée aux mots de passe et jetons, l'authentification biométrique est à la fois plus sûre, techniquement plus complexe et coûteuse. Alors qu'elle est utilisée dans de nombreuses applications spécifiques, la biométrie n'a pas encore mûri comme un outil standard pour l'authentification des personnes. [31]

2.5.2 Les caractéristiques utilisées dans les application biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La figure 2.4 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en deux catégories : biométrie physiologique et biométrie comportementale.



[21]

FIGURE 2.4 – Les caractéristiques biométriques

Les caractéristiques physiologiques

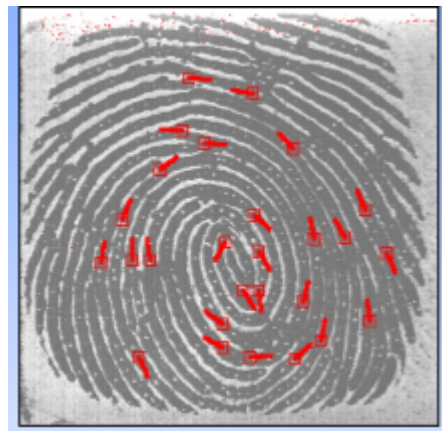
Les caractéristiques faciales : elles sont les moyens les plus communs d'identification entre les humains. Il est donc naturel de les considérer comme moyen d'authentification par les ordinateurs. L'approche la plus courante consiste à définir les caractéristiques en fonction de l'emplacement relatif et la forme des principales caractéristiques du visage, tels que les yeux, les sourcils, le nez, les lèvres et la forme du menton. Une approche alternative consiste à utiliser un appareil photo infrarouge pour produire un thermogramme de visage qui est en corrélation avec le système vasculaire sous-jacent dans le visage humain. [18]



[5]

FIGURE 2.5 – Reconnaissance faciale

L’empreinte digitale : elle a été utilisée comme moyen d’identification pendant des siècles, et le processus a été systématisé et automatisé en particulier à des fins d’application de la loi. Une empreinte digitale est le modèle de crêtes et sillons sur la surface du bout du doigt. Les empreintes digitales sont considérées comme uniques à travers toute la population humaine. En pratique, la reconnaissance automatique des empreintes digitales et le système correspondant extrait un certain nombre de caractéristiques de l’empreinte appelé minuties pour le stockage en tant que substitut numérique pour le modèle d’empreinte digitale complet.[18]



[5]

FIGURE 2.6 – L’empreinte digitale

La géométrie de la main : la reconnaissance par la main est une méthode bien établie qui date de plus de trente ans. Pour réaliser une vérification personnelle, un système peut mesurer les caractéristiques physiques des doigts ou des mains. Ceux-ci com-

prennent la longueur, la largeur, l'épaisseur et la surface de la main. Une autre caractéristique intéressante est que certains systèmes de reconnaissance utilisent un petit échantillon de quelques octets pour l'authentification des utilisateurs. Elle est aujourd'hui acceptée et implantée dans de nombreuses applications notamment dans le contrôle d'accès physique, les systèmes de gestion de temps de présence et en général les applications d'authentification [18]



[14]

FIGURE 2.7 – La géométrie de la main

Le motif rétinien : il est basé sur le modèle de vaisseau sanguin dans la rétine de l'œil et les vaisseaux sanguins à l'arrière de l'œil. Ils ont un motif unique, d'un œil à l'autre et d'une personne à l'autre. La rétine n'est pas directement visible, et donc, une source de lumière infrarouge cohérente est nécessaire pour illuminer la rétine. L'image du modèle de vaisseau sanguin de la rétine est ensuite analysée. Le scanner de la rétine exige que la personne enlève ses lunettes, place son œil près du scanner, regarde un point fixe, reste immobile et se concentre sur un emplacement spécifié pour environ 10 à 15 secondes pendant que l'analyse s'effectue. Un balayage rétinien implique l'utilisation d'une source

de lumière cohérente de faible intensité, qui est projetée sur la rétine pour éclairer les vaisseaux sanguins qui sont ensuite photographiés et analysés. Un coupleur est utilisé pour lire les modèles de vaisseaux sanguins. Dans un système de reconnaissance par motif rétinien, l'usurpation d'identité est actuellement impossible à forger. De plus, la rétine d'une personne décédée se dégrade trop rapidement pour être réutilisée à des fins d'authentification. La technologie d'identification par la rétine est très fiable avec un taux d'erreurs de 1 sur 10.000.000, comparée à l'empreinte digitale donc l'erreur d'identification est parfois aussi élevée que 1 sur 500.[8]



[8]

FIGURE 2.8 – La rétine

L'iris : chaque iris a un motif unique et complexe tel que même les motifs d'iris droit et gauche d'une personne sont complètement différents. En raison de ses propriétés et du nombre de caractéristiques mesurables, la duplication de l'iris est pratiquement impossible ; de plus l'iris est stable tout au long de la vie et n'est pas susceptible d'usure et blessure, même les lentilles de contact n'interfèrent pas avec l'utilisation de l'identifiant biométrique. L'authentification par l'iris s'impose donc comme un système fiable, largement accepté et implanté dans les systèmes sensibles tels que les salles de contrôle des centrales nucléaires. La technologie de reconnaissance par l'iris implique l'utilisation d'une caméra pour capturer une image numérique de l'œil, à partir de laquelle les données sont extraites. [8]

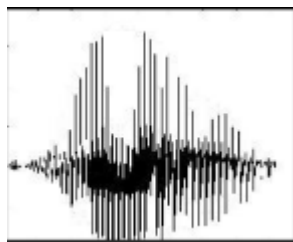


[8]

FIGURE 2.9 – L'iris

Les caractéristiques comportementales

La voix : la biométrie liée à la voix ne doit pas être confondue avec un logiciel de reconnaissance vocale qui reconnaît les mots tels qu'ils sont parlés. Les systèmes biométriques impliquent la vérification de l'identité du locuteur basée sur de nombreuses caractéristiques, telles que la cadence, la hauteur et le ton. La vérification du locuteur est considérée comme une biométrie comportementale et physiologique hybride. Le modèle vocal est déterminé, dans une large mesure, par la forme physique de la gorge et du larynx, bien qu'il puisse être modifié par l'utilisateur. La vérification est l'application préférée, la technologie est facile à utiliser et n'a pas besoin d'une grande partie de l'éducation des utilisateurs. Cependant, le bruit de fond affecte grandement le fonctionnement du système. La vérification du haut-parleur fonctionne avec un microphone ou avec un combiné téléphonique. Il est bien adapté aux applications téléphoniques où l'identité doit être vérifiée. La reconnaissance est également intégrée dans les systèmes de sécurité pour les services bancaires et électroniques en ligne.



[5]

FIGURE 2.10 – La voix

La signature manuscrite : cette technologie utilise l'analyse dynamique d'une signature pour authentifier une personne. La technologie est basée sur la mesure de la vitesse,

de la pression et de l'angle lorsqu'une signature est produite. Un objectif pour cette technologie a été les applications e-business et autres applications où la signature est acceptée comme méthode de vérification des personnes. [18] Personne ne fait une signature de manière cohérente de la même façon ; ainsi, les données obtenues à partir d'une signature d'une personne doit permettre une certaine variabilité. La plupart des systèmes de dynamique de signature ne vérifient que la dynamique. La taille des données obtenues au cours du processus de signature est d'environ 20 Ko. La taille du gabarit principal, qui est calculé de 3 à 10 signatures, varie d'environ 90 octets jusqu'à quelques Ko. Si la taille du modèle maître est relativement élevée, la reconnaissance a des problèmes de discrimination de correspondance et ne peut donc être utilisée que pour la vérification. La précision des systèmes biométriques de dynamique de signature n'est pas élevée, le taux de transition publié par les fabricants est d'environ 2 pour 100 [18]

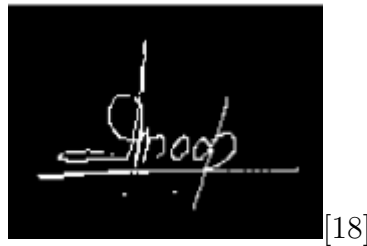


FIGURE 2.11 – La signature manuscrite

La dynamique du clavier : la biométrie de frappe est plus communément appelée dynamique du clavier. La vérification est basée sur le concept selon lequel une personne tape, en particulier selon un rythme et ce rythme est distinctif. La dynamique des frappes est comportementale et évolue au fil du temps lorsque les utilisateurs apprennent à taper et à développer leur propre modèle de frappe. La National Science Foundation et le National Bureau of Standards aux États-Unis ont mené des études établissant que les schémas de dactylographie sont uniques. La santé et la fatigue des utilisateurs, cependant, peuvent affecter le rythme de frappe. Cette technologie a récemment connu une résurgence avec le développement des applications de contrôle et accès à Internet. Un système crée des profils individuels en fonction de la manière dont les utilisateurs saisissent leur mot de passe, en tenant compte de facteurs tels que la taille de la main, la vitesse de frappe et la durée pendant laquelle les touches sont enfoncées. Selon les études, la technologie peut être utilisée avec n'importe quel clavier, (des claviers d'ordinateur aux guichets automatiques en passant par les téléphones). Auparavant, les différences de claviers avaient été l'un des problèmes limitant la mise en œuvre de la

dynamique des frappes.[18]



FIGURE 2.12 – La dynamique du clavier

2.6 Les technologies d'authentification biométrique

2.6.1 Définition

Les technologies biométriques mesurent et analysent des caractéristiques physiologiques et comportementales humaines. L'identification des caractéristiques physiologiques d'une personne est basée sur mesure d'une partie du corps notamment le bout des doigts, la géométrie de la main, le soin du visage, les rétines des yeux et les iris. L'identification des caractéristiques comportementales est basée sur des données dérivées d'actions, telles que le discours et la signature, la saisie au clavier. La biométrie est théoriquement une méthode d'identification des personnes très efficace car les caractéristiques qu'elle mesure sont considérées comme distinctes pour chaque personne. Contrairement aux méthodes d'identification classique qui utilisent quelque chose que vous avez, comme une carte d'identité pour accéder à un bâtiment, ou quelque chose que vous savez, comme un mot de passe pour se connecter à un système informatique, l'identifiant biométrique fait partie intégrante de quelque chose que vous êtes, parce qu'il est étroitement lié à un individu, il est plus fiable, ne peut être oublié et est moins facilement perdu, volé ou deviné.

2.6.2 L'architecture et fonctionnement

Les technologies biométriques varient en complexité, en capacité et en performance, mais tous partagent plusieurs éléments. Les systèmes d'identification biométrique sont essentiellement des systèmes de reconnaissance de formes. Ils utilisent des dispositifs d'acquisition comme des caméras et des dispositifs de balayage tel le scanner pour capturer des images, des enregistrements, ou mesures des caractéristiques d'un individu,

du matériel et logiciel informatique pour extraire, encoder, stocker et comparer ces caractéristiques. Parce que le processus est automatisé, la prise de décision biométrique est généralement très rapide, et dans la plupart des cas elle ne prend que quelques secondes en temps réel.

Selon l'application, les systèmes biométriques peuvent être utilisés dans l'un des deux modes : vérification ou identification. Vérification également appelée authentification est utilisée pour vérifier l'identité d'une personne, c'est-à-dire authentifier que l'individu est ce qu'il prétend être. L'identification est utilisée pour établir l'identité d'une personne, c'est-à-dire, pour déterminer qui est cette personne. Bien que les technologies biométriques mesurent différentes paramètres de manière sensiblement différentes, tous les systèmes de reconnaissance fonctionnent selon trois modes que sont : l'enrôlement, la vérification d'identité et d'identification.

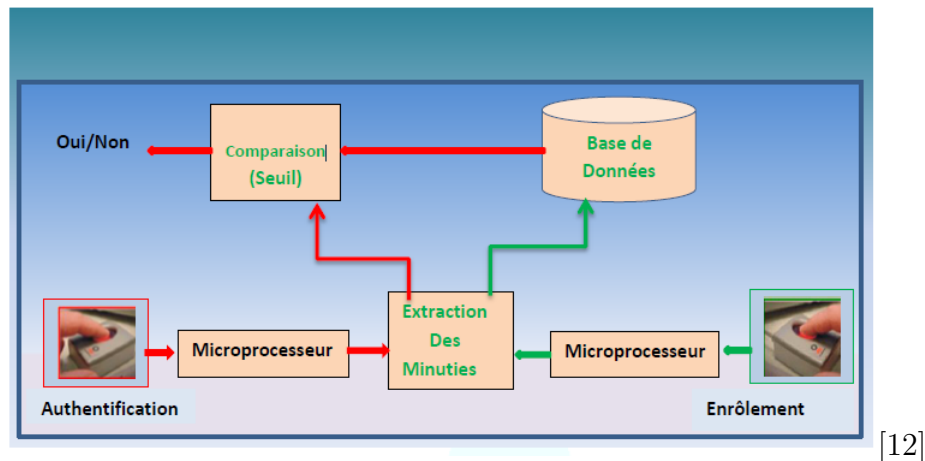


FIGURE 2.13 – Architecture d'un système de reconnaissance biométrique

2.6.3 L'enrôlement

Dans un système d'authentification biométrique, la phase d'enrôlement permet de récupérer le modèle qui servira d'identifiant dans le système. Pendant cette phase, un système biométrique est formé pour identifier un utilisateur spécifique. La personne fournit d'abord un identifiant, tel qu'une carte d'identité, puis présente les caractéristiques biométriques (par exemple, le bout des doigts, la main ou l'iris) à un dispositif d'acquisition qui capture une image ou un enregistrement. Les caractéristiques distinctives qui forment l'identifiant biométrique sont extraites, codées et stockées comme un modèle de référence qui servira pour des comparaisons futures. Selon la technologie, l'échantillon biométrique peut être collecté sous la forme d'une image, d'un enregistre-

ment ou d'un enregistrement de la dynamique associée à des mesures. Le processus de l'enrôlement dépend également de la qualité de l'identifiant fourni par l'utilisateur. Le modèle de référence est lié à l'identité spécifiée sur le document d'identification. Si le document d'identification ne spécifie pas la véritable identité de l'individu, le modèle de référence sera lié à une fausse identité.

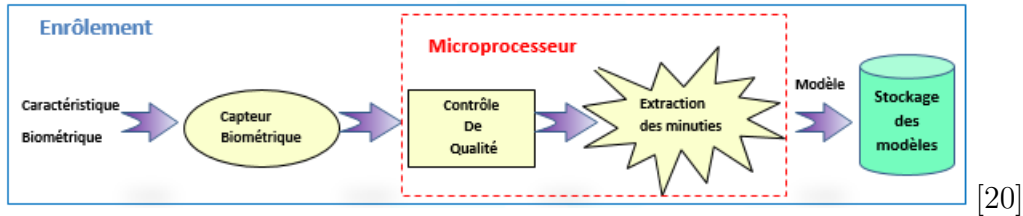


FIGURE 2.14 – Enrôlement d'un utilisateur

2.6.4 La vérification

Dans la phase de vérification, l'étape après l'enrôlement consiste à vérifier qu'un utilisateur est ce qu'il prétend être (c'est-à-dire, la personne qui s'est enrôlée dans le système). L'individu fournit l'identifiant avec lequel il s'est enrôlé, puis présente les caractéristiques biométriques à un dispositif d'acquisition qui capture une image ou un enregistrement et génère un modèle d'essai. Le système compare le modèle d'essai avec le modèle de référence de cette personne qui a été stocké dans le système lors de l'enrôlement, pour déterminer si le modèle d'essai de la personne et le modèle de référence stocké correspondent. Les systèmes de vérification peuvent contenir des bases de données allant de dizaines à des millions d'inscrits, mais sont toujours basés sur la correspondance d'un modèle d'essai d'un utilisateur contre son modèle de référence. Presque tous les systèmes de vérification peuvent rendre une décision de *match-no-match* en moins d'une seconde.

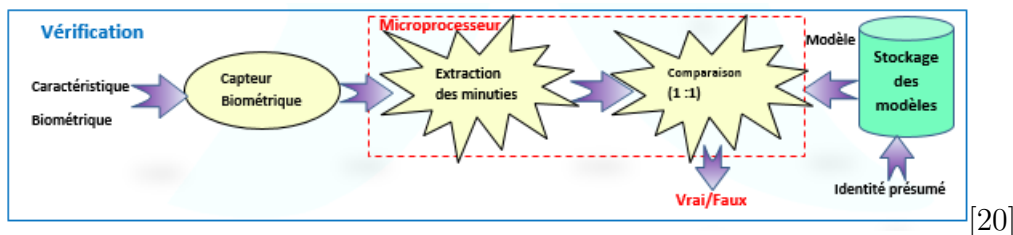


FIGURE 2.15 – Vérification d'un utilisateur

2.6.5 L'identification

Dans les systèmes d'identification, l'étape après l'enrôlement consiste à identifier les utilisateurs. Contrairement aux systèmes de vérification, aucun identifiant ne doit être fourni. Le modèle d'essai est comparé aux modèles de référence stockés de tous les utilisateurs inscrits dans le système.

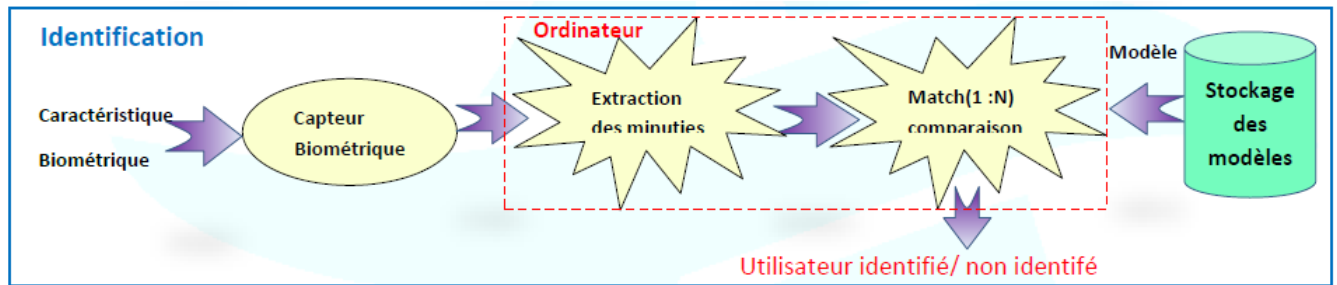


FIGURE 2.16 – L'identification d'un utilisateur

2.7 Spécification des données biométriques

Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes : [35]

Exigence 1 Universalité : toutes les personnes à identifier doivent la posséder ;

Exigence 2 Unicité : l'information doit être aussi dissimilaire que possible entre les différentes personnes ;

Exigence 3 Permanence : l'information collectée doit être présente pendant toute la vie d'un individu ;

Exigence 4 Collectabilité : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons ;

Exigence 5 Performance : doit être sûr et fonctionné à un niveau satisfaisant ;

Exigence 6 Acceptabilité : le système doit respecter certains critères (facilité d'acquisition, rapidité) afin d'être employé ;

Exigence 7 Sécurité : mesure la robustesse d'un système biométrique (capteurs et algorithmes) contre la fraude.

