# ***Rapport de projet***

## 3ème année

## Filière ingénierie informatique et réseaux

## ***Sous le thème :***

# APPROCHE DE L'APPRENTISSAGE PROFOND POUR UN SYSTEME INTELLIGENT DE DÉTECTION D'INTRUSION


***Réalisé par :***

Mohamed Yassine **Kninah**

Abdelhafid **Meskour**

Hmazaa **Bouataoun**

Adam **Hamami**

***Encadré par :***

**Madame** GHAZAL Ikram


***Année Universitaire :2023-2024***

# Dédicaces

Ce travail est dédié à tous ceux qui m'ont soutenu et inspiré tout au long de cette aventure académique.

À mes parents, pour leur amour inconditionnel et leur soutien sans faille, qui m'ont donné la force et le courage de persévérer.

À mes amis, pour leur encouragement constant et leurs précieux conseils, qui ont rendu cette expérience inoubliable.

À mon professeur, Madame Ghazal Ikram, pour son mentorat et sa patience, qui ont été essentiels à la réalisation de ce projet.

À toutes les personnes qui ont contribué, de près ou de loin, à l'aboutissement de ce travail.

Merci à vous tous. 🫶

# REMERCIMENTS

Il nous est agréable de nous acquitter d'une dette de reconnaissance envers tous ceux dont la contribution, au cours de ce projet, a favorisé son aboutissement.

Ainsi, nous tenons vivement à remercier notre professeur, Madame Ghazal Ikram, qui n'a ménagé aucun effort pour nous aider et nous orienter tout au long de notre projet.

Que le corps professoral et administratif de l'EMSI trouve ici l'expression de nos vifs remerciements.

# Abstract

Ce projet présente une étude sur l'utilisation de l'apprentissage profond pour développer un système intelligent de détection d'intrusion. Face à la complexité croissante des cyberattaques, les systèmes traditionnels de détection d'intrusion (IDS) montrent des limites en termes de précision et d'adaptabilité. Notre recherche vise à résoudre ces problèmes en utilisant des réseaux de neurones profonds (DNN) pour améliorer la détection.

Nous examinons les étapes de l'intrusion, telles que la reconnaissance et l'exploitation, et nous analysons les travaux existants sur les systèmes de détection d'intrusion réseau (NIDS) et hôte (HIDS). Notre approche intègre des techniques d'apprentissage automatique avec des modèles d'apprentissage profond dans un cadre évolutif.

# Résume

Ce projet explore l'utilisation de réseaux neuronaux profonds (DNN) pour améliorer les systèmes de détection d'intrusion (IDS), une composante cruciale de la cybersécurité. Les IDS actuels, basés sur des méthodes classiques d'apprentissage machine, rencontrent des difficultés face à la complexité et à la rapidité des cyberattaques modernes. L'adoption de DNN promet d'améliorer la capacité de détection et de classification des intrusions grâce à leur aptitude à analyser de vastes volumes de données et à s'adapter aux menaces évolutives.

L'objectif principal de ce rapport est de démontrer l'efficacité des DNN dans la détection d'intrusions en comparant leurs performances à celles des classificateurs d'apprentissage automatique traditionnels. Pour ce faire, nous avons évalué plusieurs algorithmes sur des ensembles de données publics tels que KDDCup 99, NSL-KDD, UNSW-NB15, Kyoto, WSN-DS et CICIDS 2017. De plus, nous visons à proposer une architecture hybride et évolutive, appelée scale-hybrid-IDS-AlertNet, capable de surveiller en temps réel le trafic réseau et les événements au niveau des hôtes pour alerter de manière proactive sur les cyberattaques potentielles.

Notre étude révèle que les DNN surpassent généralement les méthodes classiques d'apprentissage automatique en termes de précision et de robustesse dans la détection d'intrusions. Les résultats expérimentaux montrent des courbes ROC améliorées et une meilleure gestion des caractéristiques minimales. L'architecture scale-hybrid-IDS-AlertNet, combinant DNN et surveillance en temps réel, s'avère particulièrement efficace pour identifier les menaces contemporaines. Ce rapport ouvre des perspectives pour des recherches futures visant à intégrer des modules de surveillance supplémentaires et à optimiser l'entraînement de DNN sur des infrastructures distribuées.

