

*République Algérienne Démocratique et Populaire*  
*Ministère de l'Enseignement Supérieur et de la Recherche Scientifique*  
Université des Sciences et de la Technologie Houari Boumediene

INSTITUT DE

Mémoire du Projet de fin d'études

Pour l'obtention du diplôme  
d'ingénieur d'état en informatique

Option :

SUJET :

Conception et mise en œuvre d'un système de  
détection à base de cas

Thème proposé par :

Etudié par :

Encadré par : Mme Aliane, Mme Benmeziane

OUCHEN Mohamed  
TEHARI Mohamed

Soutenu le :

Devant le jury composé de :

Président,  
Rapporteur,  
Examineur,  
Examineur,

PROMOTION :

## SOMMAIRE

INTRODUCTION GENERALE.....-1-

### CHAPITRE 1 : INTELLIGENCE ARTIFICIELLE

I.	INTRODUCTION .....	ERREUR ! SIGNET NON DEFINI.
II.	DEFINITION .....	ERREUR ! SIGNET NON DEFINI.
III.	BREF HISTORIQUE.....	ERREUR ! SIGNET NON DEFINI.
IV.	LES DOMAINES D'APPLICATIONS.....	ERREUR ! SIGNET NON DEFINI.
	1. Les robots et systèmes autonomes .....	<b>Erreur ! Signet non défini.</b>
	2. Les systèmes experts.....	<b>Erreur ! Signet non défini.</b>
	3. Le raisonnement basé sur le cas.....	<b>Erreur ! Signet non défini.</b>
	4. La reconnaissance de la parole .....	<b>Erreur ! Signet non défini.</b>
	5. Le traitement du langage naturel (TLN).....	<b>Erreur ! Signet non défini.</b>
	6. La vision par ordinateur.....	<b>Erreur ! Signet non défini.</b>
V.	LES SYSTEMES A BASE DE CONNAISSANCE (SBC) .....	ERREUR ! SIGNET NON DEFINI.
	1. Définition (La connaissance).....	<b>Erreur ! Signet non défini.</b>
	2. Types de connaissances .....	<b>Erreur ! Signet non défini.</b>
	2.1. Connaissances empiriques.....	<b>Erreur ! Signet non défini.</b>
	2.2. Connaissances théoriques.....	<b>Erreur ! Signet non défini.</b>
	3. Représentation des connaissances .....	<b>Erreur ! Signet non défini.</b>
	3.1. Représentation procédurale .....	<b>Erreur ! Signet non défini.</b>
	3.2. Représentation déclarative .....	<b>Erreur ! Signet non défini.</b>
	3.3. Représentation structurée .....	<b>Erreur ! Signet non défini.</b>
	3.3.1 Les réseaux sémantiques.....	<b>Erreur ! Signet non défini.</b>
	3.3.2 Les schémas (frames).....	<b>Erreur ! Signet non défini.</b>
	3.4. L'orienté objets (OO).....	<b>Erreur ! Signet non défini.</b>
	4. Exemples des systèmes à base de connaissance .....	<b>Erreur ! Signet non défini.</b>
	4.1 Les systèmes expert.....	<b>Erreur ! Signet non défini.</b>
	4.1.1 Base de Connaissances .....	<b>Erreur ! Signet non défini.</b>
	4.1.2 Moteur d'Inférence .....	<b>Erreur ! Signet non défini.</b>
	4.1.3 Module d'acquisition de connaissances.....	<b>Erreur ! Signet non défini.</b>
	4.1.4 Module d'explication.....	<b>Erreur ! Signet non défini.</b>
	4.1.5 Interface avec l'utilisateur .....	<b>Erreur ! Signet non défini.</b>
	4.2 Les systèmes à base de cas .....	<b>Erreur ! Signet non défini.</b>
	4.2.1 Principes de base.....	<b>Erreur ! Signet non défini.</b>
	4.2.2 Composantes d'un système à base de cas.....	<b>Erreur ! Signet non défini.</b>
VI.	CONCLUSION.....	ERREUR ! SIGNET NON DEFINI.

