

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science 8 Mai 1945 - Sidi Bel Abbès



Master's Thesis

To obtain the diploma of Master's Degree

Field of Study: **Computer Science**

Specialization: **Artificial Intelligence and data science (IASD)**

Theme

**Comparative study of network data analysis platforms and
performance evaluation of intrusion detection based on
artificial intelligence (AI) techniques**

Presented by : **Abdelillah Serghine**

Defended on: **July 1, 2026**

In front of the jury composed of

Dr. Khaldi Miloud	ESI-SBA, Algeria	President of the Jury
Dr. Lahlou Laaziz	ÉTS, Canada	Thesis Supervisor
Pr. Benslimane Sidi Mohammed	ESI-SBA, Algeria	Co-Supervisor
Pr. Kara Nadjia	ÉTS, Canada	Co-Supervisor
Dr. Souyah Amina	ESI-SBA, Algeria	Examiner

Academic Year: 2025/2026

Abstract

Intrusion Detection Systems (IDS) are essential components for securing modern computer networks against increasingly sophisticated cyberattacks. With the rapid evolution of cloud-native infrastructures and distributed computing environments, traditional rule-based detection methods have become insufficient to address current cybersecurity challenges.

This thesis presents a state of the art of recent advances in network intrusion detection systems, focusing on feature extraction tools and artificial intelligence-based approaches. It explores the main stages of IDS pipelines, including network traffic analysis, feature extraction, data preprocessing, data augmentation and machine learning-based classification.

The thesis analyzes recent approaches addressing class imbalance in intrusion detection datasets, with particular focus on generative techniques for synthetic data generation.

Furthermore, it reviews machine learning and deep learning models also Transformer-based architectures commonly applied in IDS. The strengths and limitations of these approaches are discussed in the context of modern cybersecurity requirements.

Overall, this thesis provides a comprehensive overview of recent AI techniques used in intrusion detection systems, highlighting the evolution from traditional rule-based methods to data-driven, generative, and deep learning approaches in modern cybersecurity environments.

Keywords : Intrusion Detection System (IDS), Network Traffic Analysis, Machine Learning, Deep Learning, Generative Artificial Intelligence, Cybersecurity, Data Augmentation, Cybersecurity

Résumé

Les systèmes de détection d'intrusion (IDS) sont des composantes essentielles de la sécurisation des réseaux informatiques modernes contre les cyberattaques de plus en plus sophistiquées. Face à l'évolution rapide des infrastructures cloud-native et des environnements de calcul distribué, les méthodes de détection traditionnelles basées sur des règles sont devenues insuffisantes pour relever les défis actuels en matière de cybersécurité.

Cette mémoire présente un état de l'art des avancées récentes dans les systèmes de détection d'intrusion réseau, en mettant l'accent sur les outils d'extraction de caractéristiques et les approches basées sur l'intelligence artificielle. Elle explore les principales étapes des pipelines IDS, notamment l'analyse du trafic réseau, l'extraction de caractéristiques, le prétraitement des données, l'augmentation des données et la classification par apprentissage automatique.

La mémoire analyse les approches récentes permettant de traiter le déséquilibre des classes dans les ensembles de données de détection d'intrusion, en particulier les techniques génératives pour la génération de données synthétiques.

De plus, elle passe en revue les modèles d'apprentissage automatique et d'apprentissage profond, ainsi que les architectures basées sur les Transformers, couramment utilisées dans les IDS. Les forces et les limites de ces approches sont discutées dans le contexte des exigences actuelles en matière de cybersécurité.

Globalement, cette mémoire offre un aperçu complet des techniques d'IA récentes utilisées dans les systèmes de détection d'intrusion, en soulignant l'évolution des méthodes traditionnelles basées sur des règles vers des approches axées sur les données, génératives et d'apprentissage profond dans les environnements de cybersécurité modernes.

Mots-clés : Système de Détection d'Intrusion (IDS), Analyse du Trafic Réseau, Apprentissage Automatique, Apprentissage Profond, Intelligence Artificielle Générative, Cybersécurité, Augmentation de Données

الملخص

تُعدّ أنظمة كشف التسلل (IDS) مكونات أساسية لتأمين شبكات الحاسوب الحديثة ضد الهجمات الإلكترونية المتطورة باستمرار. ومع التطور السريع للبنى التحتية السحابية وبيئات الحوسبة الموزعة، لم تعد أساليب الكشف التقليدية القائمة على القواعد كافية لمواجهة تحديات الأمن السيبراني الحالية.

تقدم هذه الأطروحة عرضاً لأحدث التطورات في أنظمة كشف التسلل الشبكي، مع التركيز على أدوات استخلاص الميزات والأساليب القائمة على الذكاء الاصطناعي. وتستكشف المراحل الرئيسية لخطوط أنابيب أنظمة كشف التسلل، بما في ذلك تحليل حركة مرور الشبكة، واستخلاص الميزات، ومعالجة البيانات الأولية، وتوسيع البيانات، والتصنيف القائم على التعلم الآلي.

تحلل الأطروحة الأساليب الحديثة التي تعالج عدم توازن الفئات في مجموعات بيانات كشف التسلل، مع التركيز بشكل خاص على التقنيات التوليدية لإنشاء بيانات اصطناعية.

علاوة على ذلك، تستعرض الأطروحة نماذج التعلم الآلي والتعلم العميق، بالإضافة إلى البنى القائمة على المحولات (Transformer) الشائعة الاستخدام في أنظمة كشف التسلل. وتناقش الأطروحة نقاط القوة والقيود لهذه الأساليب في سياق متطلبات الأمن السيبراني الحديثة.

بشكل عام، تقدم هذه الأطروحة نظرة عامة شاملة على تقنيات الذكاء الاصطناعي الحديثة المستخدمة في أنظمة كشف التسلل، مع تسليط الضوء على التطور من الأساليب التقليدية القائمة على القواعد إلى الأساليب القائمة على البيانات والتوليدية والتعلم العميق في بيئات الأمن السيبراني الحديثة.

الكلمات المفتاحية : نظام كشف التسلل (IDS)، تحليل حركة مرور الشبكة، التعلم الآلي، التعلم العميق، الذكاء الاصطناعي التوليدي، الأمن السيبراني، زيادة البيانات