الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للاعلام الالي -8 ماي 1945- بسيدي بلعباس
École Supérieure en Informatique
-8 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **Engineering Degree**
Field : **Computer Science**
Specialty : **Computer Systems Engineering**

Theme

AI-Powered Darknet Detection for Cyber Threat Hunting

Presented by :
Nedjaa Ines

Defending on : **21 September 2025**
In front of the jury composed of

Dr. SOUYAH Amina	|	President
Dr. KHALDI Miloud	|	Supervisor
Dr. BENDELLA Mohammed Salih	|	Examinator

Academic Year : 2025-2026

Abstract

The darknet has emerged as a covert environment for illicit activities, enabling adversaries to distribute malware, conduct illegal trade, and coordinate cyberattacks beyond the reach of traditional monitoring systems. Its encrypted and obfuscated traffic presents serious challenges for organizations, creating blind spots that hinder proactive defense strategies such as cyber threat hunting. Addressing this gap requires intelligent detection frameworks capable of analyzing network flows in real time and accurately identifying darknet-related anomalies.

This research introduces an AI-driven darknet traffic detection framework that integrates machine learning, deep learning, and meta-learning to support cyber threat hunting operations. The framework is trained and evaluated on the CICDarknet2020 dataset, which provides a comprehensive collection of darknet and non-darknet traffic. For traffic type classification, we employ machine learning models including K-Nearest Neighbors, Decision Tree, Random Forest, XGBoost, and Logistic Regression, alongside deep learning architectures such as LSTM and CNN. To enhance accuracy and efficiency, feature selection is performed using Mutual Information, Recursive Feature Elimination, and Random Forest-based selection, while hyperparameter optimization is conducted with HalvingRandomSearchCV. For application type classification, the same set of machine learning and deep learning models, feature selection strategies, and hyperparameter optimization techniques are applied. In addition, a meta-learning approach is implemented to dynamically leverage predictions from base learners, ensuring optimal model selection for each instance.

Experimental results demonstrate that Random Forest achieves the highest accuracy for traffic type classification, while the meta-learning framework significantly improves application type detection over individual ML/DL models. Furthermore, real-time evaluation using live network traffic confirms the system's practicality and robustness, proving its effectiveness in operational environments.

This research delivers an efficient, accurate, and real-time darknet detection solution that combines advanced AI techniques with optimized feature selection to empower cyber threat hunters, reduce attacker dwell time, and strengthen organizational resilience against evolving cyber threats.

Keywords : Cybersecurity, Darknet Detection, Machine Learning, Deep Learning, Meta-Learning, Feature Selection, Hyperparameter Optimization, Threat Hunting.

Résumé

Le darknet s'est imposé comme un environnement clandestin facilitant les activités illicites, permettant à des acteurs malveillants de distribuer des logiciels malveillants, de mener des transactions illégales et de coordonner des cyberattaques en dehors de la portée des systèmes de surveillance traditionnels. Son trafic chiffré et obscurci présente des défis majeurs pour les organisations, créant des angles morts qui entravent les stratégies de défense proactive telles que la chasse aux cybermenaces. Combler cette lacune nécessite des systèmes de détection intelligents capables d'analyser les flux réseau en temps réel et d'identifier avec précision les anomalies liées au darknet.

Cette recherche propose un système de détection du trafic darknet piloté par l'intelligence artificielle, qui intègre l'apprentissage automatique, l'apprentissage profond et le méta-apprentissage pour soutenir les opérations de chasse aux menaces. Le système est entraîné et évalué sur le jeu de données CICDarknet2020, qui offre une collection complète de trafic darknet et non-darknet. Pour la classification du type de trafic, nous utilisons des modèles d'apprentissage automatique (K-Nearest Neighbors, Arbre de Décision, Random Forest, XGBoost, et Régression Logistique) ainsi que des architectures d'apprentissage profond (LSTM et CNN). Pour améliorer la précision et l'efficacité, une sélection des caractéristiques est effectuée à l'aide de l'Information Mutuelle, l'Élimination Récursive des Caractéristiques (RFE) et une sélection basée sur Random Forest, tandis que l'optimisation des hyperparamètres est réalisée avec HalvingRandomSearchCV. La même méthodologie est appliquée pour la classification du type d'application. De plus, une approche de méta-apprentissage est mise en œuvre pour exploiter dynamiquement les prédictions des modèles de base, garantissant une sélection optimale du modèle pour chaque instance.

Les résultats expérimentaux démontrent que l'algorithme Random Forest obtient la meilleure précision pour la classification du type de trafic, tandis que le cadre de méta-apprentissage améliore significativement la détection du type d'application par rapport aux modèles individuels. De plus, une évaluation en temps réel utilisant du trafic réseau live confirme la praticité et la robustesse du système, prouvant son efficacité en environnement opérationnel.

Cette recherche offre une solution de détection darknet efficace, précise et fonctionnant en temps réel. Elle combine des techniques avancées d'IA avec une sélection optimisée des caractéristiques pour renforcer les capacités des chasseurs de menaces, réduire le temps d'infiltration des attaquants et améliorer la résilience des organisations face aux cybermenaces en évolution.

Mots-clés : Cybersécurité, Détection du Darknet, Apprentissage Automatique, Apprentissage Profond, Méta-Apprentissage, Sélection de Caractéristiques, Optimisation des Hyperparamètres, Chasse aux Menaces.