2.8 La précision des système biométrique

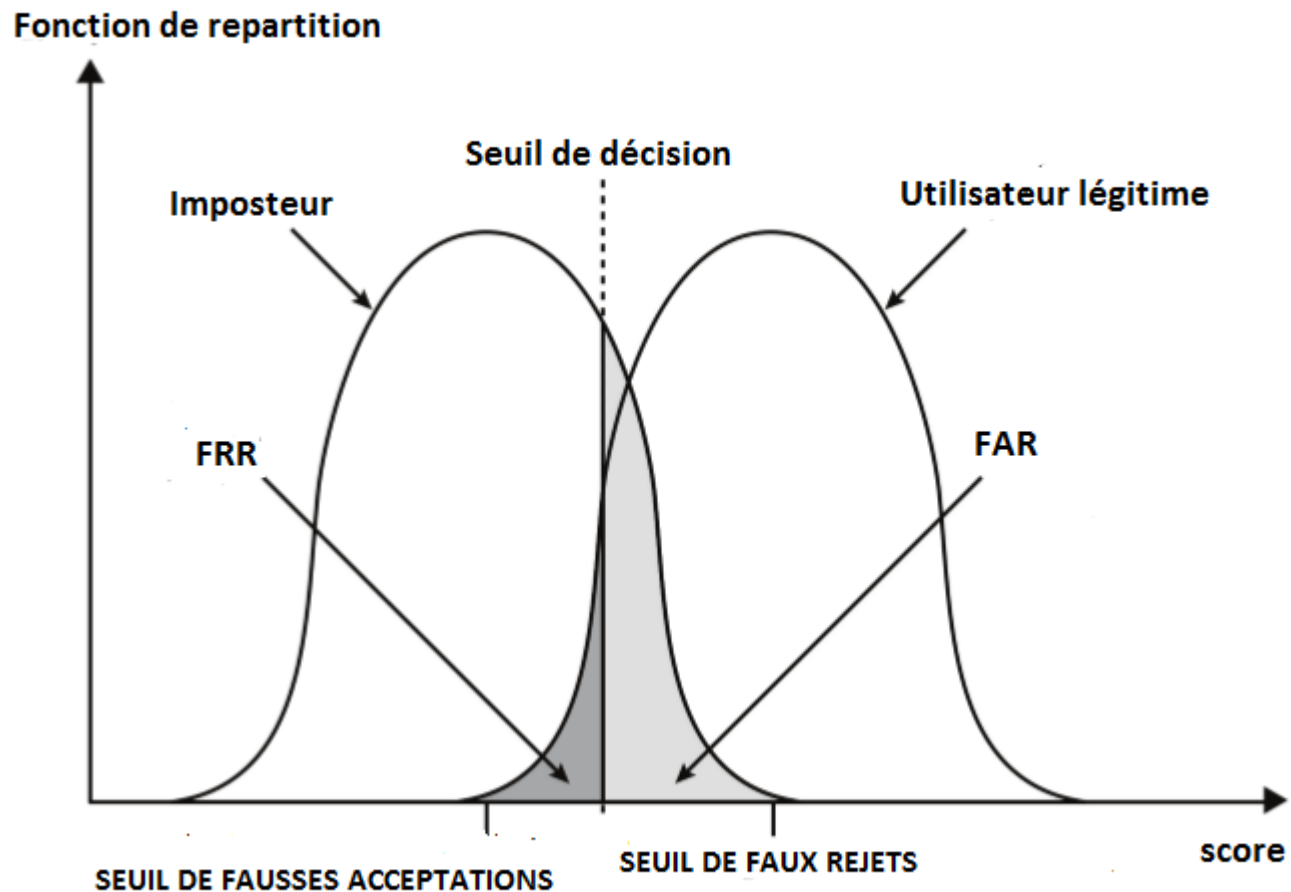
lorsque des systèmes biométriques sont utilisés, il est difficile d'obtenir des résultats 100 pour 100 exempts d'erreur. La raison est peut-être à chercher dans des différences d'environnement lors de l'acquisition de données (éclairage, température) et dans des différences dans le matériel utilisé (caméras, scanners). Les paramètres d'évaluation des performances les plus souvent utilisés sont le taux de fausses acceptations (FAR), le taux de faux rejets (FRR) et le taux d'erreur de croisement (CER) qui est le niveau auquel le nombre de faux rejets est égal aux fausses acceptations qui peuvent être adaptés en fonction du système utilisé.[33]

False Reject Rate (FRR) : le taux de faux rejets est le pourcentage d'instances d'identification dans lesquelles les utilisateurs autorisés se voient refuser l'accès en raison d'une défaillance du dispositif biométrique. Cet échec est connu comme une erreur de type I. Bien que cela constitue une source de frustration pour les demandeurs qui sont des utilisateurs autorisés, ce taux d'erreurs est probablement le moins préoccupant pour les professionnels de la sécurité puisque le rejet d'un utilisateur autorisé ne représente aucune menace pour la sécurité. Le taux de faux rejets est souvent ignoré à moins qu'il n'atteigne un niveau suffisamment élevé pour générer des plaintes des utilisateurs irrités.[33]

False Accept Rate (FAR :) le taux de fausses acceptations est le pourcentage d'instances d'identification dans lesquelles des utilisateurs non autorisés ont eu accès aux systèmes ou aux zones suite à une défaillance du dispositif biométrique. Cet échec est connu comme une erreur de type II et est inacceptable pour les professionnels de la sécurité. [33]

Cross Error Rate (CER) : Le taux d'erreur de croisement est le niveau auquel le nombre de faux rejets est égal aux fausses acceptations, et est également connu comme le taux d'erreur d'égalité. C'est probablement la mesure globale la plus commune et la plus importante de la précision d'un système biométrique. La plupart des systèmes biométriques peuvent être ajustés pour compenser à la fois les erreurs fausses positives et fausses négatives. L'ajustement à un extrême crée un système qui nécessite des correspondances parfaites et des résultats en faux rejets élevés, mais presque pas de fausses acceptations. L'ajustement à l'autre extrême produit un taux de faux rejets faibles, mais un taux de faux acceptations élevé. L'astuce consiste à trouver l'équilibre entre fournir le niveau de sécurité requis et minimiser le niveau de frustration des utilisateurs authentiques. Ainsi, le réglage optimal se situe quelque

part près du point où ces deux taux d'erreur sont égaux ; c'est-à-dire au taux d'erreur de croisement. Les CER sont utilisées pour comparer diverses données biométriques et peuvent varier selon le fabricant. Un dispositif biométrique qui fournit une CER de 1 pour 100 est un dispositif pour lequel le taux de défaillance pour faux rejets et le taux de défaillance pour fausses acceptations sont tous deux de 1 pour 100. Un appareil avec un CER de 1 pour 100 est considéré comme supérieur à un appareil avec un CER de 5 pour 100.



[31]

Source: Stallings and Brown, Computer Security, 3rd Ed., Pearson 2015, p99

FIGURE 2.17 – Le seuil d'efficacité

2.9 Vulnérabilités des systèmes d'authentification biométriques

2.9.1 Limites de performance

En comparaison aux systèmes d'authentification traditionnels qui offrent une réponse binaire (oui ou non), les systèmes biométriques sont moins précis et sont soumis à des erreurs telles que les taux de fausses acceptations (FAR) et de faux rejets (FRR). Cette variation illustrée par les taux d'erreurs peut affecter les systèmes biométriques en terme de sécurité. Doddington divise les utilisateurs légitimes en quatre catégories que sont les moutons, les agneaux, les chèvres et les loups.

- Les moutons : sont ceux qui peuvent être facilement reconnus (ils contribuent à une faible valeur du FRR).
- Les agneaux : Les agneaux sont ceux qui peuvent être facilement imités (ils contribuent à un FAR élevé).
- Les chèvres : sont ceux qui peuvent être difficilement reconnus (ils contribuent à un FRR élevé).
- Les loups : sont ceux qui ont la capacité d'usurper facilement d'autres utilisateurs légitimes (ils contribuent à un FAR élevé)

Ainsi, un système biométrique peu efficient en terme de performance, peut être vulnérable face aux agneaux et loups. Dès lors, il est indispensable de prendre en considération la performance du système dans le processus d'évaluation.

2.9.2 Limites de qualité pendant la phase d'enrôlement

La qualité des données acquises pendant la phase d'enrôlement est un facteur important à prendre en compte lors du développement des systèmes biométriques. L'absence d'un test de qualité augmente la possibilité d'avoir de faibles modèles biométriques. Ces modèles augmentent nettement la probabilité de réussite des attaques par zéro effort et force brute.

2.9.3 Mécanismes de protection des modèles biométriques

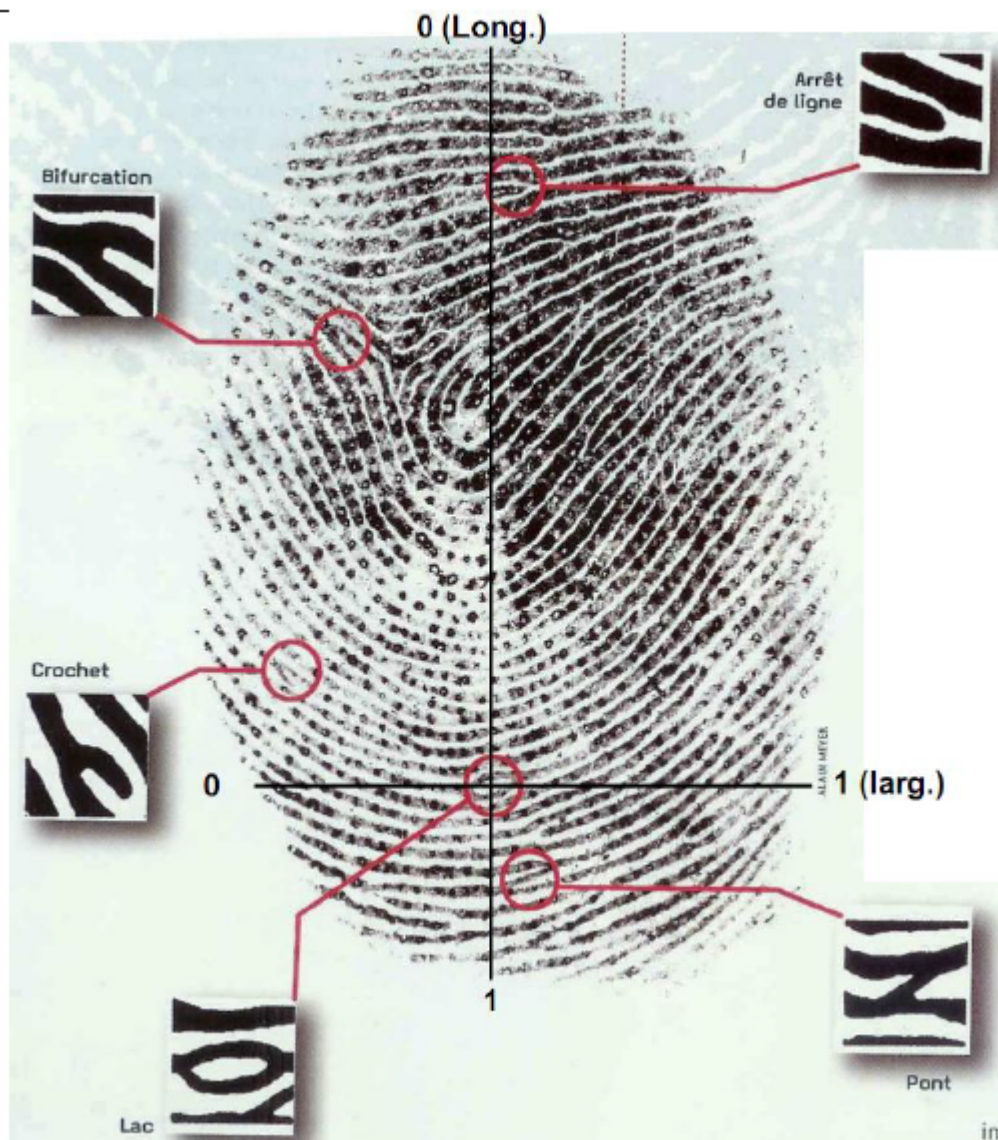
L'utilisation de la biométrie présente des vulnérabilités en termes de respect des droits et des libertés fondamentales. Le fait de conserver des modèles biométriques dans une

base de données centrale constitue une invasion de la vie privée. Ces données sont donc des données sensibles, qui ne sont pas encore protégées de façon spécifique par une norme internationale (même si la norme ISO/IEC 27000 adresse la protection des données personnelles). Parmi les solutions envisagées, on peut rendre les bases de données anonymes, et plus généralement intégrer la notion de respect de la vie privée dès la conception du système biométrique. Une autre solution plus efficace est d'utiliser le concept de biométrie révocable. Il s'agit de transformer les données biométriques brutes, à l'aide d'une fonction choisie, de telle sorte que les données transformées soient sûres, révocables et respectent la vie privée des utilisateurs (intraçabilité par exemple)

2.10 L'empreinte digitale

2.10.1 Caractéristiques des empreintes

Une empreinte est constituée d'un ensemble de lignes localement parallèles formant un motif unique et immuable pour chaque individu. On distique quelques points particuliers notamment, les bifurcations, les ponts, les lacs, les crochets, les arrêts de ligne ou terminaisons. [24]



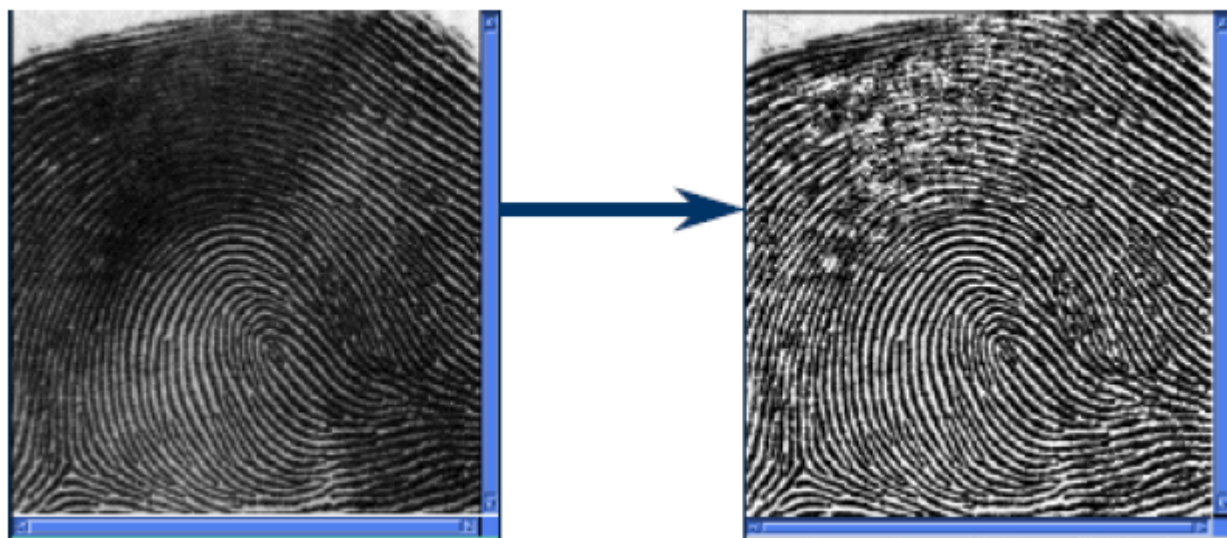
[24]

FIGURE 2.18 – Caractéristiques d’une empreinte digitale

2.10.2 Le traitement d’une empreinte digitale

Le traitement d’une empreinte digitale va de l’acquisition de l’image à l’obtention des minuties et se déroule généralement en trois phases.

Le prétraitement



[4]

FIGURE 2.19 – Phase de prétraitement

Amélioration de la qualité, uniformisation du contraste, problèmes d'encre, doigts gras ou secs.

La binarisation



[4]

FIGURE 2.20 – Phase de binarisation

La squelettisation



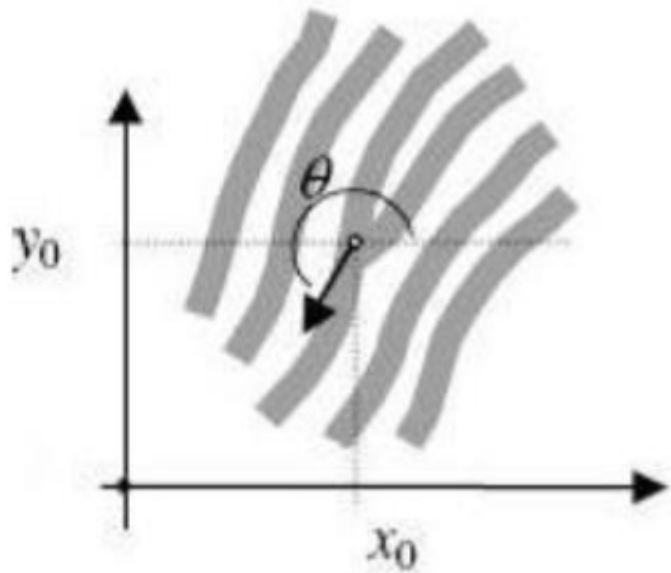
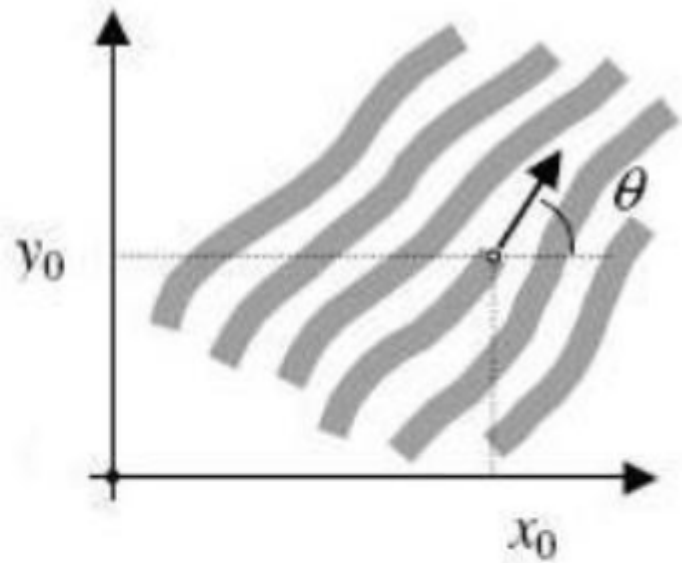
[4]

FIGURE 2.21 – Phase de squelettisation

L'extraction des minuties

chaque minutie est repérée et répertoriée comme suit :

- Le type de minutie : bifurcation ou terminaison ;
- La position de la minutie dans l'image : coordonnées (x,y) ;
- La direction du bloc local associée à la strie.



[9]

FIGURE 2.22 – Extraction des minuties

En pratique, quatre minuties sont à repérer pour permettre de déterminer une corrélation entre une trace de quelques millimètres carrés et une empreinte. La réglementation exige 12 minuties en France et 8 aux Etats-Unis.

2.11 Conclusion

Au terme de ce chapitre, nous avons présenté un aperçu théoriques des différents éléments qui permettent de sécuriser un aéroport. Nous avons aussi présenter les notions lier à l'authentification et le contrôle d'accès. En fin , nous avons terminer par une présentation de l'empreinte digitale et du processus d'extraction des minuties.

ANALYSE, MODÉLISATION ET CONCEPTION

3.1 Introduction

Après avoir présenté le contexte, ressorti la problématique et défini les objectifs de notre travail au chapitre 1, nous avons présenté les notions nécessaires à la compréhension de notre travail au chapitre 2. Il sera question dans ce chapitre de faire une analyse réelle de la situation sécuritaire sur les terrain, afin de prendre connaissance des vulnérabilités et menaces, ce qui nous permet de capter les différents besoins exprimés. Puis nous essayerons aussi de modéliser la solution envisagée.

3.2 Le cahier de charges

3.2.1 Étude de l'existant

L'Aéroport International de Maroua-Salak dispose de deux principaux points de contrôle d'accès du personnel. Le point de contrôle N°1, celui qui mène à la zone commercial, est le point de contrôle d'accès principal. Il est utilisé par l'ensemble du personnel de l'aéroport à l'exception du personnel technique chargé de la fourniture des services de la navigation aérienne. Le contrôle d'accès à ce point est assuré par des policiers qui vérifient manuellement l'identité de la personne à travers le document présenté ou se base sur la familiarité pour autoriser ou refuser l'accès à cette personne aux zones de sûreté à accès réglementé de l'aéroport.