## ***Tables des matiéres***

## ***Listes des figures***

# ***Introduction générale.***

L’introduction générale de ce rapport vise à détailler le contexte et les objectifs du projet. Les systèmes de détection d'intrusion (IDS) sont essentiels pour protéger les réseaux et les systèmes informatiques contre les cyberattaques. Les méthodes traditionnelles d'apprentissage automatique utilisées dans les IDS ont montré leurs limites face à la sophistication croissante des attaques. Ce projet explore l'utilisation de réseaux neuronaux profonds (DNN) pour améliorer la détection et la classification des intrusions. L'objectif principal est de démontrer que les DNN peuvent surpasser les méthodes classiques en termes de précision et de réactivité. En évaluant divers algorithmes sur des ensembles de données publics, nous visons à proposer une solution hybride et évolutive capable de surveiller en temps réel les réseaux et les hôtes pour fournir des alertes proactives contre les cyberattaques potentielles.

Le Chapitre 1 examine les défis et les avantages de l'utilisation des algorithmes d'apprentissage automatique pour les systèmes de détection d'intrusion, en s'appuyant sur plusieurs ensembles de données de référence.

Le Chapitre 2 décrit la conception, la sélection des hyperparamètres et les expérimentations réalisées avec le modèle de réseau de neurones profonds (DNN), montrant comment ce modèle améliore la détection des intrusions.

Le Chapitre 3 compare les performances des DNN avec celles des classificateurs traditionnels en utilisant des courbes ROC et d'autres métriques de performance pour divers ensembles de données.

Le Chapitre 4 met l'accent sur l'impact de la sélection des caractéristiques sur les performances de l'IDS, en détaillant les résultats obtenus avec des ensembles de caractéristiques minimales pour optimiser le système.

# *Chapitre 1 : Méthodes d'apprentissage automatique pour l'IDS*

## *1.1. Introduction*

Les systèmes de détection d'intrusion (IDS) jouent un rôle crucial dans la protection des réseaux et des systèmes informatiques contre les cyberattaques. Avec l'augmentation de la complexité et du volume des attaques, les méthodes traditionnelles de détection basées sur des signatures ou des heuristiques deviennent de moins en moins efficaces. C'est dans ce contexte que les méthodes d'apprentissage automatique (ML) offrent des perspectives prometteuses en permettant une analyse plus dynamique et adaptative des données de sécurité.

Ce chapitre explore les défis et les avantages associés à l'intégration des algorithmes d'apprentissage automatique dans les IDS. Nous examinerons comment ces méthodes peuvent améliorer la détection des intrusions en se basant sur plusieurs ensembles de données de référence. En particulier, nous discuterons des différentes approches ML, telles que les arbres de décision, les machines à vecteurs de support (SVM), et les réseaux de neurones, en mettant en évidence leurs performances et leurs limites dans divers scénarios de détection. Cette analyse servira de fondation pour la mise en place de systèmes IDS plus robustes et intelligents, capables de faire face aux menaces de plus en plus sophistiquées.

## 1.2. Défis de l'utilisation des méthodes d'apprentissage automatique pour l'IDS

L'utilisation des méthodes d'apprentissage automatique pour les systèmes de détection d'intrusion (IDS) présente plusieurs défis. Voici les principaux défis identifiés :

**Taux élevé de faux positifs :** Les modèles d'apprentissage automatique peuvent produire un nombre élevé de faux positifs, ce qui rend difficile la distinction entre les comportements normaux et les intrusions réelles. Cela peut entraîner une surcharge pour les administrateurs de sécurité, qui doivent examiner chaque alerte pour déterminer sa validité

**Généralisation des modèles :** Les modèles d'apprentissage automatique doivent être capables de généraliser à des environnements de réseau variés et à des types de trafic différents. Cependant, beaucoup de recherches utilisent des ensembles de données spécifiques et limités, ce qui limite la capacité du modèle à s'adapter à de nouveaux types de trafic et à des attaques inconnues

