**PFE :** A Machine Learning-Based Intrusion Detection System in Cloud-IoT for Healthcare Applications

Acknowledgments

Abstract

Résumé

ملخص

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations and Acronyms

Chapitre 1 General Introduction

1.1 Context/Motivation

1.2 Problem statement/Limitations (vulnérabilités, malwares, intrusions (attaques) dans un système healthcare ,)

1.3 Objectives/Purpose and goals (protection du système (applications healthcare), …)

1.4 Thesis Organisation/Plan Of The Thesis (structure du manuscrit)

Part I Background

Chapitre 2 : Healthcare system/applications (Smart healthcare/Internet of Medical Things + Security in healthcare/smart healthcare/Internet of Medical Things)

Chapitre 3 : Anomaly detection (IDS in healthcare/smart health)

Chapitre 4 : Machine Learning (ML)/Artificial Intelligence (AI)

Chapitre 5 : Project Management

Part II Our Contribution

Chapitre 6 : Building the Machine Learning Model

* 1. System (Solution) design/Model Topology
     1. Global Architecture
     2. Diagrams (Use case, Component, Deployment, Classe, Sequence, Activity,…)
  2. Technologies/Development Tools
     1. Artificial Intelligence Technologies

6.2.1.1 Environment

Anaconda

Python

6.2.1.2 Libraries

Jupyter notebook, Scikit-Learn, NumPy, Pandas, Matplotlib, Seaborn, ..

6.2.2 Web Application/Platform

6.2.2.1 Flask

6.3 Data-Set (NSL-KDD : Train+Test)

6.3.1 Description of Dataset

6.3.2 Description of Dataset features

6.3.3 Default classes

6.4 Data Pre-processing

6.4.1 Loading Datasets (Train+Test)

6.4.2 Overview of the data-set (Shape : columns+lignes)

6.4.3 Add header (feature columns)

6.4.4 Delete/drop the last column

6.4.5 Binary classification (Normal=0, Attaque=1)

6.4.6 Data tranformation (encoding)

1-N Encoding (Protoco\_type, Service, Flag, Label/Class) ⇒ Train+Test

6.4.7 Data normalisation (scaling)

MinMaxScaler

6.4.8 Checking for missing values (null/empty)

6.4.9 Unbalanced dataset

6.4.10 Outliers

6.4.10.1 Detect outliers

6.4.10.2 Handle outliers (Trimming/Capping)

6.5 Features selection

Embedded methods (Decision Tree/Random Forest)

Wrapper methods (RFE)

Filter methods (Correlation, …)

Hybride method (RF+RFE)

Why Random Forest/RFE?

6.5.1 Hyperparameter Tuninig

RF :Best *n\_estimator* Best *Max\_depth* + Best *Max\_leaf\_nodes* ⇒ Tree pruning

* + **Chosen method**

6.6 Building the model/Model Training

Algorithmes : LR, DT, RF, SVM, NB, …

Hyperparameter Tuninig :

DT : Best Best *Max\_depth* + Best *Max\_leaf\_nodes* ⇒ Tree pruning

Image representation (DT : graphviz + tree.dot)

* + **Chosen model**

6.7 Model Performance Evaluation

6.7.1 Confusion Matrix (TP/FP/TN/FN)

6.7.2 Accuracy

6.7.3 Precision

6.7.4 Recall/Sensitivity

6.7.5 Specificity

6.7.6 F\_measure (F1\_score)

6.7.7 False alarme

(Execution Time)

6.8 Improvements

+ Normalisation

+ Outliers

+ Features selection

+ Cross validation (10-fold cross-validation)

Chapitre 7 : Conclusion and Perspectives/Future Works

7.1 Conclusion

7.2 Perspectives/Future works

Bibliography (récente)

**Master :** A Survey on Machine Learning-Based Intrusion Detection Methods/Approaches

Comparative Study of Machine Learning-Based Intrusion Detection Methods/Approaches

Acknowledgments

Abstract

Résumé

ملخص

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Chapitre 1 : General Introduction

1.1 Context/Motivation

1.2 Thesis Organisation/Plan Of The Thesis (structure du manuscrit)

Part I Background

Chapitre 2 : Anomaly detection

Chapitre 3 : Intrusion Detection System (IDS+NIDS+Datasets : KDD CUP 99+NSL-KDD, …)

Chapitre 4 : Machine Learning (ML)/Artificial Intelligence (AI)

Part II State of the art

Chapitre 5 : Machine Learning-Based Intrusion Detection System Approaches Comparative Study Between The Related Works

Literature Review

Comparison Of The Solutions/Summary

Chapitre 6 : General Conclusion

Bibliography (récente)