Le second point de contrôle donne accès au bloc technique. Il est utilisé par le personnel technique chargé de la fourniture des services de la navigation aérienne. Cette zone est la plus sensible de l'aéroport car elle regroupe des équipements, installations et procédures nécessaires à la fourniture des services de la navigation aérienne. La sécurité dans cette zone relève du domaine de la gendarmerie et le contrôle d'accès est effectué par des gendarmes de façon analogue à celui effectuer au point de contrôle d'accès N°1.

Cette méthode de contrôle d'accès semble être peu efficace, pour les raisons suivantes.

- les méthodes de contrôle d'accès basées sur des badges, ou tous autres jetons que possède l'utilisateur sont connus inefficaces, car les pièces utilisées pour l'identification et l'authentification sont facile à dupliquer, reproduire, falsifier, voler, égarer ou oublier, surtout lorsqu'elles n'intègrent aucune protection de vérification automatique à la machine ou cryptographique comme ceux utilisés dans le cas décrit ci-dessus.
- La multiplicité des sources de production des ces badges (chaque organisme produit le badge de ses agents) serait une source de menaces potentielles. Non seulement elle rend l'authentification des documents difficile à réaliser, mais la politique de délivrance de ces badges pourraient ne pas être conforme aux exigences réglementaires en matière de sûreté de l'aviation civile. En occurrence, la Norme 4.2.1 de l'Annexe 17 stipule que : *"Chaque Etat contractant veillera à ce que les personnes autres que les passagers auxquelles est accordé un accès non accompagné aux zones de sûreté à accès réglementé de l'aéroport fassent préalablement l'objet d'une vérification de leur antécédent"*.
- L'enregistrement des autorisations d'accès n'est pas systématique, le système ne garde aucune trace fiable de l'enregistrement des personnes, dates, jours et heures qui ont accédé aux zones réservées de l'aéroport. Cet enregistrement pourrait s'avérer très utile en cas d'incident de sécurité ou de sûreté et leur exploitation pourrait être d'une importance capitale pour le succès des opérations d'investigations.

3.2.2 Identification des zones sensibles

L'étude de la méthode de contrôle d'accès existante suivit d'une évaluation de sécurité que nous avons mené donc vous trouverez les résultats en Annexe A ont permis d'identifier huit zones sensibles dont quatre secteurs de sûreté et quatre secteurs fonctionnels de sécurité. L'accès à ces zones doivent faire l'objet d'une authentification préalable de l'employé afin de restreindre l'accès aux seuls employés dont l'exercice régalière de leur fonction les oblige à y accéder.

SECTEURS DE SÛRETÉ

Secteur A (avion) : il comprend les postes de stationnement des avions utilisés pour l'embarquement et le débarquement des passagers et du fret. Chaque point de stationnement est élevé au rang de secteur de sûreté en présence de l'avion. La délimitation du secteur de sûreté correspond à la zone d'évolution contrôlée y compris les cheminements à pied ou en bus pendant l'embarquement ou le débarquement hors passerelles télescopiques.

Secteur B (bagages) : Il comprend les salles de tri, de conditionnement et de stockage des bagages au départ et en correspondance ainsi que les salles de tri des bagages.

Secteur P (passagers) : il comprend :

Au départ, les zones d'attente et de circulation des passagers entre les filtres de contrôle de sûreté des passagers de cabine et l'avion. il s'agit en particulier de la salle d'embarquement, de la zone d'enregistrement des passagers, le couloir de circulation des passagers et la passerelle.

À l'arrivée, les couloirs de circulation des passagers jusqu'à la sortie des salles de livraison des bagages.

Secteur V (salon VIP) : il comprend le salon VIP.

SECTEURS FONCTIONNELS DE SÉCURITÉ

Secteur fonctionnel NAV : il comprend la tour de contrôle, le bloc technique et les zones d'implantation des aides à la navigation aérienne, les installations de sécurité incendie.

Secteur fonctionnel MAN : il comprend la piste d'atterrissage et les voies de circulation.

Secteur fonctionnel ENE : il comprend les centrales électriques.

Secteur fonctionnel TRA : il est constitué de l'aire de trafic.

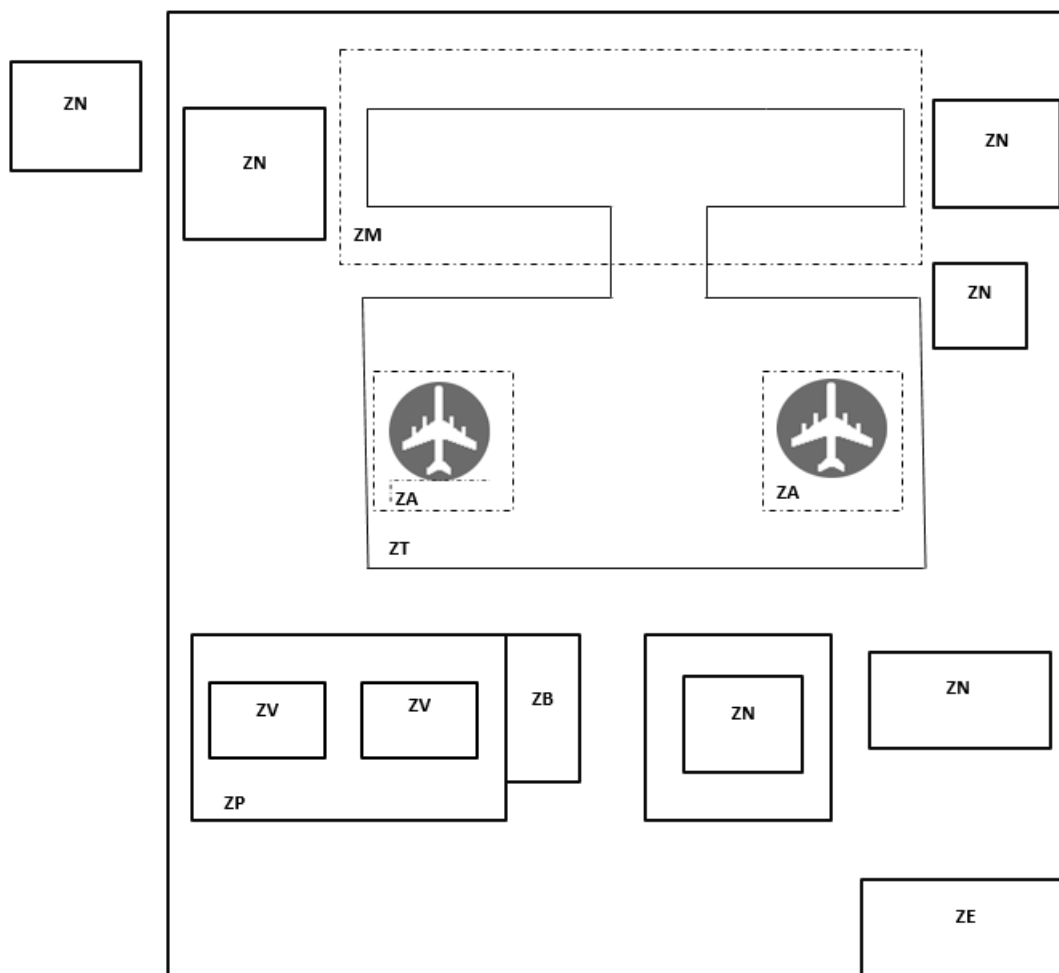


FIGURE 3.1 – Représentation des zones sensibles

Identification des ressources à protéger dans chaque zone sensible

CODE	ZONE	RESSOURCE Á PROTÉGER
ZA	Secteur de sûreté A	Avion
ZB	Secteur de sûreté B	Bagages
ZP	Secteur de sûreté P	Passagers
ZV	Secteur de sûreté V	Passagers VIP et Autorité Administratives
ZN	Secteur fonctionnel NAV	tour de contrôle et NAVAIDS
ZM	Secteur fonctionnel MAN	Piste et Voie de circulation
ZT	Secteur fonctionnel TRA	Aire de trafic
ZE	Secteur fonctionnel ENE	Centrale électrique

TABLE 3.1 – Identification des ressources à protéger

3.3 Évaluation de la sécurité

L'implémentation d'une nouvelle technologie de sécurité au sein d'une organisation est un investissement qui doit pouvoir être justifié. Elle doit à court ou à moyen terme apporter une valeur ajoutée à l'entreprise et ne saurait en aucun cas être considéré comme une dépense. Une étude de risque doit permettre d'évaluer le coût de chaque ressource à protéger en prenant en compte sa valeur réelle et celle acquise avec le temps, le coût lié à son remplacement et les pertes que subirait l'organisation si la ressource venait à être compromise. Elle s'opère à travers une étude de risque qui est une étape critique, car sans elle il y a de forte chance que des ressources ne soient pas déployées efficacement. Le résultat pourrait être le fait que plusieurs risques ne soient pas identifiés, laissant l'organisation vulnérable, pendant que des mesures de contrôle peuvent être déployées ailleurs sans justification. L'objectif de cette étude de risque est de fournir au top management, des informations fiables nécessaires à une prise de décision raisonnable sur le déploiement des ressources existantes. L'évaluation de sécurité que nous menons dans cette partie est une analyse de la situation actuelle d'exposition des ressources faces aux menaces et vulnérabilités auxquelles elles sont confrontées. Les résultats de cette étude se trouvent en annexe A.

3.3.1 L'évaluation des ressources

L'évaluation des ressources est le processus d'attribution de valeur financière à chaque ressource. Elle permet d'avoir une idée approximative du coût global des ressources afin de juger la nécessité ou non d'implémenter un contrôle spécifique pour contrer ces menaces. Au regard de la complexité de cette tâche, nous nous limiterons juste à un recensement des ressources donc la liste figure en annexe A.

3.3.2 Identification des menaces

Une source de menace est une circonstance ou un événement pouvant potentiellement causer des dommages. Le tableau 3.2 illustre quelques sources de menaces identifiées.

SOURCE	MOTIVATION	ACTION
Terroriste	Destruction Revanche Idéologie	Bombe Attaque armée Sabotage Intrusion
Employé Malformé Négligeant Malveillant Malhonnête Congédié	Curiosité Égo Omission Appât du gain Renseignement Revanche	Intrusion Sabotage Vente d'information Fraude Vol Corruption

TABLE 3.2 – Menaces identifiées

3.3.3 Identification des vulnérabilités

liste des vulnérabilités

Menaces	Secteurs							
	ZA	ZB	ZP	ZV	ZN	ZM	ZT	ZE
Sabotage	✓				✓			✓
Intrusion	✓	✓	✓	✓	✓	✓	✓	✓
Vol		✓	✓	✓				✓
Destruction	✓	✓						
Fraude	✓	✓	✓	✓				
Corruption		✓	✓	✓				
Vente d'information			✓	✓				
Bombe	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 3.3 – Identification des vulnérabilités

3.4 Fonctionnalités attendues du nouveau système

3.4.1 Expression des besoins fonctionnels

A la fin de ce projet, notre application MABAC doit être capable de :

- Enregistrer les informations d'identification et les adresses des employés dans la base de données.
- Délivrer automatiquement le badge d'identification (MARAIC).

- Implémenter une matrice de contrôle d'accès basée sur le rôle des employés au sein de l'aéroport.
- Enrôler les employés.
- Authentifier les employés.
- Identifier les employés.

3.4.2 Expression des besoins de sécurité

- Le FAR doit être très réduit pour accroître la sécurité de notre système en évitant d'accorder l'accès à une personne illégitime due à une erreur d'authentification.
- Prévenir les accès non autorisés aux données personnelles d'identification.
- Protéger le système contre le vol ou l'usurpation d'identité.

3.4.3 Expression des besoins non fonctionnels

- Protection de la vie privée : l'image naturelle de l'empreinte ne doit pas être stockée dans la base de données, seule les minuties (une représentation mathématique de l'empreinte doit être stockée dans la base de données).
- Prévention contre le vol ou l'usurpation d'identité : les minuties (représentation mathématique de l'empreinte) stockées dans la base de données ne doivent en aucun cas permettre de reconstruire l'empreinte réelle.
- FRR : doit être réduit pour éviter les frustrations liées au refus d'accès d'une personne légitime due à l'incapacité du système à l'authentifier.
- Facilité d'usage : pour accroître l'acceptabilité de la solution biométrique.
- Stockages des données : Les données biométriques (minuties) doivent être stockées en locale pour faciliter l'accès et le contrôle de ses données.

3.5 Étude de faisabilité

L'étude de faisabilité permet de déterminer la stratégie à adopter pour faire face à une vulnérabilité spécifique dans un système de sécurité. Ainsi, l'implémentation d'une nouvelle solution de sécurité doit toujours être précédée d'une étude de faisabilité qui

prend en compte toutes les conséquences économiques et non-économiques que produirait l'exploitation de la vulnérabilité sur l'organisation. Cette étude de faisabilité tente de répondre à la question suivantes : *“Quels sont les avantages réels et perceptibles de la mise en œuvre d'un contrôle par opposition aux inconvénients réels et perceptibles de la mise en œuvre du contrôle?”*. [33] Nous adoptons une approche qualitative pour déterminer la capacité de l'organisation à pouvoir implémenter et utiliser notre solution proposée à travers une étude de faisabilité déclinée en cinq axes essentiels à savoir :

- L'étude de faisabilité politique ;
- L'étude de faisabilité organisationnelle ;
- L'étude de faisabilité opérationnelle ;
- L'étude de faisabilité technique ;
- L'étude de faisabilité économique.

3.5.1 Étude de faisabilité politique

Sur le plan politique, le contexte sécuritaire que connaît le Cameroun avec plusieurs poches de violences et grands banditismes identifiés dans les régions de l'Extrême-Nord, l'Est, le Nord-Est et le Sud-Est doit amener les organisations dont les mesures d'authentifications des personnes et de contrôle d'accès physique des personnes font partie intégrante de leur politique de sécurité à les renforcer. De plus le récent audit de sûreté de l'aviation civile au Cameroun mené par l'OACI du 18 au 27 Avril 2018 sous le programme USAP, a montré certes une très grande évolution de la situation globale de la sûreté de l'aviation civile au Cameroun par rapport à 2015. Mais on note également que des efforts restent à entreprendre pour renforcer les mesures de sûreté existantes afin d'atteindre les standards de l'Annexe 17 et l'Annexe 9. Nous croyons que l'implémentation de notre solution dans les aéroports du Cameroun contribuera à renforcer les mesures de sûreté et de sécurité existantes et permettra de gagner quelques points lors des prochaines audits.

3.5.2 Étude de faisabilité organisationnelle

Sur le plan organisationnel, il est évident que l'implémentation d'une solution de contrôle d'accès biométrique apportera une valeur ajoutée à l'Aéroport International de

Maroua-salak. Elle permettra non seulement de renforcer les mesures de sécurité existantes, mais améliorera l'efficacité et l'efficience des opérations de l'aéroport par une réduction nette du temps consacré à examiner les pièces d'identifications. De plus le renforcement des mesures de sûreté dans les aéroport entre dans la stratégie et la vision de l'Autorité Aéronautique du Cameroun et elle ne lèse pas sur les moyens pour y arriver, car entre 2016 et 2017 plus de 300 personnes ont été recrutées pour les besoins de sûreté dans les aéroports internationaux de Yaoundé Nsimalen et Douala en cours de certification.

3.5.3 Étude de faisabilité opérationnelle

Elle vise à déterminer si la solution une fois implémentée sera effectivement utilisée et acceptée par les utilisateurs. Pour y arriver, nous avons mené une enquête de terrain sur la connaissance et l'acceptabilité des technologies biométriques dont les questions qui ont été posées aux acteurs figures en annexe B. Cette enquête a montré un intérêt particulier des autorités aéroportuaires pour notre solution. Les employés de l'aéroport(futurs utilisateurs) ont préféré la technologie d'authentification par vérification d'empreinte digitale parmi les technologies d'authentification biométrique présentées. Néanmoins nous avons noté quelques préoccupations particulières de la part de ces personnes notamment sur des questions relatives à la protection de leur identifiant biométrique et la protection de la vie privée. Nous avons également rencontré quelques personnes qui ont manifesté leurs désaccords concernant la prise de leurs empreintes digitales à des fins d'authentification évoquant des mœurs culturelles. Nous croyons que leur implication peut être obtenue à travers une politique d'éducation et de communication autour du projet qui pourra être mise en place par l'entreprise lors de l'implémentation.

3.5.4 Étude de faisabilité technique

L'étude de faisabilité technique vise à déterminer la capacité de l'entreprise à pouvoir gérer l'ensemble des composantes technologiques nécessaire à l'implémentation d'une solution tout en analysant la meilleur décision à prendre entre concevoir en interne, acheter ou sous-traiter tout ou une partie de la technologie nécessaire à l'implémentation d'une solution. La composante technologique clé de notre solution est l'authentification par vérification de l'empreinte digitale. Nos recherches sur le plan local ne nous ont permis d'identifier aucune entreprise camerounaise spécialisée dans ce domaine. Il reste à noter que cette technologie est aujourd'hui la vache à lait de nombreuses entreprises américaines et européennes qui sont spécialisées dans ce domaine. Afin de réduire les

coûts exorbitants liés à l'achat et la maintenance de cette technologie, nous comptons l'implémenter et l'entreprise se chargera juste de l'achat du matériel nécessaire et la formation de son personnel.

3.5.5 Étude faisabilité économique

L'étude de faisabilité économique vise à déterminer le coût et les bénéfices que produiront un projet sur une période donnée. Les coûts présentés dans cette partie sont liés à l'implémentation de la solution dans le secteur aéronautique aux attentes et exigences fortes en terme de qualité et de sécurité.

Poche de dépense	Coût
Développement	10000000
Matériel informatique	12000000
Carte à puce	2000000
Lecteur biométrique	1000000
Formation	3000000
Service après vente(Sur cinq ans)	150000000
Total	32200000

Le coût global estimé pour l'implémentation de notre solution à l'Aéroport International de Maroua-Salak s'élève à Trente deux millions deux cent mille francs CFA (32200000 CFA) pour une période de cinq (05) ans. Nous sommes très conscient de la problématique de sécurité que font face les entreprises avec des contraintes de limitation de budget et la nécessite d'un retour sur investissement claire et mesurable pendant une période donnée. En effet personne ne peut acheter un coffre-fort pour garder une somme d'argent dérisoire, autant mettre son argent sous le matelas et accepter le risque de se faire voler. Pour toute entreprise désirant implémentée notre solution d'authentification biométrique, le coût peut être estimé après une évaluation de ses attentes et exigences en terme de sécurité et de qualité.

3.6 Planification des activités du projet

La méthodologie que nous utilisons adopte une approche de project pour la résolution d'un problème ; ainsi, nous avons fait une représentation des tâches axée sur le calendrier à l'aide de MS Project 2010. Nous avons suivi le canevas ci-dessous pour l'exécution de nos tâches.