**Problèmes de jeux de données** : Les ensembles de données utilisés pour entraîner les modèles IDS présentent souvent des problèmes tels que des corruptions de données, une variété de trafic limitée, des incohérences, et des attaques obsolètes. Ces problèmes affectent la précision et l'efficacité des modèles d'apprentissage automatique pour la détection des intrusions

**Coût computationnel élevé :** Les modèles d'apprentissage profond, en particulier, nécessitent des ressources computationnelles importantes pour l'entraînement et la mise en œuvre. Cela inclut l'utilisation de matériel avancé comme les GPU, ce qui peut être coûteux et difficile à déployer dans des environnements à grande échelle

***Complexité des caractéristiques :*** *La sélection et l'extraction des caractéristiques pertinentes pour la détection des intrusions sont cruciales. Des ensembles de caractéristiques mal choisis peuvent entraîner une mauvaise classification des attaques et augmenter le temps de formation du modèle*

***Évolution des techniques d'attaque :*** *Les attaquants adaptent constamment leurs techniques pour contourner les systèmes de détection. Les modèles d'apprentissage automatique doivent être continuellement mis à jour et re-entraînés pour rester efficaces face à de nouvelles menaces et méthodes d'attaque.*

***Scalabilité et latence :*** *Les systèmes IDS doivent être capables de traiter de grandes quantités de données en temps réel. Cela nécessite des architectures distribuées et évolutives qui peuvent gérer le volume et la vitesse des données de réseau modernes sans introduire de latence excessive.*

*En conclusion, bien que les méthodes d'apprentissage automatique offrent des possibilités prometteuses pour améliorer la détection des intrusions, elles présentent également des défis significatifs qui doivent être surmontés pour assurer leur efficacité et leur fiabilité dans des environnements réels.*

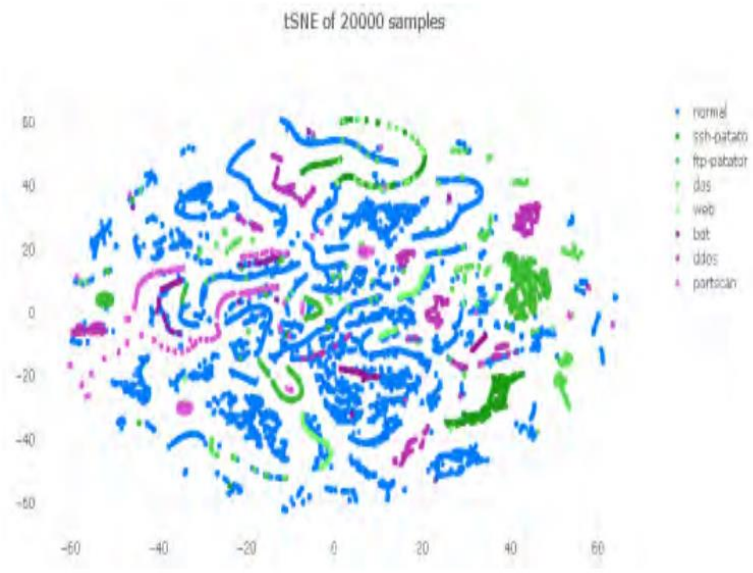


**FIGURE 3.** **t-SNE visualization of CICIDS 2017.**

## 1.3. Jeu de données de référence pour l'évaluation des IDS

Pour l'évaluation des systèmes de détection d'intrusion (IDS), plusieurs jeux de données de référence sont utilisés afin de mesurer l'efficacité des algorithmes de machine learning et de deep learning. Voici les jeux de données les plus couramment utilisés :

**KDDCup 99 :** Ce dataset est un des plus anciens et a été largement utilisé pour l'évaluation des IDS. Il contient des enregistrements de connexions réseau, classifiés en normal ou en différentes catégories d'attaques.