### CHAPITRE 2 : SECURITE INFORMATIQUE

I.	INTRODUCTION .....	ERREUR ! SIGNET NON DEFINI.
II.	CONCEPTS DE SECURITE.....	ERREUR ! SIGNET NON DEFINI.
	1. Le domaine de la sécurité.....	<b>Erreur ! Signet non défini.</b>
	2. Les Aspects de la sécurité informatique.....	<b>Erreur ! Signet non défini.</b>
	2.1 Confidentialité des données.....	<b>Erreur ! Signet non défini.</b>

2.2 Intégrité des données .....	<b>Erreur ! Signet non défini.</b>
2.3 Disponibilité de service .....	<b>Erreur ! Signet non défini.</b>
3. Méthodologie .....	<b>Erreur ! Signet non défini.</b>
<b>III. LES MENACES.....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. Que peut faire une attaque ? .....	<b>Erreur ! Signet non défini.</b>
2. Pourquoi il y a des menaces ? .....	<b>Erreur ! Signet non défini.</b>
3. Classification des menaces .....	<b>Erreur ! Signet non défini.</b>
3.1. Les menaces accidentelles .....	<b>Erreur ! Signet non défini.</b>
3.2. Les menaces intentionnelles (les attaques) .....	<b>Erreur ! Signet non défini.</b>
3.2.1 Les attaques passives .....	<b>Erreur ! Signet non défini.</b>
3.2.2 Les attaques actives .....	<b>Erreur ! Signet non défini.</b>
4. Quelques types d'attaques .....	<b>Erreur ! Signet non défini.</b>
4.1 Le déni de service (DoS) .....	<b>Erreur ! Signet non défini.</b>
a) Syn flooding .....	<b>Erreur ! Signet non défini.</b>
b) Smurf .....	<b>Erreur ! Signet non défini.</b>
d) Déni de service distribué .....	<b>Erreur ! Signet non défini.</b>
4.2 Le spamming .....	<b>Erreur ! Signet non défini.</b>
4.3 Les chevaux de Troie .....	<b>Erreur ! Signet non défini.</b>
4.4 Les bombes logiques .....	<b>Erreur ! Signet non défini.</b>
4.5 Les vers .....	<b>Erreur ! Signet non défini.</b>
4.6 Les virus .....	<b>Erreur ! Signet non défini.</b>
4.7 Le sniffing .....	<b>Erreur ! Signet non défini.</b>
<b>IV. LES SERVICES DE SECURITE .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. La confidentialité des données .....	<b>Erreur ! Signet non défini.</b>
2. L'intégrité des données .....	<b>Erreur ! Signet non défini.</b>
3. L'authentification .....	<b>Erreur ! Signet non défini.</b>
4. Le contrôle d'accès .....	<b>Erreur ! Signet non défini.</b>
5. La non répudiation .....	<b>Erreur ! Signet non défini.</b>
<b>V. LES MECANISMES DE SECURITE .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. La cryptographie .....	<b>Erreur ! Signet non défini.</b>
1.1 Chiffrement symétrique .....	<b>Erreur ! Signet non défini.</b>
1.2 Chiffrement asymétrique .....	<b>Erreur ! Signet non défini.</b>
1.3 Signature numérique .....	<b>Erreur ! Signet non défini.</b>
2. L'authentification .....	<b>Erreur ! Signet non défini.</b>
3. Le contrôle d'accès .....	<b>Erreur ! Signet non défini.</b>
4. Sécurité de communication .....	<b>Erreur ! Signet non défini.</b>
<b>VI. QUELQUES OUTILS DE SECURITE.....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. Les firewalls .....	<b>Erreur ! Signet non défini.</b>
2. Les systèmes de détection d'intrusion .....	<b>Erreur ! Signet non défini.</b>
<b>VII. CONCLUSION.....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>

### CHAPITRE 3 : LES SYSTEMES DE DETECTION D'INTRUSIONS

<b>I. INTRODUCTION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>II. DEFINITIONS.....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. L'intrusion .....	<b>Erreur ! Signet non défini.</b>
2. La détection d'intrusion .....	<b>Erreur ! Signet non défini.</b>
3. Système de détection d'intrusion .....	<b>Erreur ! Signet non défini.</b>