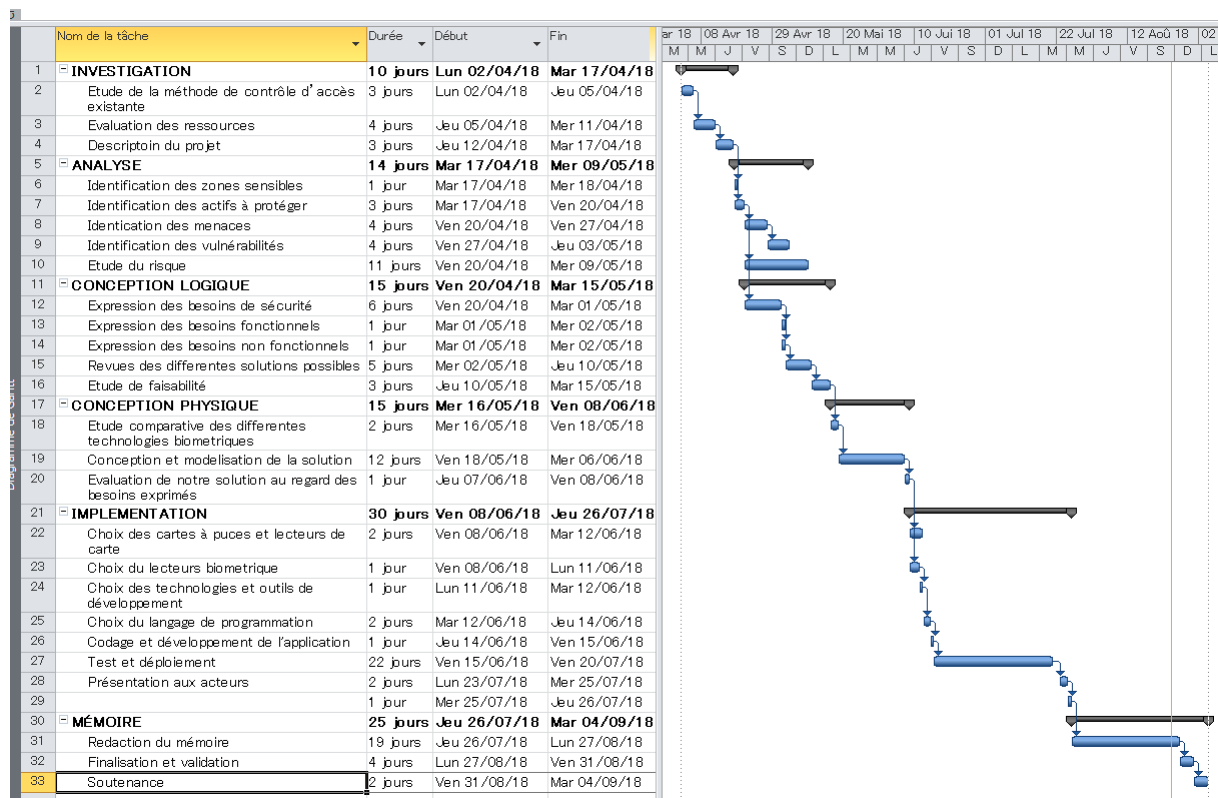


FIGURE 3.2 – planification des tâches

3.7 Étude comparative des technologies biométriques

Une étude comparative des différents systèmes d'authentification biométrique au regard des exigences décrites à la section 2.7 a permis d'obtenir les résultats suivants :

Biométrie	Exigences						
	Universalité	Unicité	Permanence	Collectabilité	Performance	Acceptabilité	Sécurité
Face	E	F	M	E	F	E	E
Main	M	M	M	E	M	M	M
Empreinte	M	E	E	M	E	M	M
Iris	E	E	E	M	E	F	F
Rétine	E	E	M	F	E	F	F
keystroke	F	F	F	M	F	M	M
Voix	M	F	F	M	F	E	E
Signature	F	F	F	E	F	E	E

TABLE 3.4 – Tableau comparatif des technologies biométriques

[21]

Légende : **E** : élevé, **M** : Moyen, **F** : Faible,

3.8 Architecture de notre système

3.8.1 Architecture globale

La figure 3.3 présente l'ensemble des composants matériels et humains nécessaires à l'exploitation de notre solution.

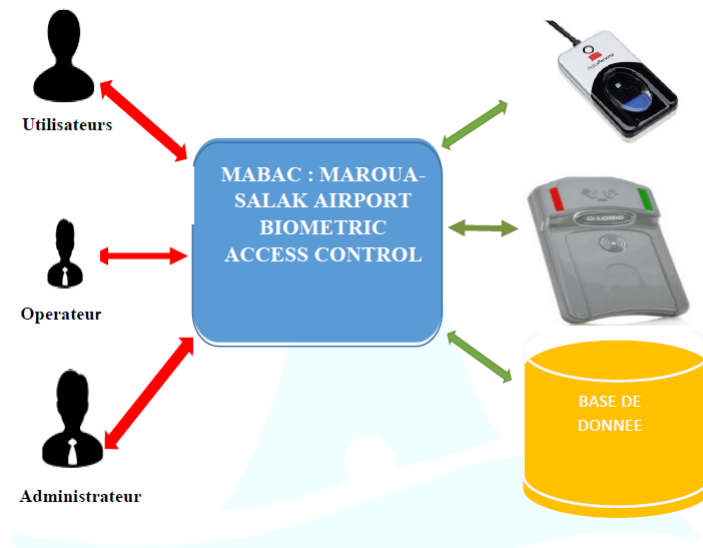


FIGURE 3.3 – Architecture globale

3.8.2 Architecture fonctionnelle

La figure 3.4 illustre l'architecture fonctionnelle de l'authentification par vérification de l'empreinte digitale que nous aurons à implémenter.

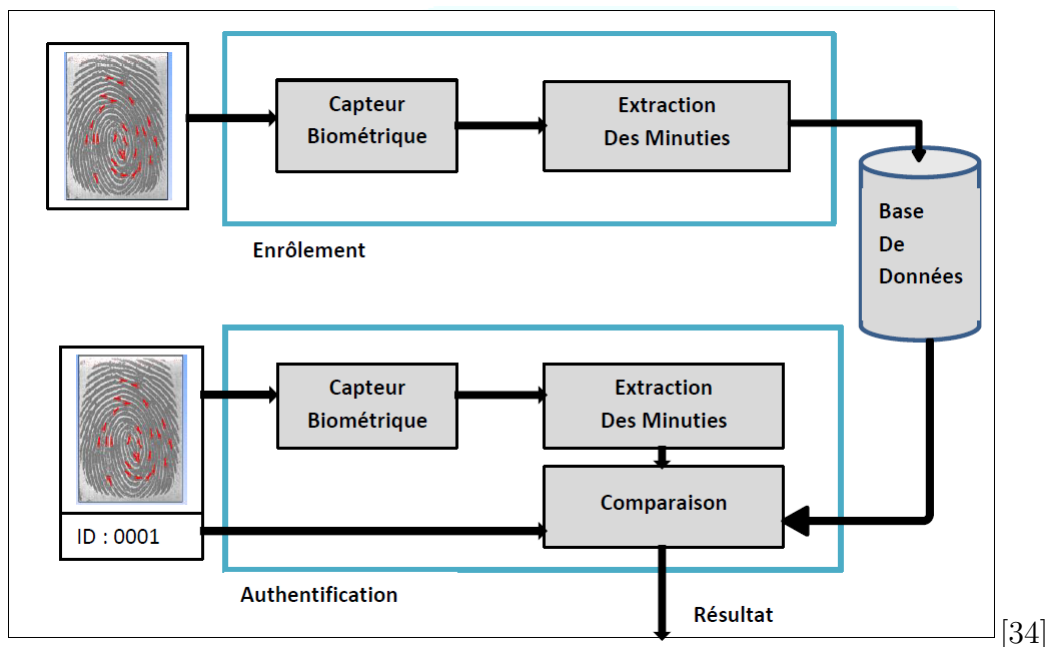


FIGURE 3.4 – Architecture fonctionnelle

3.8.3 Matrice de contrôle d'accès

Cette matrice de contrôle représente l'ensemble des professions que l'on rencontre au sein de l'Aéroport International de Maroua-Salak avec pour chaque profession les différentes zones de l'aéroport auxquelles cette personne peut accéder pour être en mesure de remplir ses missions au sein de l'aéroport. Nous utilisons ici le principe du privilège minimum, cet- à-dire qu'une personne ne se voit attribuer une zone spécifique que s'il est clairement établi que l'exercice de ses fonctions dans les conditions normales d'exploitation l'oblige à s'y rendre. Puis nous avons essayé de regrouper dans un même groupe les personnes qui ont les mêmes droits d'accès ; ainsi six groupes différents ont été identifiés comme l'illustre le tableau ci-dessous.

Corps professionnel	Secteurs								Groupe
	ZA	ZB	ZP	ZV	ZN	ZM	ZT	ZE	
Contrôleur aérien			✓		✓	✓	✓		2
Agent sureté compagnie	✓	✓	✓				✓		4
Accueil personne VIP		✓	✓	✓					5
Police		✓	✓	✓					5
Personnel d'appui CCAA			✓						6
Douane		✓	✓	✓					5
Personnel suété CCAA	✓	✓	✓	✓	✓	✓	✓	✓	1
Bagagiste	✓	✓	✓				✓		4
Assistant escale			✓		✓	✓	✓		2
Manshaller	✓	✓	✓				✓		4
Gendarmerie	✓	✓	✓	✓	✓	✓	✓	✓	1
Personnel d'appui ADC			✓						6
Directeur de l'aéroport	✓	✓	✓	✓	✓	✓	✓	✓	1
Technicien de maintenance			✓		✓	✓	✓	✓	3
Agent meteo			✓		✓	✓	✓		2
Personnel d'appui compagnie			✓						6
Commandant d'aéroport	✓	✓	✓	✓	✓	✓	✓	✓	1
Commissaire de l'aéroport	✓	✓	✓	✓	✓	✓	✓	✓	1
Pompier d'aérodrome			✓		✓	✓	✓	✓	3
Agent AIM			✓		✓	✓	✓		2
Agent sûreté compagnie		✓	✓						4
Autres			✓						6

TABLE 3.5 – Matrice de contrôle d'accès

Groupe 1 : Commandant d'aéroport, Directeur de l'aéroport, Commissaire de l'aéroport, Agent AVSEC CCAA.

Groupe 2 : Contrôleur aérien, Agent AIM, Agent météo, Assistant escale.

Groupe 3 : Pompier d'aérodrome, Technicien de maintenance NAVAIDS.

Groupe 4 : Bagagiste, Marshaller, Agent AVSEC compagnie aérienne.

Groupe 5 : Police, Accueil personne VIP, Douane.

Groupe 6 : Personnel d'appui CCAA, Personnel d'appui ADC, Personnel d'appui Compagnie aérienne.

Groupes	Secteurs							
	ZA	ZB	ZP	ZV	ZN	ZM	ZT	ZE
Groupe 1	✓	✓	✓	✓	✓	✓	✓	✓
Groupe 2			✓		✓	✓	✓	
Groupe 3			✓		✓	✓	✓	✓
Groupe 4	✓	✓	✓			✓		
Groupe 5		✓	✓	✓				
Groupe 6			✓					

TABLE 3.6 – Matrice de contrôle d'accès réduite

La figure 3.5 est une schématisation de la matrice de contrôle d'accès présentée plus haut. Les codes de couleurs à l'entrée de chaque zone indiquent que le groupe de personnes indexées par la couleur indiquée ont accès à cette zone.



FIGURE 3.5 – Matrice de contrôle d'accès

3.9 Les opérations réalisées par notre système

Notre système réalisera cinq opérations essentielles à savoir :

1. L'enregistrement
2. L'enrôlement
3. L'authentification/ Vérification
4. L'identification
5. L'audit.

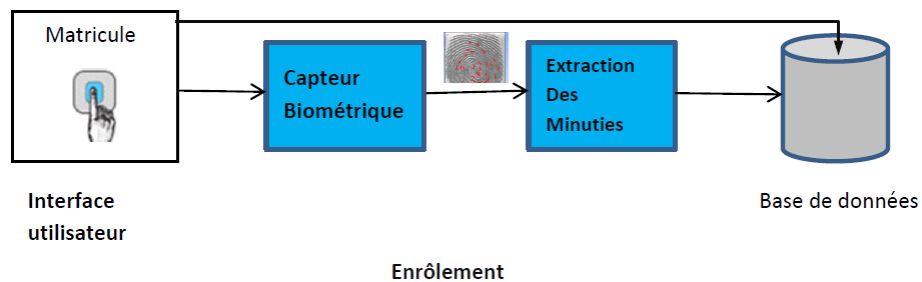
3.9.1 L'enregistrement

Description

- 1- L'employé ou son employeur fait une demande du badge MARAIC.
- 2- La demande est étudiée, acceptée ou refusée.
- 3- Si la demande est acceptée, le dossier est soumis à l'opérateur.
- 4- L'opérateur saisie les données d'identification dans le système.
- 5- Vérifie que l'employé n'est pas encore enregistré dans la base de données.
- 6- L'opérateur sauvegarde les données de la personne dans la base de données.
- 7- Délivre le badge.

3.9.2 L'enrôlement

Architecture



[31]

Source :Stallings and Brown, Computer Security, 3rd Ed., Pearson 2015, p98

FIGURE 3.6 – L'enrôlement

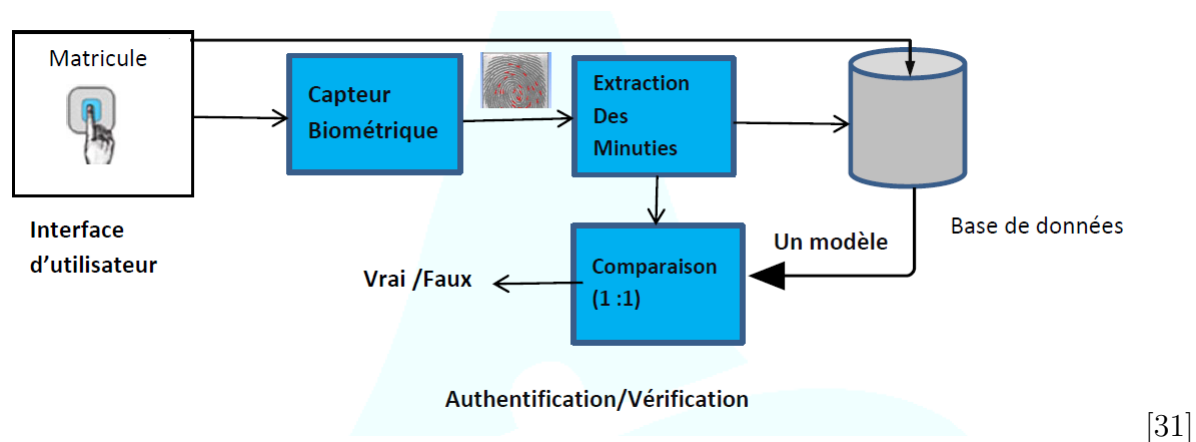
Description

- 1- L'employé se présente devant l'opérateur avec son badge.
- 2- L'opérateur capture l'empreinte de l'employé en utilisant un lecteur d'empreinte.

- 3- Vérifie la qualité de l'image.
- 4- Extrait les minuties.
- 5- Associe l'empreinte(les minuties) à la personne.
- 6- Sauvegarde dans la base de données.

3.9.3 L'authentification /La vérification

Architecture



Source :Stallings and Brown, Computer Security, 3rd Ed., Pearson 2015, p98

FIGURE 3.7 – L'authentification /vérification

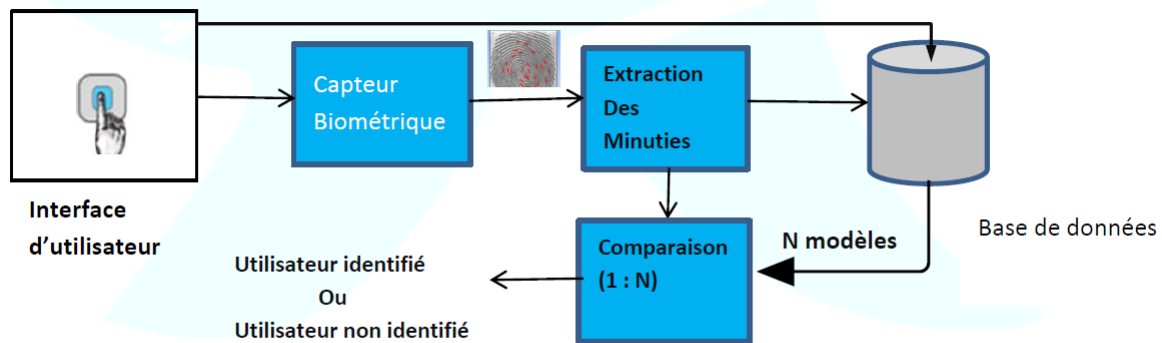
Description

- 1- saisir l'identifiant de la personne dans le système.
- 2- capturer l'empreinte de la personne en utilisant un lecteur d'empreinte.
- 3- Extraire les minuties.
- 4- Obtenir le modèle de référence (minuties obtenu au moment de l'enrôlement) de la personne dans la base de données.

- 5- Comparer les minuties extraites (modèle de test) au modèle de référence. (comparaison (1 :1)).
- 6- Autoriser ou refuser l'accès selon le résultat.

3.9.4 L'identification

Architecture



Identification

[31]

Source :Stallings and Brown, Computer Security, 3rd Ed., Pearson 2015, p98

FIGURE 3.8 – L'identification

Description

- 1- capturer l’empreinte de la personne en utilisant un lecteur d’empreinte.
- 2- Extraire les minuties.
- 3- Comparer les minuties extraites (modèle de test) avec tous les modèles de référence stockés dans la base de données. (comparaison 1 : N).
- 4- Autoriser ou refuser l’accès selon le résultat.

Description

- 1- Le superviseur s'authentifie au système
- 2- Le superviseur consulte les journaux (journalier, hebdomadaire, mensuel et annuel).

3.10 Modélisation

Pour la modélisation de notre solution, nous utilisons l'approche qui est présentée dans le livre SYSTEMS ANALYSIS AND DESIGN IN A CHANGING WORLD, Sixth edition 2012. Elle utilise le langage UML 2.0 pour la modélisation des diagrammes.