**NSL-KDD :** Une version améliorée du dataset KDDCup 99, créée pour pallier certains déséquilibres et redondances présents dans le dataset original. Ce dataset est divisé en jeux de données d'entraînement et de test, ce qui permet une évaluation plus équilibrée des modèles d'IDS.

**UNSW-NB15 :** Ce dataset a été développé pour surmonter les limitations des datasets précédents. Il comprend des activités normales et des comportements d'attaque capturés à l'aide de l'outil IXIA Perfect Storm. Ce dataset est composé de 100 GB de données, divisées en enregistrements de connexion pour l'entraînement et le test .

**Kyoto :** Basé sur les systèmes honeypot de l'université de Kyoto, ce dataset contient des logs réseau collectés sur une période d'un an. Il inclut 24 caractéristiques statistiques, dont 14 proviennent du dataset KDDCup 99.

**WSN-DS :** Conçu pour les réseaux de capteurs sans fil (WSN), ce dataset comprend des attaques de type 'DoS' comme Blackhole, Grayhole, Flooding, et Scheduling. Les données ont été collectées en utilisant le protocole LEACH et le simulateur de réseau NS-2 .

**CICIDS2017 :** Ce dataset représente des activités réseau réelles, incluant des trafics normaux et des attaques injectées sur plusieurs jours. Les attaques comprennent Brute Force, 'DoS', Heartbleed, et d'autres.

Ces jeux de données permettent de tester et de comparer différents modèles de détection d'intrusion en termes de précision, taux de faux positifs, taux de détection, et d'autres métriques de performance. Utiliser plusieurs jeux de données de référence est crucial pour évaluer la robustesse et la généralisabilité des systèmes de détection d'intrusion

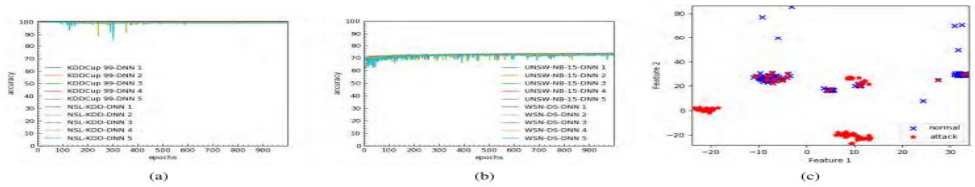

FIGURE 4. Train accuracy. (a) KDDCup 99 and NSL-KDD. (b) UNSW-NB-15 and WSN-DS. (c) Visualization of 100 connection records with their corresponding activation values of the last hidden layer neurons from Kyoto.

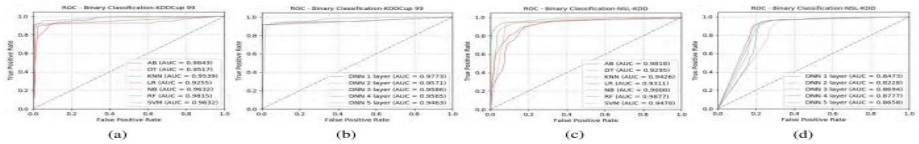

FIGURE 5. ROC curves of (a) KDDCup 99-using classical machine learning classifiers, (b) KDDCup 99-using DNNs, (c) NSL-KDD-using classical machine learning classifiers, (d) NSL-KDD-using DNNs.

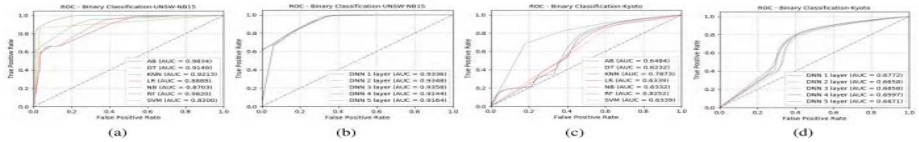

FIGURE 6. ROC curves of (a) UNSW-NB 15-using classical machine learning classifiers, (b) UNSW-NB 15-using DNNs, (c) Kyoto-using classical machine learning classifiers, (d) Kyoto-using DNNs.

