Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Monsieur AGALIT MOHAMED AMINE

Discipline : Sciences et Techniques d'Information et de Communication
Spécialité : Informatique

Sujet de la thèse

Vers une nouvelle génération des systèmes de détection d'intrusion et de prévention intelligents et distribués

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique"

Thèse présentée et soutenue **le samedi 30 novembre 2024 à 10h** à l'Ecole Nationale des Sciences Appliquées de Fès, devant le jury composé de :

NOM ET PRÉNOM	TITRE	ETABLISSEMENT	
Saad BENNANI DOSSE	PES	Ecole Nationale des Sciences Appliquées de Fès	Président
Moulay Driss EL OUADGHIRI	PES	Faculté des Sciences de Meknès	Rapporteur
Omar EL BANNAY	MCH	Ecole Nationale des Sciences Appliquées de Khouribga	Rapporteur
Said HRAOUI	MCH	Ecole Nationale des Sciences Appliquées de Fès	Rapporteur
Younes LAKHRISSI	MCH	Ecole Nationale des Sciences Appliquées de Fès	Examinateur
Kaouthar CHETIOUI	MCH	Ecole Nationale des Sciences Appliquées de Fès	Examinateur
Youness IDRISSI KHAMLICHI	PES	Ecole Nationale des Sciences Appliquées de Fès	Directeur de Thèse

Laboratoire de recherche : Systèmes Intelligents, Géo-ressources et Energies Renouvelables
Etablissement : Faculté des Sciences et Techniques de Fès

Résumé de la thèse

Avec la prolifération des réseaux informatiques et l'émergence de l'Internet des Objets (IoT), les infrastructures critiques sont de plus en plus exposées à des cyberattaques sophistiquées. Les systèmes de détection d'intrusion (IDS) traditionnels, basés sur des règles ou des signatures, montrent leurs limites face à ces menaces en constante évolution, notamment les attaques zero-day. Cette thèse explore l'utilisation de l'apprentissage profond pour optimiser la détection d'intrusions, en s'appuyant sur le dataset KDD Cup 99.

L'introduction présente les défis actuels de la cybersécurité et l'importance des IDS dans la protection des réseaux, soulignant les avantages potentiels de l'intégration de l'apprentissage profond pour améliorer la précision et la robustesse des IDS. Le développement d'un système hybride de prévention des intrusions pour les réseaux sans fil (WIPS) est présenté. Ce système combine des approches de détection par signature et par anomalie pour offrir une protection renforcée contre les menaces. L'architecture, les méthodes de détection et l'évaluation des performances du système hybride sont détaillées.

L'optimisation de la détection d'intrusion avec l'apprentissage profond est explorée à travers une méthodologie rigoureuse, incluant la préparation des données, le développement du modèle et les algorithmes d'apprentissage utilisés. Les résultats montrent une amélioration significative de la performance des IDS, avec une précision et une robustesse accrues. L'exploitation du deep learning distribué pour la détection d'intrusion est examinée, avec un modèle de détection d'intrusions distribué proposé et détaillé. Les performances du modèle, testées sur le dataset KDD Cup 99, démontrent une précision exceptionnelle et une capacité accrue à gérer divers types d'attaques.

Les résultats obtenus, avec des performances élevées en termes de précision (99,90%), de rappel (99,89%) et de spécificité (100%), valident l'application des réseaux neuronaux convolutifs et d'autres techniques avancées pour la cybersécurité. En plus d'améliorer la sécurité des réseaux, ce modèle peut être adapté à d'autres domaines nécessitant une détection précise et rapide des anomalies, tels que la surveillance des systèmes industriels, la détection de fraudes financières et la sécurisation des infrastructures critiques.

Mots clés : Sécurité informatique, Systèmes de Détection d'Intrusion, Apprentissage profond, Faux positifs, Faux négatifs, Deep Learning, Réseaux neuronaux convolutifs, KDD Cup 99, Cybersécurité.