3.10.1 Les acteurs du système et leur but

Acteurs	Son but /objectif
L'employé	s'enregistrer / s'enrôler / s'authentifier
L'opérateur	Enregistrer/Authentifier les employés
Le superviseur	Enrôler/Identifier l'employé/Auditer le système

TABLE 3.7 – Les acteurs du système et le but

3.10.2 Cas d'utilisation que réalise chaque acteur

Les cas d'utilisation	Utilisateurs /acteurs
Enregistrer employé	Employé/Opérateur
Enrôler employé	Employé/Superviseur
Authentifier employé	Employé/Opérateur
Identifier employé	Employé/Superviseur
Auditer	Superviseur

TABLE 3.8 – Cas d'utilisation que réalise chaque acteur

3.10.3 Les diagrammes de cas d'utilisation

Cas d'utilisation du système global

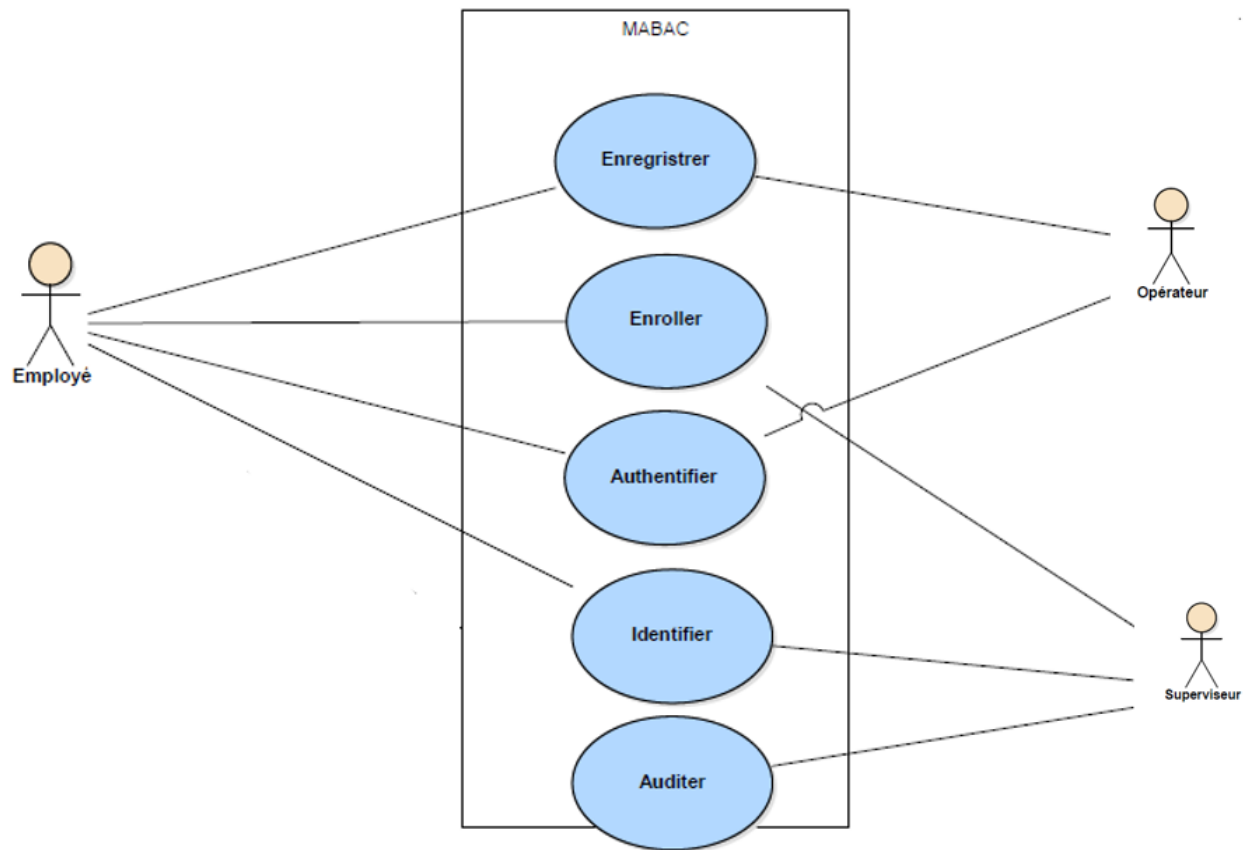


FIGURE 3.9 – Diagramme de cas d'utilisation du système global

Cas d'utilisation du sous système enregistrement

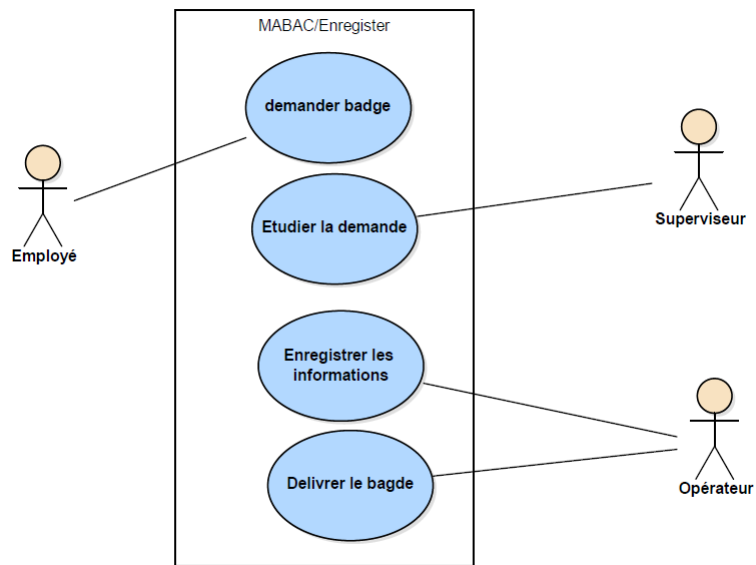


FIGURE 3.10 – Diagramme de cas d'utilisation du sous système enregistrement

Cas d'utilisation du sous système enrôlement

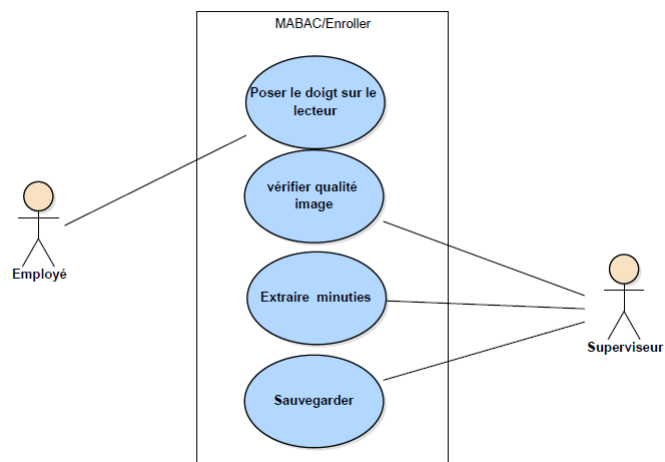


FIGURE 3.11 – Diagramme de cas d'utilisation du sous système enrôlement

Cas d'utilisation du sous système authentification

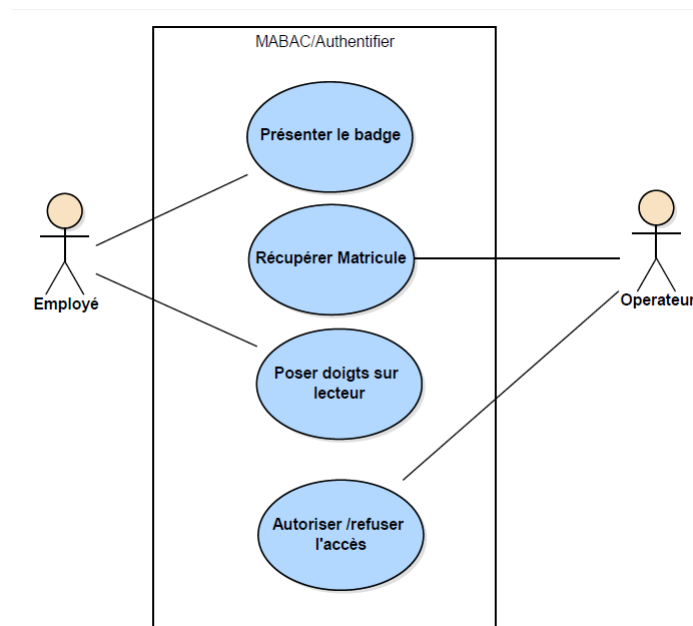


FIGURE 3.12 – Diagramme de cas d'utilisation du sous système authentification

Cas d'utilisation du sous système identification

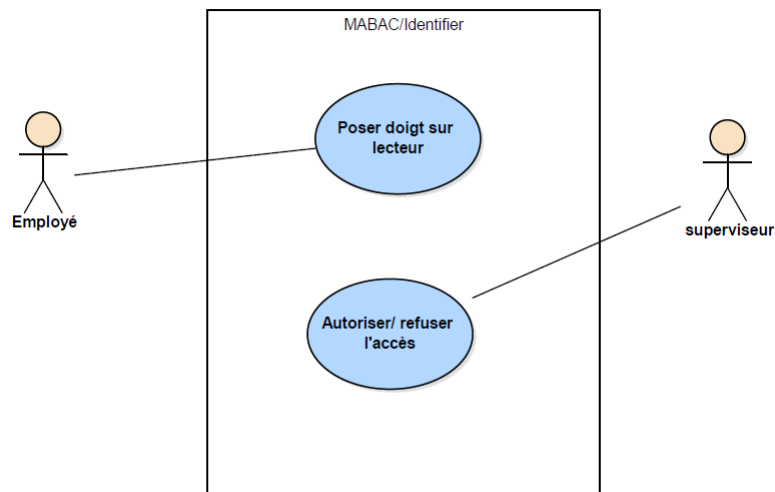


FIGURE 3.13 – Diagramme de cas d'utilisation du sous système identification

Cas d'utilisation du sous système Audit

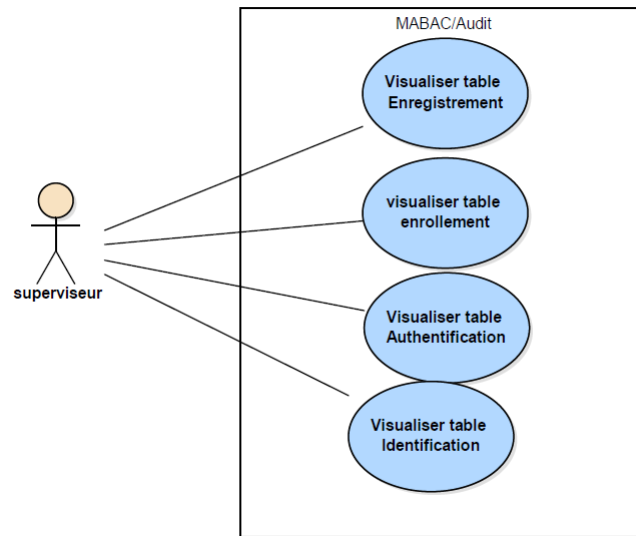


FIGURE 3.14 – Diagramme de cas utilisation du sous système auditer

3.10.4 Description des cas d'utilisation

Cas d'utilisation du sous système enregistrer un employé

Nom du cas d'utilisation	Enregistrer employé	
Scénario	Enregistrer employé/délivrer MARAIC	
Évènement déclencheur	Demande d'un badge MARAIC	
Brève description	L'opérateur saisit les données d'identification de la personne, sauvegarde ces informations dans la base de données et délivre le badge MARAIC.	
Acteurs	Opérateur	
Cas d'utilisations associés	Auditer, Enrôler, Authentifier	
Parties prenantes	Opérateur, Employé	
Pré conditions	La demande doit être validée par le Commandant d'Aéroport.	
Post conditions	L'employé doit être enregistré dans le système et son badge délivré	
Flux d'activités	Acteur	Système
	1- L'employé se présente chez l'opérateur	a) L'opérateur saisit les données d'identification de l'employé b) L'opérateur délivre le badge d'identification de l'employé.
Exception	Aucune	

TABLE 3.9 – Description du cas d'utilisation enregistrer employé

Cas d'utilisation du sous système enrôler un employé

Nom du cas d'utilisation	Enrôler employé	
Scénario	Enrôler l'empreinte d'un employé dans la base de données	
Évènement déclencheur	Délivrance d'un nouveau badge MARAIC	
Brève description	Le superviseur capture L'empreinte d'un employé, extrait les minuties, associe le matricule aux minuties pour cet employé et sauvegarde dans la base de données.	
Acteurs	Employé/Superviseur	
Cas d'utilisations concerné/associé	Auditer, Authentifier, Identifier	
Parties prenantes	Superviseur, Employé	
Pré conditions	L'employé est déjà enregistré dans le système.	
Post conditions	Le matricule + minuties de l'employé doivent être sauvegardés dans la base de données.	
Flux d'activités	Acteur	Système
	1- L'employé fournie son badge MARIC	a) Le superviseur récupère le matricule de l'employé
	2- L'employé pose son doigt sur le lecteur biométrique	b) Le superviseur capture l'empreinte c) Contrôle la qualité de l'image et extrait les minuties d) Associe l'identifiant de l'employé à son empreinte e) Sauvegarde dans la base de données
Exception	1- Les caractéristiques biométriques de l'employé ne permettent pas d'obtenir un modèle de référence.	

TABLE 3.10 – Description du cas d'utilisation enrôler employé

Cas d'utilisation du sous système Authentifier un employé

Nom du cas d'utilisation	Authentification/Vérification	
Scénario	Authentifier un employé et l'autoriser l'accès aux zones réservées de l'aéroport.	
Évènement déclencheur	L'employé veut accéder à l'aéroport	
Brève description	L'authentification/ vérification permet de vérifier l'identité d'un employé, en comparant ses caractéristiques biométriques au modèle de référence connu du système pour cet employé.	
Acteurs	Employé/Opérateur	
Cas d'utilisations concerné/associé	Enrôler, Auditer	
Parties prenantes	Opérateur, Employé	
Pré conditions	L'employé doit être enrôlé.	
Post conditions	L'utilisateur doit être formellement identifié et l'accès lui sera autoriser ou refuser le cas échéant.	
Flux d'activité	Acteur	Système
	1- L'utilisateur approche son badge près du lecteur de carte à puce sans contact.	a) Le lecteur récupère l'ID de la carte. b) L'empreinte associé à cet ID est affiché.
	2- L'utilisateur dépose son doigt sur le lecteur d'empreinte.	a) L'opérateur capture l'empreinte digitale de l'utilisateur. b) Extrait les minuties (modèles de test) c) Compare le modèle de test avec le modèle de référence de l'utilisateur concerné s'il y a concordance, l'accès est autorisé sinon, il est refusé
Exception	1- Les caractéristiques biométriques de l'employé ne permettent pas d'obtenir un modèle de biométrie.	

TABLE 3.11 – Description du cas d'utilisation enrôler employé

Cas d'utilisation du sous système identifier un employé

Nom du cas d'utilisation	Identification	
Scénario	1- Identifier un employé 2- Vérifier la performance du système d'authentification.	
Évènement déclencheur	Un employé demande l'accès sans fournir son badge d'identification/Le superviseur veut s'assurer de la performance du système d'authentification.	
Brève description	L'identification permet d'authentifier un utilisateur à comparant son modèle biométrique de test à l'ensemble des modèles de références enregistrés dans le système et de déterminer sans équivoque son identité.	
Acteurs	Employé/Opérateur	
Cas d'utilisations concerné/associé	Enrôler, Auditer	
Parties prenantes	Opérateur	
Pré conditions	1- L'employé doit être enregistré dans le système. 2- L'employé doit être en mesure de fournir ses caractéristiques biométriques.	
Post conditions	L'employé doit être formellement identifié et l'accès lui sera autoriser ou refuser le cas échéant.	
Flux d'activité	Acteur	Système
	1- L'employé dépose son doigt sur le lecteur d'empreinte.	a) L'opérateur capture l'empreinte digitale de l'utilisateur. b) Extrait les minuties (modèles de test). c) Compare le modèle de test avec tous les modèles de référence stockés dans la base de données, s'il y a concordance, l'accès est autorisé sinon, il est refusé.
Exception	1- Les caractéristiques biométriques de l'employé ne permettent pas d'obtenir un modèle de biométrique.	

Cas d'utilisation du sous système Audit

Nom du cas d'utilisation	Auditer	
Scénario	L'administrateur veut auditer le système (visualiser les journaux)	
Évènement déclencheur		
Brève description	L'administrateur accède aux journaux journalier, hebdomadaire, mensuel et annuel du système	
Acteurs	Administrateur	
Cas d'utilisations concerné/associé	Enregistrer, l'enrôler, authentifier (Vérifier/ identifier)	
Parties prenantes	Opérateur, employé	
Pré conditions	Les employés doivent être enrôlés	
Post conditions	Avoir un ensemble d'informations sur la fonctionnalités et les performances de l'application.	
Flux d'activité	Acteur	Système
Exception	Aucune	

TABLE 3.13 – Description du cas d'utilisation du sous système audit

3.10.5 Les diagrammes d'activité

Diagramme d'activité du sous système enregistrement

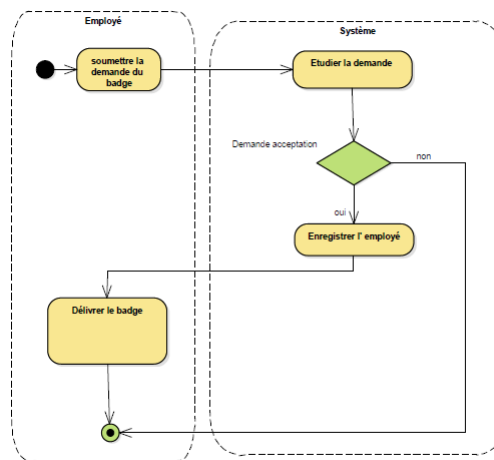


FIGURE 3.15 – Diagramme d'activité du sous système enregistrement

Diagramme d'activité du sous système enrôlement

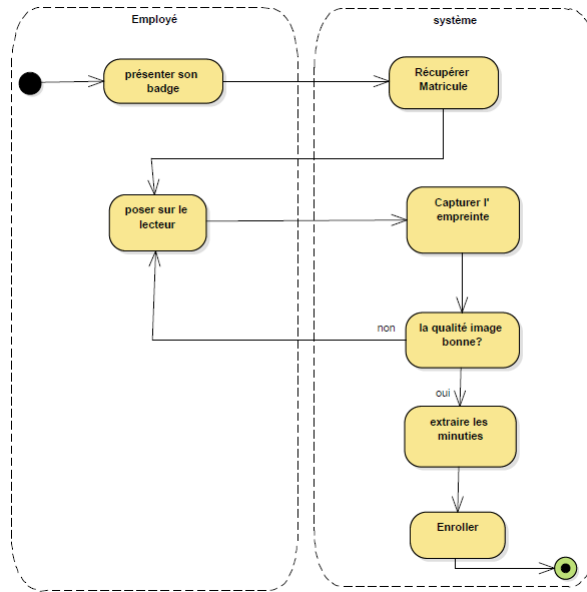


FIGURE 3.16 – Diagramme d'activité du sous système enrôlement

Diagramme d'activité du sous système authentification

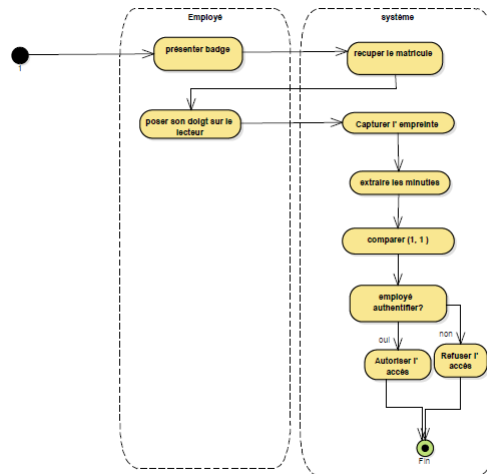


FIGURE 3.17 – Diagramme d'activité du sous système authentification

Diagramme d'activité du sous système identification

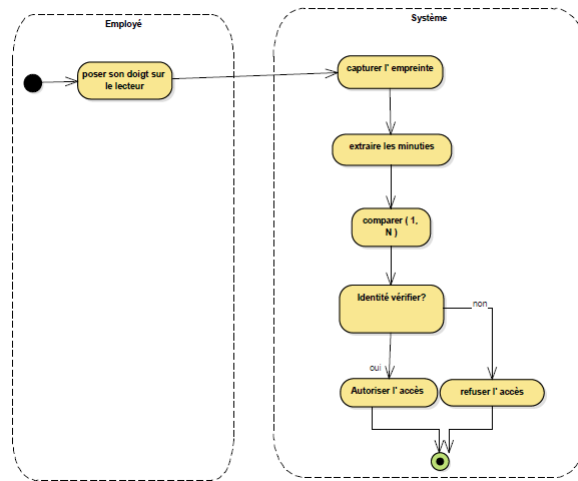


FIGURE 3.18 – Diagramme d'activité du sous système identification

3.10.6 Diagramme de classe

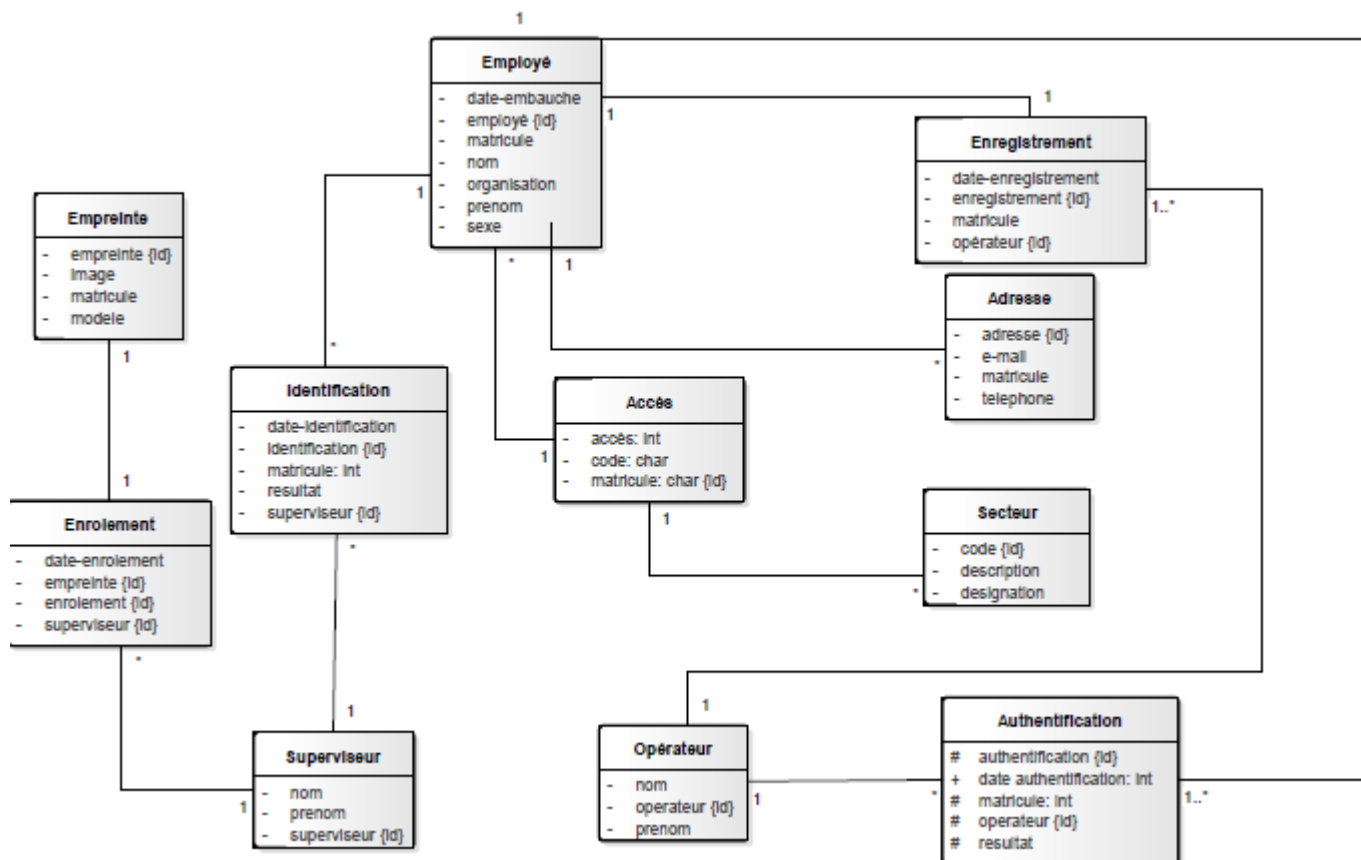


FIGURE 3.19 – Diagramme de classe système MABAC

3.11 Conclusion

Il était question dans ce chapitre d'évaluer la situation sécuritaire sur le terrain, de cerner le périmètre à protéger, d'identifier les vulnérabilités et de désigner les menaces. Nous avons modélisé et conçu la solution que nous comptons implémentée.