<b>III. IDS : BREF HISTORIQUE .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>IV. LES COMPOSANTS D'UN IDS .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>V. LES CARACTERISTIQUES SOUHAITEES D'UN IDS .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>VI. LA CLASSIFICATION DES IDS .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. Méthode d'analyse .....	<b>Erreur ! Signet non défini.</b>
1.1 Approche comportementale .....	<b>Erreur ! Signet non défini.</b>
a) Méthodes statistiques .....	<b>Erreur ! Signet non défini.</b>
b) Systèmes experts .....	<b>Erreur ! Signet non défini.</b>
c) Réseaux de neurones .....	<b>Erreur ! Signet non défini.</b>
1.2 Approche par scénarios .....	<b>Erreur ! Signet non défini.</b>
a) les systèmes experts .....	<b>Erreur ! Signet non défini.</b>
b) Pattern Matching .....	<b>Erreur ! Signet non défini.</b>
2. Source de données .....	<b>Erreur ! Signet non défini.</b>
2.1 La détection d'intrusion basée sur un hôte (HIDS) .....	<b>Erreur ! Signet non défini.</b>
2.2 La détection d'intrusion réseau (NIDS) .....	<b>Erreur ! Signet non défini.</b>
3. Réaction après détection .....	<b>Erreur ! Signet non défini.</b>
4. Fréquence d'utilisation .....	<b>Erreur ! Signet non défini.</b>
<b>VII. FORCES ET LIMITATIONS DES IDS .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. Les forces des systèmes de détection d'intrusion .....	<b>Erreur ! Signet non défini.</b>
2. Les limitations des IDS .....	<b>Erreur ! Signet non défini.</b>
<b>VIII. UTILISATION DU RAISONNEMENT A BASE DE CAS POUR LA DETECTION D'INTRUSION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>IX. CONCLUSION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>

#### **CHAPITRE 4 : LA CONCEPTION DU CBRIDS**

<b>I. INTRODUCTION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>II. NOTATION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>III. ARCHITECTURE GLOBALE .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
<b>IV. ARCHITECTURE DETAILLEE .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
1. Gestion des paquets fragmentés .....	<b>Erreur ! Signet non défini.</b>
2. Fournisseur des paquets .....	<b>Erreur ! Signet non défini.</b>
3. Détection des attaques par signatures .....	<b>Erreur ! Signet non défini.</b>
3.1 La base des signatures d'attaques .....	<b>Erreur ! Signet non défini.</b>
3.1.1 Les types des signatures d'attaques .....	<b>Erreur ! Signet non défini.</b>
3.1.2 Les sous bases des signatures d'attaques .....	<b>Erreur ! Signet non défini.</b>
3.2 Le moteur de recherche et de similarité .....	<b>Erreur ! Signet non défini.</b>
4. Contrôleur de l'intégrité .....	<b>Erreur ! Signet non défini.</b>
5. Gestion des alertes .....	<b>Erreur ! Signet non défini.</b>
<b>V. CONCLUSION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>

#### **CHAPITRE 5 : IMPLEMENTATION DU CBRIDS**

<b>I. INTRODUCTION .....</b>	<b>ERREUR ! SIGNET NON DEFINI.</b>
------------------------------	------------------------------------

<b>II. ENVIRONNEMENT DE DEVELOPPEMENT</b> .....	ERREUR ! SIGNET NON DEFINI.
1. Choix du langage de programmation .....	Erreur ! Signet non défini.
2. La capture des paquets.....	Erreur ! Signet non défini.
<b>III. PRESENTATION DU CBRIDS</b> .....	ERREUR ! SIGNET NON DEFINI.
1. Description de l'interface.....	Erreur ! Signet non défini.
1.1 Gestion de la base des signatures.....	Erreur ! Signet non défini.
1.2 La configuration .....	Erreur ! Signet non défini.
1.3 La Visualisation des alertes .....	Erreur ! Signet non défini.
2. Test du CbrIDS.....	Erreur ! Signet non défini.
<b>IV. CONCLUSION</b> .....	ERREUR ! SIGNET NON DEFINI.