## 1.4. Analyse comparative des algorithmes d'apprentissage automatique09O

L'article "Deep Learning Approach for Intelligent Intrusion Detection System" de Vinayakumar et al. (2019) offre une analyse comparative des performances des algorithmes d'apprentissage automatique classiques et des réseaux de neurones profonds (DNN) pour la détection d'intrusions. Les algorithmes classiques évalués comprennent l'arbre de décision (DT), le boosting adaptatif (AB), la forêt aléatoire (RF), la régression logistique (LR), le Naïve Bayes (NB), le K-plus proches voisins (KNN), et les machines à vecteurs de support avec noyau radial (SVM-rbf). Pour les algorithmes profonds, différents modèles de réseaux de neurones profonds (DNN) avec des topologies de 1 à 5 couches ont été testés. Les auteurs ont utilisé plusieurs ensembles de données de détection d'intrusion, dont KDDCup 99, NSL-KDD, UNSW-NB15, WSN-DS, et CICIDS 2017, afin de comparer les performances de ces algorithmes.

Les résultats montrent que les algorithmes DT, AB et RF ont des performances supérieures en termes de précision par rapport aux autres algorithmes classiques, mais que les DNN surpassent tous les algorithmes classiques, notamment dans les tâches de classification binaire et multi-classes. Les DNN démontrent une meilleure capacité d'apprentissage des caractéristiques complexes des données d'intrusion, affichant des taux de vrais positifs (TPR) plus élevés et des taux de faux positifs (FPR) plus bas.

Les réseaux DNN avec 3 couches, en particulier, offrent un bon équilibre entre la performance de détection et la complexité computationnelle. Les algorithmes AB et SVM-rbf, quant à eux, montrent des faiblesses dans les tâches de classification multi-classes par rapport aux autres algorithmes classiques et aux DNN.

En conclusion, les réseaux de neurones profonds (DNN) surpassent les algorithmes d'apprentissage automatique classiques dans la détection d'intrusions, grâce à leur efficacité pour apprendre des représentations complexes et généraliser sur divers ensembles de données, tout en maintenant des taux de faux positifs plus bas. Les auteurs ont optimisé les DNN en utilisant différentes topologies et des méthodes de sélection d'hyperparamètres, démontrant que des architectures plus complexes nécessitent plus d'époques pour atteindre une précision optimale. Pour une analyse détaillée des résultats, les tableaux et figures du document original présentent des visualisations complètes des courbes ROC et des taux de précision et de rappel.

## 1.5. Conclusion

En conclusion l'intégration des algorithmes d'apprentissage automatique dans les systèmes de détection d'intrusion (IDS) montre des résultats prometteurs pour améliorer la sécurité des réseaux et des systèmes informatiques. L'analyse comparative de Vinayakumar et al. (2019) révèle que les réseaux de neurones profonds (DNN) surpassent les algorithmes classiques, tels que les arbres de décision et les forêts aléatoires, en termes de précision et de capacité à détecter les intrusions.

Les DNN sont particulièrement efficaces pour apprendre des représentations complexes des données d'intrusion, offrant de meilleures performances globales avec des taux de faux positifs plus bas. Cependant, leur mise en œuvre présente des défis, notamment en termes de coûts computationnels et de généralisation des modèles. Pour maximiser les avantages des DNN dans les IDS, il est essentiel d'optimiser les architectures, d'utiliser des jeux de données variés et de développer des méthodes pour réduire les faux positifs.

# ***Chapitre 2: Modèle de Réseau de Neurones Profonds (DNN) proposé***

## 2.1 Introduction.

Les réseaux de neurones profonds (DNN) représentent une avancée significative dans le domaine de la détection d'intrusions, grâce à leur capacité à apprendre des représentations complexes et à généraliser à partir de données variées. Ce chapitre présente le modèle de DNN proposé pour améliorer l'efficacité et la précision des systèmes de détection d'intrusion (IDS).