MISE EN ŒUVRE DE LA SOLUTION

4.1 Introduction

Dans le présent chapitre, il sera question pour nous de présenter les technologies et outils de développement que nous avons utilisé pour la conception de contre solution et pour l'implémentation. Nous passerons en revue le langage de programmation utilisé, l'environnement de développement et le lecteur biométrique utilisé pour la prise d'empreinte digitale.

4.2 Technologies et outils de développement

4.2.1 Langage et outils de modélisation

Langage de modélisation

Pour la modélisation de notre application, nous avons choisi le langage de modélisation UML 2.0. C'est un langage de modélisation orienté objet qui représente un intermédiaire simple et efficace entre concepteurs intervenant dans le projet et futurs utilisateurs du nouveau système. En effet, les différents diagrammes qu'il propose simplifient d'une part le processus de développement aux concepteurs, et permettent, d'autre part, aux utilisateurs et chefs d'entreprises de suivre les étapes de développement du système et de valider ainsi chacune d'elles. Son efficacité réside dans son approche object qui consiste à se concentrer sur la modélisation des systèmes, indépendamment de la technologie qui sera utilisée pour la réalisation. Cette propriété très intéressante permet aux chefs d'entreprises, soit d'arrêter le processus de développement du logiciel, soit de le modifier selon leurs besoins, et cela en étant encore à l'étape de modélisation. UML 2.0 comporte ainsi treize types de diagrammes représentant autant de vues distinctes que de concepts particuliers du système à développer. Notre modélisation utilise trois de ces diagrammes notamment :

- Le diagramme de cas d'utilisation (Use case diagram).
- Le diagramme d'activités (Activity diagram).
- Le diagramme de classe (Class diagram).

Entreprise Architect 6.5 a été utilisé pour la réalisation de ces diagrammes.

Méthode

SecSDLC que nous avons présentée à la section 1.6 est la méthode que nous utiliserons tout au long de notre développement car elle est très adaptée pour la conception et l'implémentation des systèmes de sécurité. MSPROJECT 2010 est utilisé comme outil de planification et de suivi des différentes activités de développement.

4.2.2 Langage de programmation

JAVA

Pour la réalisation de notre application, nous avons opté pour le langage Java. Ces principaux avantages sont : une portabilité excellente, il est orienté objet, de très haut niveau, il possède un JDK très riche et des librairies tierces (club des développeurs et IT pro, 2017).

MySQL

SQL (Structured Query Language) est un langage d'interrogation de base de données très populaire. Il permet de récupérer des informations depuis un simple fichier ou un serveur S.Q.L., aussi appelé SGBDR.

Les figures ci-dessous montre les détails de l'implémentation de notre base de données avec le langage MySQL.

```
mysql> USE MABAC;
Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_mabac |
+-----+
| acces            |
| adresse          |
| authentication   |
| employe          |
| empreinte        |
| enregistrement  |
| enrolement      |
| identification   |
| operateur        |
| secteur          |
| superviseur      |
+-----+
11 rows in set (0.02 sec)
```

FIGURE 4.1 – Implémentation de la base de données

Field	Type	Null	Key	Default	Extra
employe_id	smallint(6)	NO	PRI	NULL	auto_incr
matricule	char(9)	NO	UNI	NULL	
nom	varchar(25)	NO		NULL	
prenom	varchar(25)	YES		NULL	
sex	enum('masculin','feminin')	NO		NULL	
organisation	enum('CCAA','ADC','CAMAIRCO','WFP','POLICE','GENDARMERIE','OTHERS')	NO		NULL	
fonction	varchar(20)	NO		NULL	
date_embauche	timestamp	YES		NULL	

8 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
empreinte_id	smallint(6)	NO	PRI	NULL	auto_increment
matricule	char(9)	NO	UNI	NULL	
modele	longblob	NO		NULL	
image	varbinary(200)	YES		NULL	

4 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
code	enum('ZA','ZB','ZV','ZP','ZN','ZM','ZT','ZE')	NO	PRI	NULL	
designation	varchar(25)	NO		NULL	
description	varchar(200)	YES		NULL	

3 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
access_id	smallint(6)	NO	PRI	NULL	auto_increment
code	enum('ZA','ZB','ZV','ZP','ZN','ZM','ZT','ZE')	NO	MUL	NULL	
matricule	char(9)	NO	MUL	NULL	

3 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
enrolement_id	smallint(6)	NO	PRI	NULL	auto_increment
empreinte_id	smallint(6)	YES	MUL	NULL	
superviseur_id	smallint(6)	YES	MUL	NULL	
dateEnrolement	timestamp	YES		NULL	on update CURRENT_TIMESTAMP

4 rows in set (0.01 sec)

FIGURE 4.2 – Visualisation des tables 1

Field	Type	Null	Key	Default	Extra
authentication_id	smallint(6)	NO	PRI	NULL	auto_increment on update CURRENT_TIMESTAMP
matricule	char(9)	YES	MUL	NULL	
opérateur_id	smallint(6)	YES	MUL	NULL	
dateAuthentication	timestamp	YES		NULL	
resultat	enum('VRAIE','FAUX')	YES		NULL	

5 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
identification_id	smallint(6)	NO	PRI	NULL	auto_increment on update CURRENT_TIMESTAMP
matricule	char(9)	YES	MUL	NULL	
superviseur_id	smallint(6)	YES	MUL	NULL	
dateIdentification	timestamp	YES		NULL	
resultat	enum('VRAIE','FAUX')	YES		NULL	

5 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
enregistrement_id	smallint(6)	NO	PRI	NULL	auto_increment on update CURRENT_TIMESTAMP
matricule	char(9)	YES	MUL	NULL	
opérateur_id	smallint(6)	YES	MUL	NULL	
dateEnregistrement	timestamp	YES		NULL	

4 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
code	enum('ZA','ZB','ZV','ZP','ZN','ZM','ZT','ZE')	NO	PRI	NULL	
designation	varchar(25)	NO		NULL	
description	varchar(200)	YES		NULL	

3 rows in set (0.01 sec)

Field	Type	Null	Key	Default	Extra
access_id	smallint(6)	NO	PRI	NULL	auto_increment
code	enum('ZA','ZB','ZV','ZP','ZN','ZM','ZT','ZE')	NO	MUL	NULL	
matricule	char(9)	NO	MUL	NULL	

3 rows in set (0.02 sec)

FIGURE 4.3 – Visualisation des tables 2

4.2.3 Les outils de développement

Environnement de développement : NETBEANS

Netbeans est un environnement de développement intégré (EDI), placé en open source par Sun permettant de supporter différents langages, comme java C, C++, JavaScript, XML, PHP et HTML de façon native ainsi que bien d'autres (comme Python ou Ruby) par l'ajout de greffons. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, Projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages Web). Netbeans constitue une plateforme qui permet le développement d'applications spécifiques.

Base de données : SGBD MYSQL

MySQL est un serveur de base de données relationnelles SQL qui fonctionne sur de nombreux systèmes d'exploitation (dont Linux, Mac OS X, Windows, Solaris, FreeBSD...) et qui est accessible en écriture par de nombreux langages de programmation, incluant notamment PHP, Java, Ruby, C, C++, .NET, Python.

4.2.4 Choix du lecteur biométrique

Pour obtenir l'image de l'empreinte, le lecteur biometrique numérique Digital persona U.are.U 4500 est utilisé avec les caractéristiques suivantes.

- LED bleue.
- Fonctionne bien avec les empreintes sèches ou humides.
- Compatible avec Windows Vista, XP Professionnel, Windows Server 2000 et 2000, 2003, 2008 et 2010
- Résolution de pixel : 512 dpi (sur la zone de numérisation).
- Zone de capture : 14,6 mm (largeur au centre) 18,1 mm (longueur).
- Niveaux de gris 8 bits (256 niveaux de gris).
- Taille du lecteur (approximative) : 65 mm x 36 mm x 15,56 mm.
- Compatible avec USB 1.0, 1.1 et 2.0 (haute vitesse).

Il a été décidé d'utiliser ce lecteur optique en raison de la qualité de la lecture et de la facilité d'usage amicale.



FIGURE 4.4 – Lecteur biométrique

[3]

4.3 Conclusion

Dans ce chapitre, il était question de présenter les technologies, outils de développement, les langages de programmation, nécessaires à la conception et l'implémentation de notre solution. Le chapitre suivant sera consacré à la présentation et l'analyse des résultats obtenus.

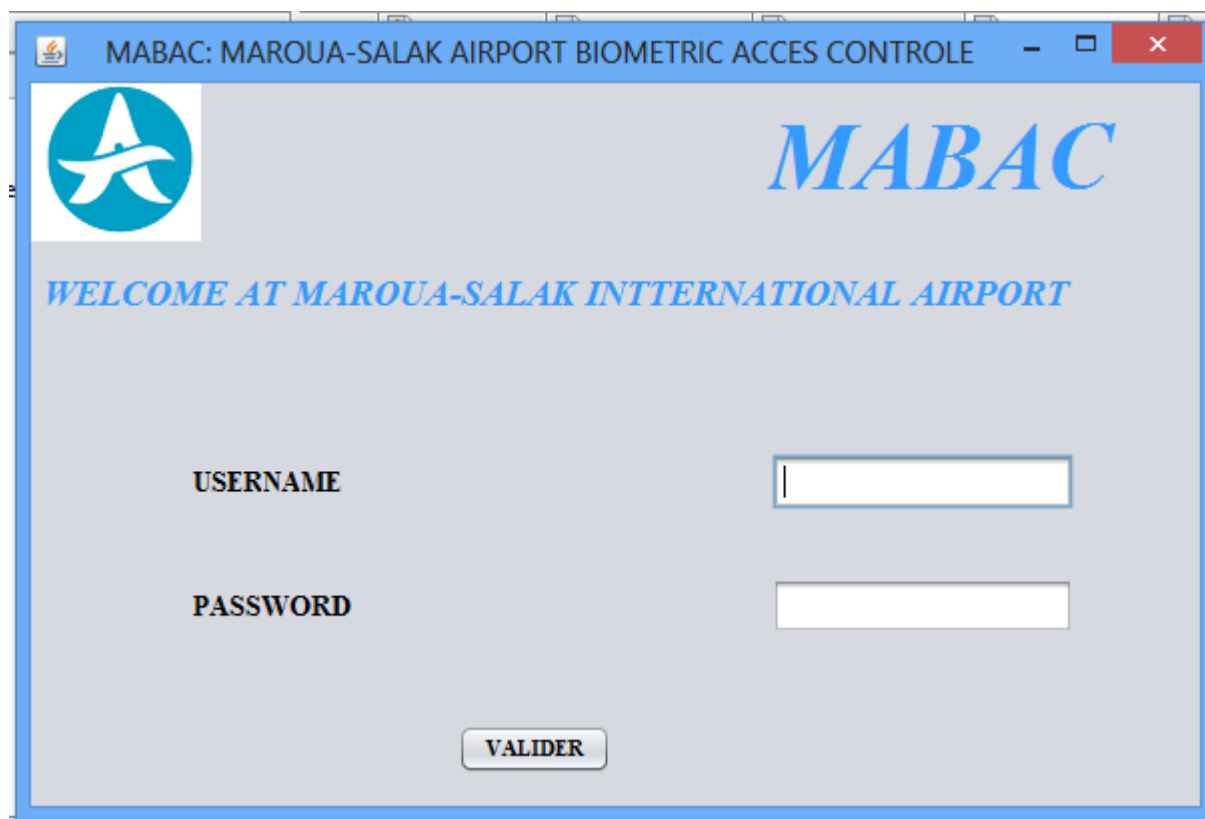
RÉSULTATS ET COMMENTAIRE

5.1 Introduction


Après avoir modélisée et conçue notre solution au chapitre 3, le chapitre précédent nous a permis de présenter les outils nécessaires à l'implémentation de notre solution. Il sera question dans cette partie de présenter les résultats obtenus et d'analyser leurs pertinences par rapport aux objectifs fixés.

5.2 Page d'accueil application

La page d'accueil de notre application est la première interface présentée à l'opérateur et au superviseur. Elle leur donne la possibilité de se connecter afin de pouvoir utiliser l'application.



MABAC: MAROUA-SALAK AIRPORT BIOMETRIC ACCES CONTROLE

 **MABAC**

WELCOME AT MAROUA-SALAK INTERNATIONAL AIRPORT

USERNAME

PASSWORD

VALIDER

FIGURE 5.1 – Page de login à l'application

Une fois que la personne a pu franchir cette étape, il lui reste à choisir l'opération à effectuer parmi les cinq opérations que fournit notre application.



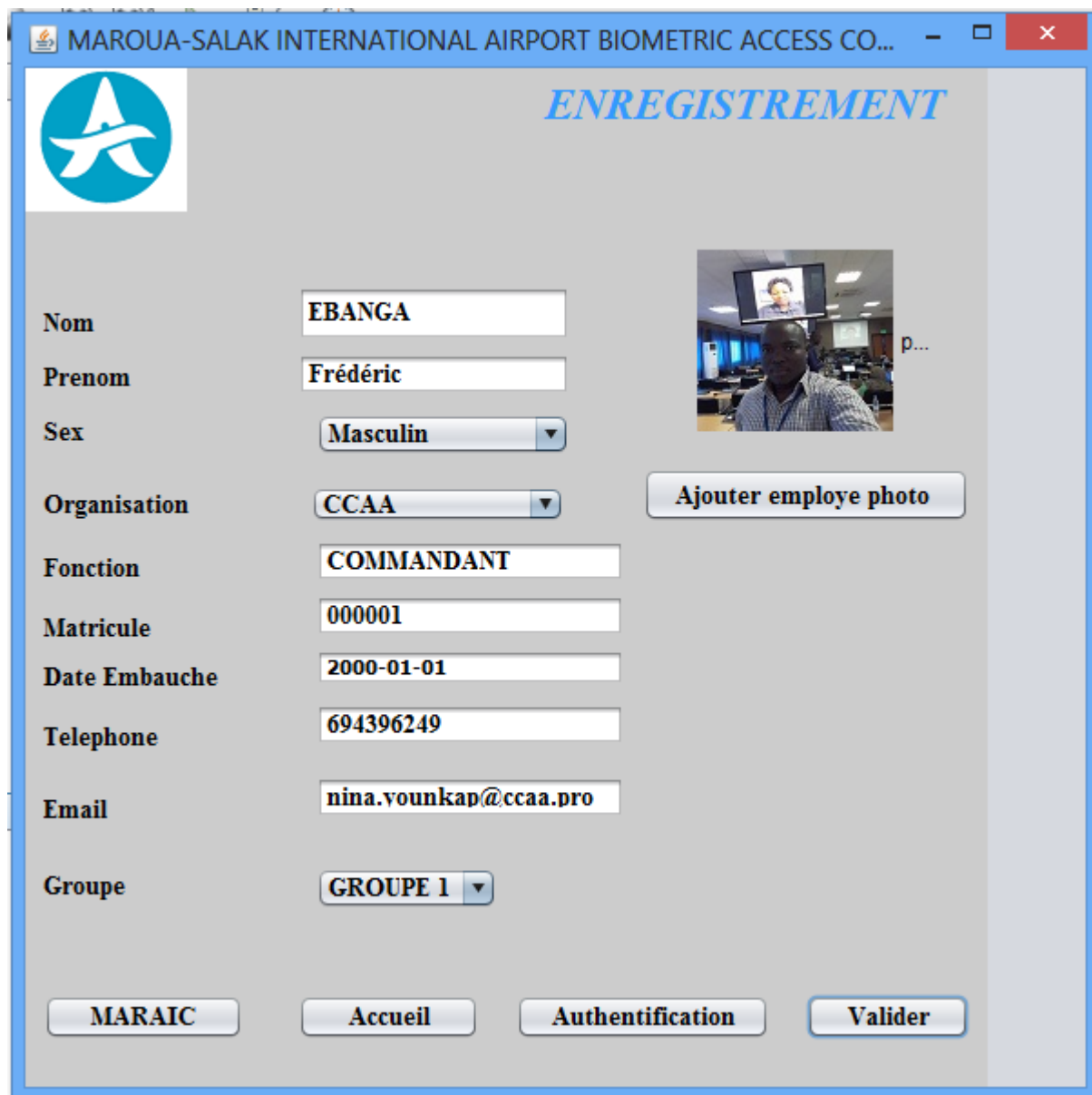
FIGURE 5.2 – Page d'accueil de l'application

5.3 Phase d'enregistrement

Dans cette partie nous montrons comment enregistrer les informations d'un employé dans la base de données et délivrer son badge de circulation MARAIC grâce notre application. Conformément à la matrice de contrôle d'accès présentée à la section 3.8.3, un employé de groupe 1 a les privilèges d'accès les plus élevés et peut accéder à toutes les zones de l'aéroport. C'est ce que nous allons vérifier en affichant son badge.

5.3.1 Enregistrement d'un employé de groupe 1

On peut constater que l'employé enregistré sur cette image appartient au groupe 1 de notre matrice de contrôle d'accès. Il s'agit en effet du Commandant d'Aéroport donc une personne qui possède en principe le privilège d'accéder à toutes les zones de l'aéroport.



The screenshot shows a web application window titled "MAROUA-SALAK INTERNATIONAL AIRPORT BIOMETRIC ACCESS CO...". The main heading is "ENREGISTREMENT". On the left is a logo featuring a stylized white bird or wing inside a blue circle. The form contains the following fields and values:

Label	Value
Nom	EBANGA
Prenom	Frédéric
Sex	Masculin
Organisation	CCAA
Fonction	COMMANDANT
Matricule	000001
Date Embauche	2000-01-01
Telephone	694396249
Email	nina.vounkap@ccaa.pro
Groupe	GROUPE 1

To the right of the form is a photo of a man, with a small inset image of a person's face on a screen. Below the photo is a button labeled "Ajouter employe photo". At the bottom of the window are four buttons: "MARAIC", "Accueil", "Authentification", and "Valider".

