République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي و البحث العلمي
Ecole Supérieure en Informatique
08-Mai-1945
المدرسة العليا للاعلام الالي سيدي بلعباس

MEMOIRE

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

Filière : **Informatique**

Spécialité: Ingénierie des Systèmes Informatiques (ISI)

THEME

Detection of Cyber Attacks in Iot systems

Présenté par:

Delfi Aya

Soutenu le: 06/07/2023 ..., 2023, Devant le jury composé de:

Dr. **Amina SOUYAH** :	ESI	- Supervisor
Dr. **Yasmine Harbi**	Univ-Setif	- Co-supervisor
Dr. **Bendaoued Faissel** :	ESI	- Président
Dr. **Baba Ahmed Manel** :	ESI	- Examinateur

Année Universitaire: 2022 / 2023

Dedications

In loving memory of **My dear father**, who is not with us today . Your unwavering love, guidance, and support continue to inspire me every day. This work is dedicated to you, as a tribute to the lasting impact you have had on my life.

To **My family My mother , My sister, my brothers Sami and Salah , My niece Ritel** , who has been my source of strength and encouragement throughout this journey. Your belief in me and your constant support have been invaluable. This accomplishment is as much yours as it is mine.

To **My dearest friends : Abir , Aya , Dacine , kawther , Kenza**, who have stood by my side through thick and thin. Your unwavering friendship and unwavering support have been a constant source of joy and inspiration. Thank you for always being there for me.

This dedication is a token of my deepest appreciation and gratitude to all of you. Your love, encouragement, and presence have made this journey worthwhile.

Acknowledgement

We want to start by saying a big thank you to **Allah** for helping us and giving us the patience and motivation to finish this work. We are grateful for His guidance, support, and blessings that have been with us every step of the way.

We would like to express our heartfelt gratitude to all those who have contributed to the completion of this thesis.

First and foremost, we extend our deepest appreciation to our **supervisor Dr. Amina Souyah** for their valuable guidance, mentorship, and continuous support throughout the research process. Their expertise, insightful feedback, and encouragement have been instrumental in shaping this thesis.

We are also thankful to all **the professors and all the staff of the ESI-SBA** for their knowledge-sharing and for providing us with a conducive learning environment. Their dedication to education and research has been a source of inspiration.

Abstract

In order to meet the pressing need for effective security solutions, this research examines the confluence of computer security, automatic learning (ML), deep learning (DL), and IoT systems. The study deepened fundamental computer security principles and revealed the significance, dangers, and various forms of cyberthreats. She gives a comprehensive overview of the areas of automatic and deep learning while highlighting the different learning styles and model-building processes.

She also looks at IoT systems, their architectures, communication protocols, and associated risks, as well as the significance of automatic learning in IoT cybersecurity. The study is supported by five approaches that were developed using various characteristic selection techniques and contrasted in terms of their performances, precision, score F1, speed, etc. With the right ML and DL approaches, this research offers invaluable perspectives for enhancing the security of IoT systems.

In contrast to solutions that rely solely on machine learning or deep learning, we propose a hybrid solution that combines the strengths of two models: decision trees and LSTM whitch gives a good results. this solution applied on a dataset of mqtt protocols

---

key-words : Cyber-attacks, threats , IoT, deep learning, , network traffic, detection system .

Résumé

Cette étude examine comment la Cyber security, l'apprentissage automatique (ML), l'apprentissage profond (DL) et les systèmes IoT peuvent être combinés pour répondre à la demande urgente de solutions de sécurité efficaces. Les concepts fondamentaux de la sécurité informatique sont abordés dans la recherche, qui met en évidence l'importance, les menaces et les différents types de cybermenaces. En mettant l'accent sur les types d'apprentissage et les étapes de construction des modèles, elle présente une vue d'ensemble des domaines de l'apprentissage automatique et de l'apprentissage profond.

Elle examine également les systèmes IoT, leurs architectures, les protocoles de communication et les risques associés, ainsi que l'importance de l'apprentissage automatique dans la cybersécurité IoT. Cinq approches développées à l'aide de différentes méthodes de sélection de caractéristiques, comparées en termes de performances, de précision, de score F1, de temps et d'autres facteurs, soutiennent l'étude. En choisissant les méthodes ML et DL appropriées, cette recherche offre des perspectives utiles pour renforcer la sécurité des systèmes IoT.

Contrairement aux solutions qui reposent uniquement sur le machine learning ou le deep learning, nous proposons une solution hybride qui combine les points forts de deux modèles : les arbres de décision et le LSTM qui donne de bons résultats. cette solution appliquée sur un jeu de données de protocoles mqtt.

Mots-clés : Cyber-attaques, Dispositifs IoT, Apprentissage Automatique, Apprentissage Profond, Analyse du Trafic Réseau, Système de Détection.

ملخص

من أجل تلبية الطلب الملح على حلول أمنية فعالة، تقوم هذه الأطروحة بدراسة التقارب بين أمن المعلومات، وتعلم الآلة ، وتعلم العمق ، وأنظمة الإنترنت من الأشياء .

تقوم هذه الدراسة بالبحث بعمق في مفاهيم الأمن السيبراني، مسلطة الضوء على أهميته وتهديداته ومختلف أنواع التهديدات السيبرانية. توفر الدراسة نظرة عامة على مجالات تعلم الآلة وتعلم العمق، مع التركيز على أنواعها (تعلم مشرف، تعلم غير مشرف، تعلم بالتعزيز) وخطوات بناء النماذج. وتستعرض الدراسة أنظمة أنترنت الاشياء وهياكلها وبروتوكولات الاتصال والمخاطر المرتبطة بها، مع التأكيد أيضًا على أهمية تعلم الآلة في أمن انترنت الاشياء. ويتم دعم الدراسة بخمسة استراتيجيات تم تطويرها باستخدام طرق مختلفة لاختيار السمات، مع المقارنة بين هذه الاستراتيجيات من حيث الأداء والدقة ونسبة والوقت، وما إلى ذلك.

على عكس الحلول التي تعتمد فقط على التعلم الآلي أو التعلم العميق ، نقترح حلاً هجينًا يجمع بين نقاط القوة في نموذجين: أشجار القرار و بصةp الذي يعطي نتائج جيدة. يتم تطبيق هذا الحل على مجموعة بيانات من بروتوكولات مقتت .

الكلمات المفتاحية: الهجمات السيبرانية، أجهزة انترنت الاشياء، التعلم الآلي، التعلم العميق، تحليل حركة المرور عبر الشبكة، نظام كشف.

acronyms

DOS	*Denial of service*
SQL	*Structured Query Language*
CIA	*Confidentiality, Integrity, Availability*
ML	*Machine learning*
DL	*Deep Learning*
KNN	*K-nearest neighbo*
NB	*Naive Bays*
SVM	*Suport vector machine*
DT	*Decision tree*
RF	*Random Forest*
NLP	*Natural Language Processing*
MLP	*Multilayer Perception*
CNN	*Convolutional Neural Network*
Rnn	*Recurrent Neural Networks*
LSTM	*Long Short-Term Memor*
IoT	*Internet of Things*
SVC	*Support Vector Classifier*
DNN	*Deep neural network*
MQTT	*Message Queuing Telemetry Transport*