Le modèle proposé utilise plusieurs couches de neurones pour extraire et apprendre des caractéristiques à différents niveaux d'abstraction, permettant ainsi une meilleure détection des anomalies et des comportements malveillants dans les réseaux. Nous décrirons ici la structure du DNN, les méthodes de sélection et d'extraction des caractéristiques, ainsi que les techniques d'entraînement utilisées pour optimiser les performances du modèle.

En explorant ces aspects, nous démontrerons comment le modèle de DNN proposé peut surpasser les méthodes traditionnelles de détection d'intrusion et offrir une solution plus robuste et adaptable face aux cybermenaces de plus en plus sophistiquées.

## 2.2. Sélection des hyperparamètres.

La sélection des hyperparamètres est une étape cruciale dans la conception et l'entraînement des réseaux de neurones profonds (DNN). Les hyperparamètres déterminent la structure et le comportement du modèle, influençant directement sa performance et sa capacité de généralisation. Voici les principaux hyperparamètres à considérer pour le modèle de DNN proposé pour la détection d'intrusion :

### 1 Nombre de couches et de neurones par couche

Le nombre de couches et de neurones par couche est fondamental pour définir la complexité du modèle. Une profondeur accrue (plus de couches) permet au DNN de capturer des caractéristiques plus abstraites des données, tandis que la largeur (plus de neurones par couche) augmente la capacité de stockage de l'information. Toutefois, des modèles trop complexes peuvent entraîner un surapprentissage, où le modèle s'adapte trop aux données d'entraînement et performe mal sur les données non vues.

### 2 Taux d'apprentissage

Le taux d'apprentissage détermine la vitesse à laquelle le modèle ajuste ses poids pendant l'entraînement. Un taux d'apprentissage élevé peut accélérer la convergence mais risque de dépasser le minimum global, tandis qu'un taux trop bas peut ralentir l'entraînement et tomber dans un minimum local. Il est courant d'utiliser des techniques de réglage adaptatif du taux d'apprentissage, telles que l'Adam, pour équilibrer ces défis.

### 3 Fonction de perte

La fonction de perte mesure l'erreur entre les prédictions du modèle et les valeurs réelles. Pour la détection d'intrusion, les fonctions de perte couramment utilisées incluent la cross-entropie pour les classifications binaires et multi-classes. La sélection de la fonction de perte appropriée est essentielle pour guider efficacement l'entraînement du modèle.

### 4 Méthode de régularisation

La régularisation aide à prévenir le surapprentissage en pénalisant les poids excessivement grands. Les techniques de régularisation courantes incluent la régularisation L2 (ridge) et la régularisation L1 (lasso). Le dropout est une autre technique populaire qui désactive aléatoirement des neurones pendant l'entraînement pour encourager le modèle à généraliser mieux.

### 5 Taille de batch

La taille de batch détermine le nombre d'échantillons d'entraînement utilisés pour mettre à jour les poids du modèle en une seule fois. Des tailles de batch plus petites peuvent offrir une meilleure généralisation mais augmentent le temps d'entraînement. Des tailles de batch plus grandes accélèrent l'entraînement mais risquent de converger vers des minima de moindre qualité.

## 2.3 Topologies et paramètres de réseau optimaux.

Les topologies de réseau optimales pour entraîner un modèle IDS avec le jeu de données KDDCup 99 sont les suivantes :

1. **DNN 1 couche**
2. **DNN 2 couches**
3. **DNN 3 couches**
4. **DNN 4 couches**
5. **DNN 5 couches**

Pour toutes ces topologies de réseau, 3 essais d'expérimentation ont été réalisés pour 300 époques chacun. Il a été observé que la plupart des architectures d'apprentissage profond ont appris les modèles de catégories normales des données d'entrée pour moins de 400 époques, tandis que le nombre d'époques nécessaires pour découvrir la catégorie d'attaque fluctuait. Les réseaux DNN à 1 couche et à 2 couches ont complètement échoué à apprendre les catégories d'attaque "R2L" et "U2R". La performance des catégories d'attaque "DoS" et "Probe" était bonne avec les DNN à 3 couches par rapport aux DNN à 2 couches et à 1 couche. Les architectures de réseaux complexes ont nécessité un grand nombre d'époques pour atteindre une précision optimale. La performance des DNN à 5 couches pour les différentes catégories d'attaque et la catégorie normale était bonne par rapport aux autres topologies de réseaux DNN. En tenant compte de tous ces facteurs, il a été décidé d'utiliser un réseau DNN à 5 couches pour le reste du processus d'expérimentation.