FIGURE 5.3 – Enregistrement d'un employé de groupe 1

5.3.2 le badge d'un employé

Une fois l'employé enregistré dans notre système, l'action suivante consiste à délivrer son badge MARAIC. On peut vérifier sur cette image que toutes les zones sont activées, pour indiquer que la personne à accès a toutes les zones de l'aéroport.

MARAIC

MAROUA-SALAK AIRPORT RESTRICTED AREA IDENTIFICATION CARD

NAME: EBANGA

SURNAME: Frédéric

MATRICULE: 000001

FONCTION: COMMANDANT

ORGANIZATION: CCAA

AUTHORIZED AREA

ZA	<input checked="" type="checkbox"/>	ZP	<input checked="" type="checkbox"/>
ZB	<input checked="" type="checkbox"/>	ZN	<input checked="" type="checkbox"/>
ZE	<input checked="" type="checkbox"/>	ZT	<input checked="" type="checkbox"/>
ZM	<input checked="" type="checkbox"/>	ZV	<input checked="" type="checkbox"/>

SIGNATURE

Exit

FIGURE 5.4 – Architecture d'un système de reconnaissance biométrique

5.4 Phase d'enrôlement

Dans cette phase d'enrôlement, il est question de capturer l'empreinte de l'employé préalablement enregistré et de stocker dans la base de données pour des opérations futures. Nous avons identifié plusieurs marques de lecteurs biométriques sur le marché, et avons permis à notre application de pouvoir prendre en charge quelques unes les

plus répandues ; ceci pour permettre à notre application de pouvoir être utilisée avec différents types de lecteur biométrique.

5.4.1 Connection à la base de données et choix du lecteur biométrique

Une fois l'application lancée, l'opérateur doit saisir le nom de la base de données utilisée, le mot de passe pour l'accès à la base de données et choisir le ou les lecteur(s) qu'il compte utiliser.

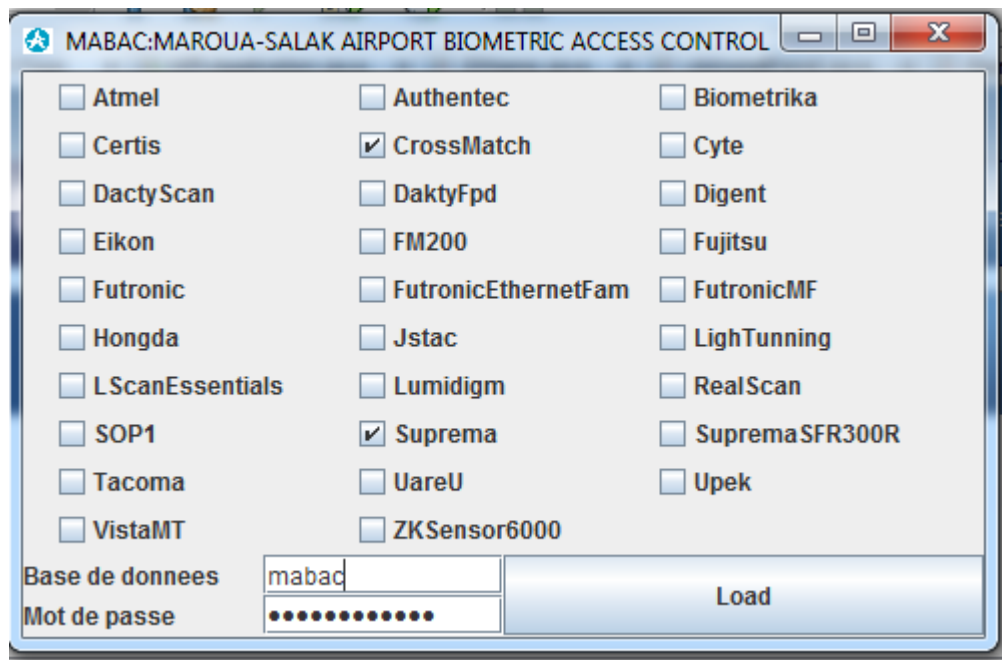


FIGURE 5.5 – Connection à la base de données et choix du lecteur

5.4.2 Enrôlement

Ici on aperçoit à droite la liste des personnes enrôlées dans notre base de données ; l'empreinte affichée est celle de l'employé ETOA sélectionné.

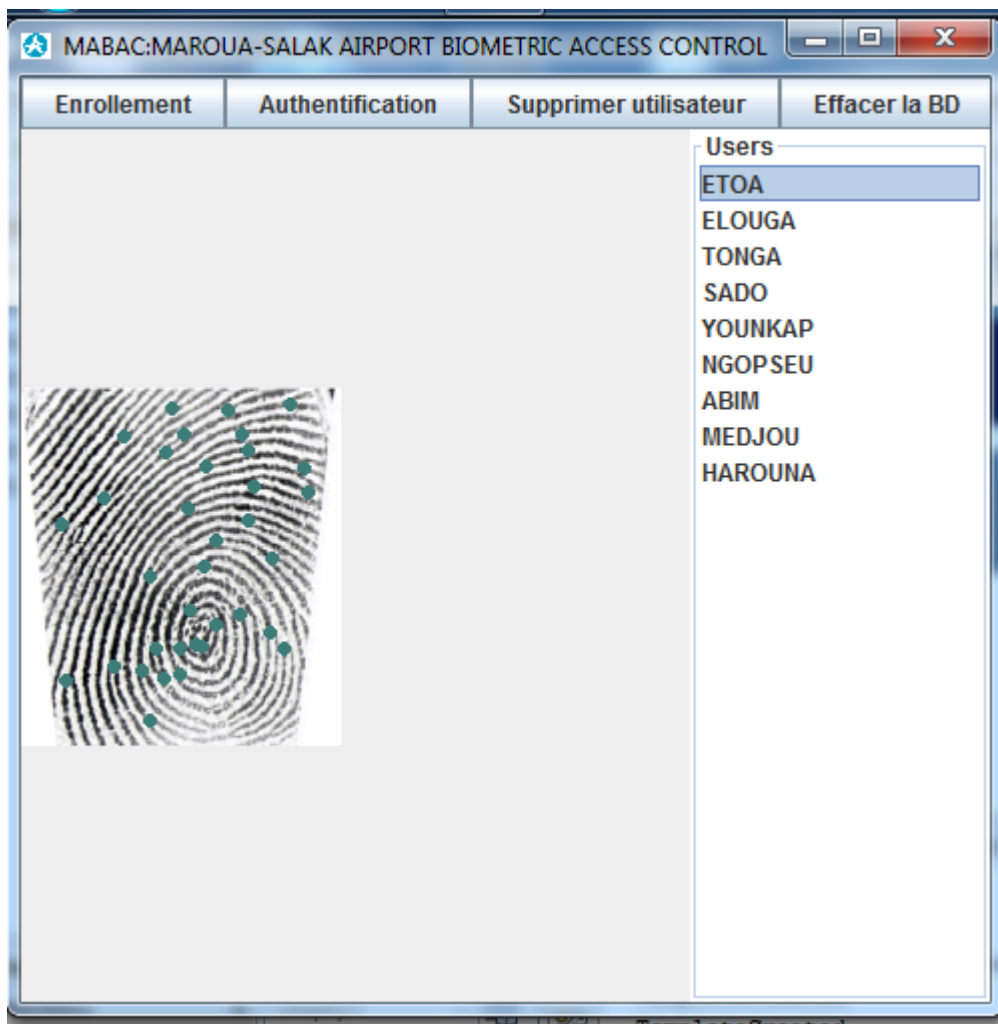


FIGURE 5.6 – Enrôlement d’un employé

5.5 Phase d’authentification

L’authentification consiste à s’assurer que la personne est bien celle qu’elle prétend être ; elle peut être positif dans le cas où un employé légitime tente de s’authentifier et négative en cas de fraude ou de tentative d’usurpation d’identité.

5.5.1 Authentification d’un utilisateur légitime

Ici l’utilisateur YOUNKAP préalablement enrôlé tente de s’authentifier, on voit bien que l’authentification est réussie.

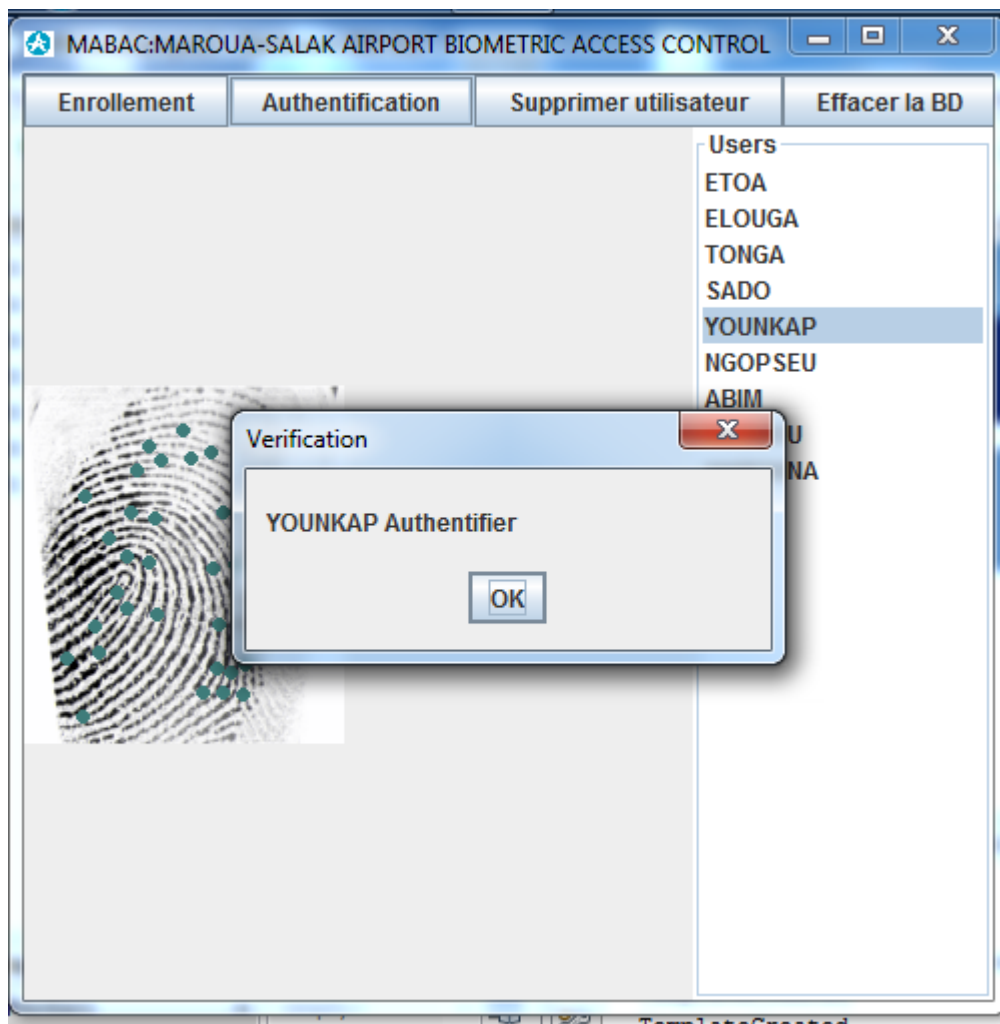


FIGURE 5.7 – Authentification d'un utilisateur légitime

5.5.2 Tentative d'usurpation d'identité

Ici un utilisateur tente de se faire passé pour TONGA, mais l'authentification échoue car son empreinte digitale ne correspond pas au modèle appartenant à TONGA qui a été stocké dans la base de données. Le système renvoie bien un échec d'authentification.

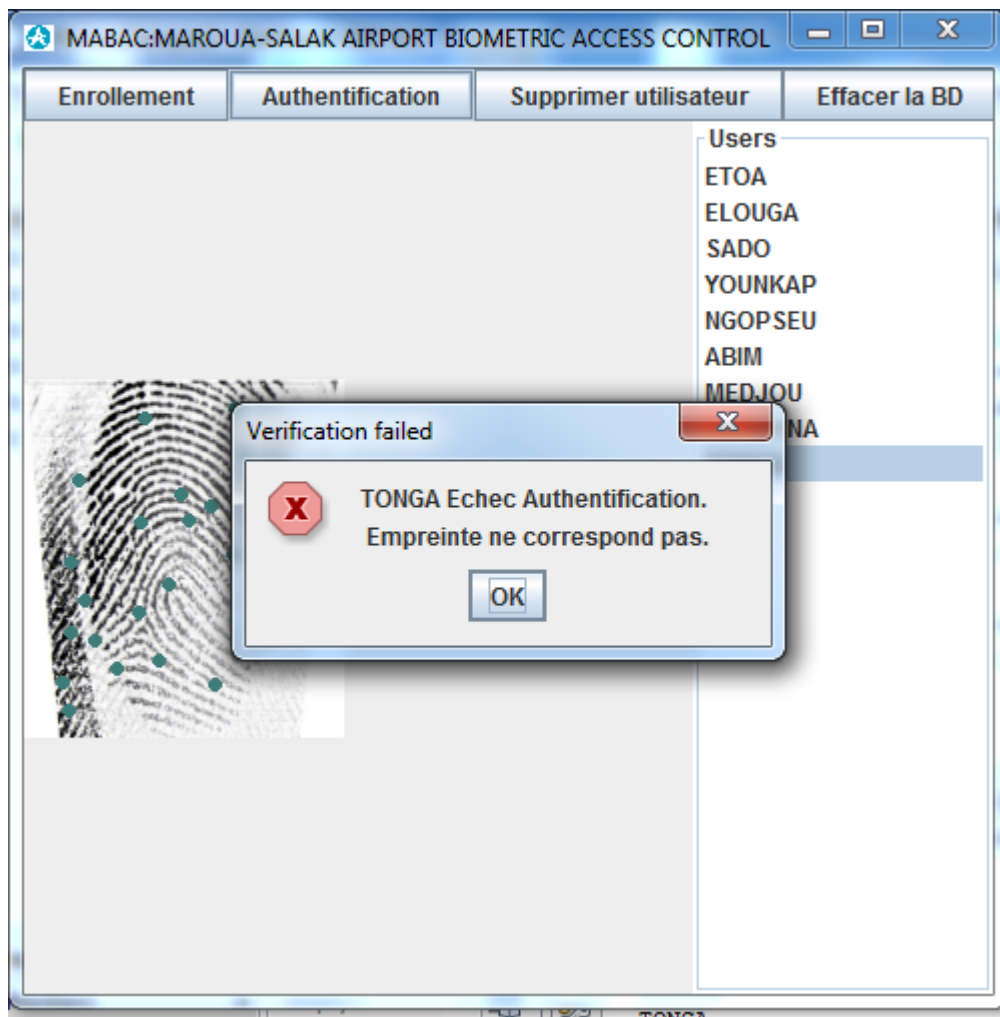


FIGURE 5.8 – Tentative d’usurpation d’identité

5.6 Conclusion

Dans ce chapitre, nous fait un état du fonctionnement de notre application MABAC qui implémente une solution de contrôle d’accès biométrique basée sur la vérification de l’empreinte digitale. Différentes interfaces ont été présentées ; les résultats obtenus répondent aux attentes exprimées en termes d’objectifs et de besoins.

CONCLUSION ET PERSPECTIVES

Parvenu au terme de notre travail, il était question de concevoir et implémenter une solution de sécurité pour l'Aéroport International de Maroua-Salak autour de la biométrie. Pour y arriver, nous avons dans un premier temps étudié la méthode de contrôle d'accès existante, puis une évaluation de sécurité que nous avons menée à travers une analyse du risque nous a permis de recenser l'ensemble des ressources à protéger ; identifier les menaces qui pèsent sur ces ressources et les vulnérabilités. Notre solution permet d'authentifier les personnes qui accèdent aux zones sensibles de l'aéroport et fournir un moyen de contrôle du mouvement des personnes à l'intérieur de ces zones afin de s'assurer que seuls les employés auxquels des privilèges d'accès ont été accordés à des zones sensibles en conformité avec leur zones de travail respectives peuvent accéder à ces zones.

Pour y arriver, nous avons proposé une solution à deux niveaux. En première ligne, nous avons conçu et implémenté une solution d'authentification biométrique basée sur la vérification de l'empreinte digitale. Cette solution doit être placée au niveau des principaux points d'entrée à l'aéroport. Très conscient de la difficulté à pouvoir placer un lecteur biométrique à l'entrée de chaque zone qui sont pour la plupart des zones exposées sans portes, nous avons proposé une matrice de contrôle d'accès basée sur le principe du privilège minimum qui utilise des badges pour faciliter le mouvements des personnes à l'intérieure de ces zones. Cette solution de permis de circulation est une mesure qui est d'ailleurs proposée dans l'Annexe 17 relative à la sûreté de l'aviation civile.

Une enquête sur la connaissance et l'acceptabilité des technologies d'authentification biométrique que nous avons menée nous a permis de capturer les besoins fonctionnels de l'application à développer, ainsi que les attentes des futures utilisateurs. Au départ, cinq opérations ont été prévues dans notre système et quatre ont été implémentées avec succès. Nous avons rencontré d'énormes difficultés, la première est la non disponibilité du lecteur biométrique sur le marché camerounais ; nous l'avons acheté en ligne aux États-Unis.

Une orientation futur à ce travail peut être la biométrie sur carte à puce, il s'agit d'un système où les données biométriques ne sont plus stockées dans une base de don-

nées, mais directement sur le badge de l'employé. L'absence d'une base de données pour stocker les modèles biométriques offre à ce système une meilleure garantie en terme de protection de la vie privée et peut être utilisé à l'échelle nationale pour authentifier les employés dans tous les aéroports du Cameroun. Il est actuellement utilisé dans certains grands aéroports du monde comme Amsterdam Schiphol Airport en Hollande qui permet de gérer les accès de plus 60000 employés appartenant à plus de 500 entreprises différentes ou encore la Canadian Airport Restricted Area Identification Card permettant de gérer les employés dans 29 grands aéroports au Canada.[28]

RÉFÉRENCES

- [1] Makori Abanti, Cyrus. Integration of biometrics with cryptographic techniques for secure authentication of networked data access, jul 2009. Information Technology, 13 pages.
- [2] Dennis ALAN., Haley BARBARA, and M. ROTH ROBERTA L. *Systems Analysis and Design IN CHANGING WORLD, Sith Edition*. COURSE TECHNOLOGY Cengage Learning, Fith v Edition, 2012.
- [3] Sanchez Rinza Barbara, Emma and gonzalez Otto, Hernandez. Rfid identification cards at 13.56 mhz using biometric techniques, Aug 2011. 9th Latin American and Caribbean Conference for Engineering and Technology, August 3-5, Medellín, Colombia, 10 pages.
- [4] LAOUKOURA Charles. *Reconnaissance automatique des empreintes digitales*. Ecole Nationale Polythenique de Maroua, 2018.
- [5] Le Chien. A survey of biometrics security systems, Nov 2011. <http://www.cse.wustl.edu/jain/cse571-11/ftp/biomet/index.html>, Last Modified on : November 28, 2011 10 pages.
- [6] Crossmatch. U.are.u® sdk v3, developer guide, Jun 2006. www.crossmatch.com, Revised : June 14, 2017, version 3.0.1.
- [7] Crossmatch. U.are.u® sdk v3, platform guide for windows, Feb 2017. www.crossmatch.com, Published : February 22, 2017 v3.0.0.
- [8] Bhattacharyya Debnath, Ranjan Rahul, A. Farkhod, Alisherov, and Choi Minkyu. Biometric authentication : A review. *International Journal of u- and e- Service, Science and Technology*, page 16, sep 2009.
- [9] Emanuil Dimitrov. Fingerprints recognition, Jun 2009. Reports from MSI, School of Mathematics and Systems Engineering, Växjö University, 50 pages.