## 2.4 Expérimentations et résultats

Les résultats des expérimentations ont montré que les réseaux de neurones profonds (DNN) ont surpassé les algorithmes classiques d'apprentissage machine en termes de précision, souvent avec une marge importante, à la fois en classification binaire et en classification multi-classe. Les DNN ont obtenu un taux de détection des attaques plus élevé et un taux de faux positifs plus faible par rapport aux autres algorithmes classiques. En outre, les résultats ont montré que la représentation textuelle en N-gram et l'incorporation Keras ont bien fonctionné par rapport à la méthode de représentation tf-idf. Les expériences ont montré que l'utilisation de l'incorporation Keras a donné de meilleurs résultats que la représentation en N-gram.

## 2.5 Conclusion

La sélection minutieuse des hyperparamètres, la détermination des topologies de réseau optimales et les expérimentations approfondies ont démontré que les modèles de détection d'intrusion basés sur les réseaux de neurones profonds (DNN) surpassent les approches classiques en termes de précision de détection des attaques et de réduction des faux positifs. En ajustant des facteurs tels que le nombre de couches et de neurones, le taux d'apprentissage, la fonction de perte et la méthode de régularisation, les DNN ont été capables de capturer efficacement les caractéristiques complexes des données, tout en évitant le surapprentissage. Les résultats ont souligné l'efficacité des architectures plus complexes, comme les DNN à 5 couches, et l'importance des représentations textuelles telles que les incrustations Keras. Ces conclusions mettent en lumière le potentiel des DNN pour renforcer la sécurité des systèmes informatiques en identifiant de manière fiable les comportements malveillants

# ***Chapitre 3: Évaluation des Performances***

## *3.1. Introduction*

L'évaluation des performances des systèmes de détection d'intrusion est essentielle pour mesurer l'efficacité des techniques utilisées dans la détection et la classification des cyberattaques. Ce chapitre se concentre sur l'évaluation des performances des réseaux de neurones profonds (DNN) par rapport aux algorithmes classiques d'apprentissage machine dans le domaine de la détection d'intrusion. En utilisant divers ensembles de données de détection d'intrusion réseau et au niveau de l'hôte, les expériences ont été menées pour comparer la précision, le taux de détection des attaques et le taux de faux positifs entre les deux approches. Les courbes ROC ont été utilisées comme métrique de comparaison pour évaluer la capacité des modèles à distinguer les attaques des activités normales. Les résultats détaillés de ces expérimentations fournissent un aperçu des performances des DNN par rapport aux méthodes traditionnelles, mettant en lumière les avantages de l'utilisation de l'apprentissage profond dans la détection proactive des cyberattaques.

## 3.2. Comparaison des performances des DNN avec les classificateurs classiques

Les performances des réseaux de neurones profonds (DNN) ont été comparées à celles des classificateurs classiques d'apprentissage machine dans le domaine de la détection d'intrusion. Les résultats ont montré que les DNN ont surpassé les algorithmes classiques en termes de précision, de taux de détection des attaques et de taux de faux positifs. Les courbes ROC ont été utilisées pour évaluer la capacité des modèles à distinguer les attaques des activités normales, et les DNN ont généralement obtenu des performances supérieures. Cette comparaison démontre l'efficacité des approches basées sur les réseaux de neurones profonds dans la détection proactive des cyberattaques, mettant en évidence leur potentiel pour améliorer la sécurité des systèmes informatiques.