- [10] Etat du Cameroun. Loi n°2010/012 du 21 decembre 2010 relative à la cybersécurité et la cybercriminalité au cameroun, Décembre 2010.
- [11] Simon Fong and Yan Zhuang. Using medical history embedded in biometrics medical card for user identity authentication : Privacy preserving authentication model by features matching. *Journal of Biomedicine and Biotechnology*, page 11, May 2012.
- [12] GAO. Using biometrics for border security. *United States General Accounting Office*, November 2002.
- [13] Shelly Gary B. and Rosenblatt Harry J. *Systems Analysis and Design*. COURSE TECHNOLOGY Cengage Learning, Ninth Edition, 2012.
- [14] Tialk Girish and Shivamurthy. Applications of biometric in automobiles. *International Research Journal of Engineering and Technology (IRJET)*, page 6, Feb 2018.
- [15] Steven Gordon. User authentication, its335 : It security, Oct 2013. Sirindhorn International Institute of Technology, Thammasat University, 40 pages.
- [16] Satzinger Jhon W., Jackson Robert B., and Burd Stephen D. *Systems Analysis and Design IN CHANGING WORLD, Sith Edition*. COURSE TECHNOLOGY Cengage Learning, Sith Edition, 2012.
- [17] Liou Jing-Chiou, Egan Gregory, Patel Jay K., and Bhashyam Sujith. A sophisticated rfid application on multi-factor authentication. *Departement of Computer Science, Kean University, USA*, 2014.
- [18] Choudhary Jitendra. Survey of different biometrics techniques. *International Journal of Modern Engineering Research(IJMER)*, September 2012.
- [19] Condon Mable. *Introduction to Biometrics*. Library Press, 2016.
- [20] Davide Maltoni. *BioLab, Fingerprint Recognition Basics and Recent Advances*. University of Bologna - ITALY.
- [21] Manivannan and Padma. Comparative and analysis of biometric systems. *International Journal on Computer Science and Engineering*, page 07, May 2011.
- [22] Véronique Messéant. *Modélisation, Les empreintes digitales*. Université de Paris VII, 2006.

- [23] Chandra Namita, Taksal Ashwini, Shinde Dhanshri, and Lomte Prof., Archana. Sensitive data protection using bio-metrics. *International Journal of Advanced Research in Computer Science and Software Engineering*, page 07, Jan 2014.
- [24] GALY Nicola. *Etiude d'un système complet de reconnaissance d'empreinte digitales pour un capteur microsysteme à balayage*. PhD thesis, Institut Nationale polytechnique de grenoble, 2005.
- [25] OBI NTUI. *Cours de formation en surété de l'aviation civile*. OACI, 2017.
- [26] OACI. *Annexe 17 à la convention relative à l'aviation civile internationale*. Organisation de l'aviation civile internationale, 2011.
- [27] G. Priya, Lakshmi, M. Pandimadevi, G. Priya, Ramu, and P. Ramya. Implementation of attendance management system using smart-fr. *International Journal of Advanced Research in Computer and Communication Engineering*, page 05, Nov 2014.
- [28] Alliance Smart, Card. Smart cards and biometrics. *SmartCard Alliance Physical Access Council*, page 24, March 2011.
- [29] Alliance Smart, Card. Module 1 : Smart card fundamentals, May 2015. Version 5, <http://www.smartcardalliance.org>, 68 pages.
- [30] Ghernaouti Solange. *Sécurité informatique et réseaux*. DUNOD, 2004.
- [31] William Stallings and Lawrie Brown. *Computer Security Principles and Pratices, Third Edition*. Pearson Education, Inc, www.allitebooks.com, 2015.
- [32] Edward Stead. Integration of physical access security and logical access security using microsoft active directory, 2006. thesis, Computing and Management, 83 pages.
- [33] Michael Whitman, E. and Herbert Mattord, J. *Principles of Information Security, Fourth Edition*. Cengage Learning, www.course.com, 2012.
- [34] Saheed Yakub K. and Hambali Moshood A. Fingerprint based approach for examination clearance in higher institutions. *FUOYE Journal of Engineering and Technology*, page 6, March 2017.
- [35] N. Yanushkevich, S. Fundamentals of biometric system design, Jun 2014. 38 pages.

ANNEXE A : ÉVALUATION DE SÉCURITÉ DE L'AÉROPORT

I- Contexte

Cette évaluation de sécurité entre dans le cadre du mémoire de fin d'étude d'Ingénieur de conception en Informatique et Télécommunication spécialité Sécurité informatique et cryptographie à l'Ecole Nationale Supérieure Polytechnique de Maroua dont le thème est intitulé « **Sécurisation de l'Aéroport International de Maroua-Salak par une solution de contrôle d'accès biométrique** ».

II- Objectifs du thème

Notre étude vise à concevoir et implémenter une politique de contrôle d'accès simple, efficace et fiable pour l'authentification des personnes, la gestion des autorisations d'accès aux zones réservées de l'aéroport et le contrôle du mouvement des personnes dans les zones réservés de l'aéroport en conformité avec leurs zones de travail respectives. Elle se limitera au contrôle d'accès du personnel de l'aéroport, c'est-à-dire des personnes qui sont amenées à exercer de façon temporaire ou permanente une fonction spécifique au sein de l'aéroport. La solution proposée devra être conforme aux dispositions réglementaires en matière de sûreté de l'aviation civile notamment : l'Annexe 17(Sûreté), le DOC 8973 (Manuel de sûreté de l'aviation civile) et du PNS (Programme National de sûreté de l'aviation civile).

III- Objectifs évaluation de sécurité

Cette étude vise à identifier les ressources à protéger, les vulnérabilités et les menaces qui pèsent sur ces ressources. Une analyse du risque au regard des contre-mesures existants permettra de capturer les exigences de sécurité pour chaque ressource et les besoins fonctionnelles de l'application. Ce qui permettra de choisir une solution adaptée qui implémentera les contre-mesures pour résoudre les problèmes identifiés dans la

méthode de contrôle d'accès existante.

IV- Méthodologie

La méthodologie adoptée de cette étude est une approche informelle basée sur le jugement des experts. Elle s'inspire de celle présentée dans le livre intitulé « Computer Security Principles and Practice, Third Edition, PEARSON, 2015 (page 492 à 509) » de l'auteur « William Stallings » que vous trouverez ci-joint. L'intérêt de cette méthodologie réside dans le fait qu'elle fournit un résultat rapide à moindre coût et est adaptée pour les structures de petite taille comme la nôtre ; elle est également compatible avec la norme **ISO 27005 « Information security risk management »** relative à la gestion de risque dans les systèmes d'information.

V- Définitions importantes

Sécurité : la notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité et s'exprime le plus souvent par les objectifs de sécurité suivants : la disponibilité, l'intégrité, la confidentialité, la non répudiation et l'authentification.

la disponibilité d'une ressource est relative à la période de temps pendant laquelle le service est offert et opérationnel. Il ne suffit pas qu'elle soit disponible, elle doit pouvoir être accessible et utilisable par l'ensemble des ayants droits avec un temps de réponse acceptable.

Le critère d'intégrité des ressources physiques et logiques est relatif au fait qu'elles ne doivent pas être détruites ou modifiées à l'insu de leur propriétaire tant de manière intentionnelle qu'accidentelle.

La confidentialité peut être vue comme la protection des données contre une divulgation, elle permet de s'assurer que seules les personnes habilitées à lire ou à modifier une information puissent le faire.

Authentification : critère de sécurité défini par un processus mis en œuvre notamment pour vérifier l'identité d'une personne physique ou morale et s'assurer que l'identité fournie correspond à l'identité de cette personne préalablement enregistrée (Cf Loi N°2010/012).

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu ; à ce critère de sécurité peuvent être associés les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité.

L'imputabilité se traduit par l'attribution d'une action (événement) à une entité déterminée (ressource, personne).

Sûreté de l'Aviation Civile : Combinaison de mesures et ressources humaines et matérielles destinées à protéger l'aviation civile contre les actes d'intervention illicite.

Contrôle d'accès = Identification+Authentification+Autorisation+Auditabilité

VI- Tableau d'enregistrement des risques

Objets à protéger	Menaces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
Piste 13	Incursion sur piste/Trous dans la clôture de sureté	Visite de piste régulière, Surveillance des contrôleurs	Probable	Insignifiant	Moyen
Piste 31	Incursion sur piste/Trous dans la clôture de sureté	Visite de piste régulière, Surveillance des contrôleurs	Probable	Insignifiant	Moyen
Feux de piste	Destruction, vol, sabotage/ Trous dans la clôture de sureté	Visite de piste régulière, Surveillance des contrôleurs	Improbable"	Modéré	Moyen
PAPI 13	Destruction, vol, sabotage	Visite régulière des installations	Improbable	Majeur	Extrême
PAPI 31	Destruction, vol, sabotage	Visite régulière des installations	Improbable	Majeur	Extrême
Feux d'approche	Destruction, vol, sabotage	Visite régulière des installations	Improbable	Majeur	Extrême
Passager VIP	Atteinte physique/morale	protection des aires de mouvement et des salles VIP par le personnel de sûreté	Probable	Majeur	Extrême
AVION	Destruction, sabotage	protection des aires de mouvement par le personnel de sûreté	Improbable	Catastrophique	Extrême
PILOTE	Atteinte physique/morale	protection des aires de mouvement par le personnel de sûreté	Improbable	Majeur	Extrême

Objets à protéger	Me- naces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
PNC	Atteinte physique/morale	protection des aires de mouvement par le personnel de sûreté	Improbable	Modéré	Élevé
PNT	Atteinte physique/morale	protection des aires de mouvement par le personnel de sûreté	Rare	Modéré	Élevé
Passager	Atteinte physique/morale	protection du circuit passager par le personnel de sûreté	Possible	Mineur	Élevé
Bagage	Vol, bagage endommagé, bagage piégé de matériels dangereux (explosifs, ...)	Protection du circuit de bagage par le personnel de sûreté	Possible	Modéré	Élevé
NDB	Destruction, vol, sabotage	Local verrouillé, visite quotidienne,Présence de gardien en permanence/trous dans la clôture de sûreté	Rare	Modéré	Moyen
ILS/LLZ	Destruction, vol, sabotage	Observation régulière/trous dans la clôture, exposition	Improbable	Majeur	Moyen
ILS/DME	Destruction, vol, sabotage	Observation régulière/trous dans la clôture, exposition	Improbable	Majeur	Moyen
ILS/GP	Destruction, vol, sabotage	Observation régulière/trous dans la clôture, exposition	Rare	Majeur	Extrême
VOR	Destruction, vol, sabotage	Observation régulière/trous dans la clôture, exposition	Rare	Majeur	Extrême
VOR/DME	Destruction, vol, sabotage	Présence des gardien, surveillance à distance/Hors de la clôture	Possible	Majeur	Extrême

Objets à protéger	Menaces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
Capteur vent	Destruction, vol, sabotage	Visite régulière, surveillance continue par les contrôleurs	Rare	Modéré	Extrême
Capteur pression	Destruction, vol, sabotage	Visite régulière, surveillance continue par les contrôleurs	Rare	Modéré	Extrême
Télémètre de nuage	Destruction, vol, sabotage	Visite régulière, surveillance continue par les contrôleurs	Rare	Modéré	Extrême
Capteur visibilité	Destruction, vol, sabotage	Visite régulière, surveillance continue par les contrôleurs	Rare	Modéré	Extrême
Groupe électrogène	Destruction, vol, sabotage	Local verrouillé	Possible	Majeure	Extrême
Soute carburant	Destruction, sabotage	Local Verrouillé	Rare	Majeure	Catastrophique
Télécommande feux piste	Destruction, sabotage	Local sûr, surveillé en permanence	Improbable	Modéré	Moyen
Caisse à outils	vol	Coffre verrouillé	Improbable	Modéré	Extrême
Surveillance NAVAID	Sabotage de l'appareil de surveillance	Local sécurisé, surveillance continue	Improbable	Majeure	Extrême

Objets à protéger	Me- naces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
Serveur INTER-CONNEX	Destruction, vol, sabotage	Surveillance continue, salle verrouillée	Improbable	Insignifiant	Moyen
Ordinateur CIMEL	Destruction, vol, sabotage	Surveillance continue, salle verrouillée	Improbable	Majeure	Extrême
Téléphone interne	Destruction, vol	Surveillance continue, salle verrouillée	Improbable	Insignifiant	Moyen
Téléphone externe	Destruction, vol	Surveillance continue, salle verrouillée	Improbable	Modéré	Élevé
Téléphone fixe	Destruction, vol	Surveillance continue, salle verrouillée	Rare	Insignifiant	Moyen
Caisse redevances	Vol	Coffre fort/ accès à la salle par des personnes étrangère	Possible	Majeure	Extrême
Véhicules incendies et accès-soires	sabotage	Surveillance régulière	Possible	Majeure	Extrême
Manuel d'exploitation	Vol, sabotage	Surveillance continue	Rare	Insignifiant	Faible

Objets à protéger	Menaces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
Document bureau	Vol, sabotage	Surveillance continue	Rare	Insignifiant	Faible
Document diverse	Vol, sabotage	Surveillance continue	Rare	Insignifiant	Faible
VHF	Vol, sabotage, brouillage	Surveillance continue/absence de moyen anti-brouillage,Local non verrouillé	Possible	Majeur	Extrême
Contrôleur aérien	Atteinte physique, morale	Local non verrouillé	Improbable	Modéré	Élevé
VHF	Vol, sabotage	Surveillance continue/Local non verrouillé	Possible	Insignifiant	Moyen
Téléphone de coordination	Vol, sabotage		Possible	Majeure	Moyen
Procédure de vol	vol, sabotage	Surveillance continue/Local non verrouillé	Possible	Modéré	Extrême
Biens passagers	vol, sabotage	Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Improbable	Insignifiant	Élevé
Biens personnes VIP	vol, sabotage	Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Possible	Modéré	Extrême

Objets à protéger	Menaces/Vulnérabilités	Contre-mesure existantes	Probabilité	Conséquence	Niveau de risque
Autorité administratives	Atteinte physique, morale	Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Improbable	Mineure	Élevé
Autorité locale	Atteinte physique, morale	Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Improbable	Mineure	Élevé
Autorité aéroportuaire	Atteinte physique, morale	Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Improbable	Mineure	Élevé
Véhicules de transport personnel technique	sabotage, vol	Visite routinière par le chauffeur, Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Possible	Modéré	Extrême
Véhicules agence transport personnel ADC	sabotage, vol	Visite routinière par le chauffeur, Présence des agents de sûreté et de sécurité/contrôlé d'accès peu fiable	Probable	Mineure	Élevé

ANNEXE B : ENQUÊTE DE TERRAIN

Contexte

Cette enquête entre dans le cadre du mémoire de fin d'étude d'Ingénieur de conception en Informatique et Télécommunication spécialité Sécurité informatique et cryptographie à l'Ecole Nationale Supérieure Polytechnique de Maroua dont le thème est intitulé. **Sécurisation de l'Aéroport International de Maroua-Salak par une solution de contrôle d'accès biométrique**

Objectif du thème

Notre étude vise à concevoir et implémenter une politique de contrôle d'accès simple, efficace et fiable pour l'authentification des personnes, la gestion des autorisations d'accès aux zones réservées de l'aéroport et le contrôle du mouvement des personnes dans les zones réservées de l'aéroport en conformité avec leurs zones de travail respectives. Elle se limitera au contrôle d'accès du personnel de l'aéroport, c'est-à-dire des personnes qui sont amené à exercer de façon temporaire ou permanente une fonction spécifique au sein de l'aéroport de Maroua-Salak. La solution proposée devra être conforme aux dispositions réglementaires en matière de sûreté de l'aviation civile notamment : l'Annexe 17(Sûreté), le DOC8 973 (Manuel de sûreté de l'aviation civile) et du PNS (Programme National de sûreté de l'aviation civile).

Objectif de l'enquête

Cette enquête vise à identifier les paramètres qui peuvent influencer l'acceptabilité d'une technologie d'authentification par les utilisateurs. Les facteurs tels que, l'aisance, la protection de la vie privée, les mœurs culturelles, permettront de capturer les besoins non fonctionnels de l'application. L'analyse de ces besoins non fonctionnels permettra de prendre en compte les exigences des utilisateurs dans la conception de notre solution et

le choix des technologies et équipements qui permettront de l'implémenter.

Définitions importantes

Sécurité : la notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité et s'exprime le plus souvent par les objectifs de sécurité suivants : la disponibilité, l'intégrité, la confidentialité, la non répudiation et l'authentification.

La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service est offert et opérationnel. Il ne suffit pas qu'elle soit disponible, elle doit pouvoir être accessible et utilisable par l'ensemble des ayant droit avec un temps de réponse acceptable.

Le critère d'intégrité des ressources physiques et logiques est relatif au fait qu'elles ne doivent pas être détruites ou modifiées à l'insu de leur propriétaire tant de manière intentionnelle qu'accidentelle.

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu ; à ce critère de sécurité peuvent être associés les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité.

L'imputabilité se traduit par l'attribution d'une action (événement) à une entité déterminée (ressource, personne).

Sûreté de l'Aviation Civile : Combinaison de mesures et ressources humaines et matérielles destinées à protéger l'aviation civile contre les actes d'intervention illicite.

Contrôle d'accès = Identification + Authentification + Autorisation + Auditabilité

Question

Question 1 : Quelle place occupe l'authentification des personnes dans la politique globale de sécurité de l'aéroport ?

- a) Très important
- b) Important
- c) Peu important
- d) Sans intérêt

Commentaire(si nécessaire) :

Question 2 : Que pensez-vous de la méthode d'authentification des personnes et de la gestion des autorisations d'accès aux zones règlementées de l'aéroport existante ?

- a) Très satisfaisant
- b) Satisfaisant
- c) peu satisfaisant

Commentaire(si nécessaire) :

Question 3 : Quelles sont les critères qui peuvent influencer votre choix d'une méthode d'authentification des personnes ?

Critère	Degré d'importance			
	Très important	Important	Peu important	Sans importance
Efficacité				
Cout				
Réduction de délai d'attente				
Facilité d'usage				
Protection de la vie privée				

Commentaire(si nécessaire) :

Question 4 : Êtes-vous familier avec les méthodes d'authentification suivantes ?

Méthode d'authentification	Degré de familiarité		
	Familier	Peu familier	Jamais utiliser
Mot de passe (code PIN)			
Carte à puce (ex carte bancaire)			
Biométrie			
Carte à puce + PIN			
Biométrie + PIN			
Biométrie + carte			

Commentaire(si nécessaire) :

Question 5 : Aviez-vous assez d'information sur les technologies biométriques suivantes ?

Technologie d'authentification	Degré d'information			
	Très informé	Informé	Peu informé	Aucune idée
La voix				
La géométrie de la main				
La reconnaissance faciale				
L'iris				
La rétine				
La voix				
La dynamique du clavier				

Commentaire si nécessaire :

Question 6 : Quels sont les facteurs qui vous dérange dans la technologie biométrique ?

Technologie	Facteurs				
	Aspect policier	Incompatibilité avec les mœurs culturelles	Violation de la vie privée	Possibilité de vol d'identité	Autre (préciser)
L'empreinte digitale					
La voix					
La géométrie de la main					
La reconnaissance faciale					
L'iris					
La rétine					
La voix					
La dynamique du clavier					

Commentaire(si nécessaire) :

Maitrise du document

Rôle	Nom	Fonction	Qualité	Signature
Rédacteur	YOUNKAP NINA Duplex	Elève Ingenieur en sécurité informatique	Elève Ingénieur	
Vérificateur	Dr.OUMAROU	Enseignant à ENS de MAROUA	Encadreur académique	
Superviseur	CDT EBANGA Frédéric	Commandant d'Aéroport de Maroua-salak	Encadreur professionnel	

Répondu par :

Nom	Prénom	Organisation	Fonction	Signature