## 3.2. Analyse des courbes ROC

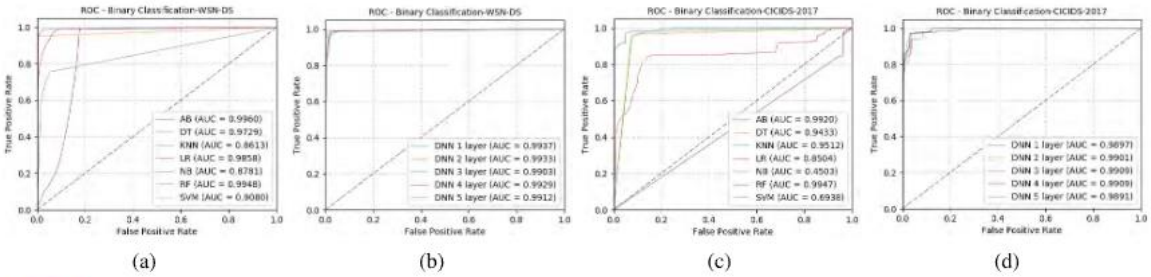


**FIGURE 7.** ROC curves of (a) WSN-DS-using classical machine learning classifiers, (b) WSN-DS-using DNNs, (c) CICIDS 2017-using classical machine learning classifiers, (d) CICIDS 2017-using DNNs.

Les courbes ROC (Receiver Operating Characteristic) ont été utilisées pour évaluer les performances des réseaux de neurones profonds (DNN) par rapport aux classificateurs classiques dans la détection d'intrusion. Les courbes ROC permettent de visualiser le trade-off entre le taux de vrais positifs et le taux de faux positifs à différents seuils de classification. En analysant les courbes ROC des DNN et des classificateurs classiques, il est possible de comparer leur capacité à distinguer les attaques des activités normales. Les résultats montrent généralement que les DNN ont obtenu des courbes ROC plus proches du coin supérieur gauche, indiquant une meilleure performance en termes de sensibilité et de spécificité par rapport aux classificateurs classiques. Cette analyse confirme l'efficacité des DNN dans la détection proactive des cyberattaques.

## 3.3. Conclusion

En guise de conclusion, l'évaluation comparative des performances des systèmes de détection d'intrusion, axée sur la confrontation entre les réseaux de neurones profonds (DNN) et les algorithmes classiques d'apprentissage machine, révèle que les DNN surpassent significativement les approches traditionnelles. Les expériences ont démontré une meilleure précision, un taux de détection des attaques plus élevé et des taux de faux positifs réduits avec les DNN. L'utilisation des courbes ROC a solidifié ces résultats en montrant que les DNN tendent à être plus proches du coin supérieur gauche, indiquant une sensibilité et une spécificité supérieures. Ainsi, cette analyse renforce l'efficacité des DNN dans la détection proactive des cyberattaques, soulignant leur potentiel pour renforcer la sécurité des systèmes informatiques face aux menaces actuelles.

# ***Conclusion Générale.***

*En conclusion, ce rapport de projet de 3ème année en ingénierie informatique et réseaux a exploré l'approche de l'apprentissage profond pour un système intelligent de détection d'intrusion. L'objectif principal était de démontrer l'efficacité des réseaux de neurones profonds (DNN) par rapport aux méthodes classiques de détection d'intrusion.*

*L'étude a mis en évidence que les DNN surpassent les algorithmes traditionnels en termes de précision, de taux de détection des attaques et de réduction des faux positifs. Les expérimentations ont montré que les DNN sont capables d'apprendre des représentations complexes des données d'intrusion, offrant ainsi une meilleure performance globale.*

*En ajustant minutieusement les hyperparamètres, en déterminant les topologies de réseau optimales et en réalisant des expérimentations approfondies, il a été démontré que les modèles basés sur les DNN sont plus efficaces pour détecter les comportements malveillants dans les réseaux. L'utilisation des courbes ROC a confirmé la supériorité des DNN en termes de sensibilité et de spécificité par rapport aux classificateurs classiques.*

*En fin de compte, ce rapport ouvre des perspectives pour l'avenir de la recherche en matière de détection d'intrusion, mettant en lumière le potentiel des réseaux de neurones profonds pour renforcer la sécurité des systèmes informatiques face aux cybermenaces croissantes.*