JOURNAL AFRICAIN DES SCIENCES
VOL. 3, **2** (2026) 73-79

https://jafrisci.org

ISSN (online) : 3107-0949 ; ISSN (print) : 3107-0930

OPEN ACCESS

ARTICLE DE RECHERCHE

Article Info.:
Reçu : le 08/01/2026
Accepté: le 18/02/2026
Publié : le 28/02/2026

IDENTIFICATION D'ANOMALIES PAR APPRENTISSAGE SUPERVISÉ A L'AIDE D'UNE ARCHITECTURE PROFONDE HYBRIDE ORIENTÉE SIMILIARITÉ: UNE APPROCHE POUR LA GESTION DES CLASSES DÉSÉQUILIBRÉES

Steve Ngeleka Musangu [1,*], Simon Ntumba Badibanga [1], Eugène Mbuyi Mukendi [1], Pierre Kafunda Katalay [2], David Okitesse [2]

https://doi.org/10.70237/jafrisci.2026.v3.i2.06

Résumé

L'identification des anomalies en matière de cybersécurité constitue un enjeu majeur du fait du déséquilibre considérable entre les données normales, qui sont largement prédominantes, et les attaques, qui bien que rares, sont d'une grande importance. Pour traiter cette question, nous proposons une approche d'apprentissage supervisé fondée sur une architecture profonde hybride orientée similarité, utilisant un réseau siamois combinant des CNN pour l'extraction de caractéristiques et des LSTM pour la représentation des dépendances temporelles. Cette architecture a pour objectif d'améliorer la discrimination des classes minoritaires tout en renforçant la solidité du modèle face aux attaques adversariales. Les résultats expérimentaux montrent que le modèle siamois CNN-LSTM atteint une précision de 98,9%, mettant ainsi en évidence son efficacité dans la gestion des classes déséquilibrées et l'amélioration des performances des systèmes de détection des intrusions.

Mots-clés: Deep Learning, Cybersécurité, Les classes déséquilibrées, Modèle SIAMOIS, CNN et LSTM.

Abstract

Anomaly detection in cybersecurity is a major challenge due to the significant imbalance between normal data, which are largely predominant, and attacks, which, although rare, are highly critical. To address this issue, we propose a supervised learning approach based on a similarity-oriented hybrid deep architecture, using a Siamese network that combines CNNs for feature extraction and LSTMs for modeling temporal dependencies. This architecture aims to improve the discrimination of minority classes while enhancing the model's robustness against adversarial attacks. Experimental results show that the Siamese CNN–LSTM model achieves an accuracy of 98.9%, highlighting its effectiveness in handling class imbalance and improving the performance of intrusion detection systems.

Keywords: Deep Learning; Cybersecurity; Imbalanced Classes; Siamese Model, CNN, and LSTM.

1. Introduction

À l'ère numérique, la sécurité des systèmes d'information est devenue un enjeu crucial, tant pour les gouvernements que pour les entreprises et les particuliers. Avec l'explosion du volume de données échangées et l'essor des technologies connectées, les cyberattaques se sont multipliées et ont pris une tournure de plus en plus sophistiquée. Face à cette menace grandissante, de nombreux chercheurs ont mis au point des systèmes intelligents de détection d'intrusions, utilisant des techniques d'apprentissage supervisé pour faire la distinction entre le trafic normal et les activités malveillantes. Dans ce contexte, plusieurs études ont prouvé l'efficacité des méthodes de Machine Learning et de Deep Learning pour repérer les comportements anormaux dans les réseaux informatiques. Les réseaux de neurones artificiels, en particulier, ont été largement adoptés pour modéliser des comportements complexes grâce à leur capacité à saisir des relations non linéaires dans les données. De plus, des approches plus traditionnelles comme les arbres de décision, les forêts aléatoires ou les k-plus proches voisins ont montré des résultats satisfaisants sur des ensembles de données équilibrés. Cependant, ces méthodes rencontrent des limites significatives lorsque les classes sont fortement déséquilibrées, une situation courante dans le domaine de la détection d'intrusions, où les attaques réelles sont généralement rares par rapport au trafic normal.

Ce déséquilibre entre les classes a un impact majeur sur la performance des modèles de classification, les orientant souvent vers la classe majoritaire. Par conséquent, un système

Correspondance : *1ngelekasteve01unikin@gmail.com* ***(S. N. Musangu)***

Copyright : © The Author(s) Published under a Creative Commons Attribution 4.0 International Licence (CC BY 4.0)

[1]*Faculté des Sciences et Technologies, Université de Kinshasa, Kinshasa, République Démocratique du Congo*
[2]*Faculté des Sciences Appliquées, Université de Mbujimayi, Mbujimayi, République Démocratique du Congo*

peut afficher une précision globale impressionnante tout en peinant à détecter efficacement les intrusions, ce qui diminue considérablement son utilité dans le domaine de la cybersécurité. Pour remédier à ce problème, plusieurs études ont examiné des techniques de rééquilibrage des données, comme la pondération des classes, le sur-échantillonnage ou le sous-échantillonnage, mais les résultats sont parfois décevants. Dans ce cadre, les architectures de Deep Learning présentent des perspectives intéressantes, notamment les réseaux de neurones convolutifs (CNN), qui sont très efficaces pour extraire automatiquement des caractéristiques pertinentes, et les réseaux récurrents à mémoire à long et court terme (LSTM), qui peuvent modéliser les dépendances temporelles du trafic réseau. Cependant, lorsqu'ils sont utilisés de manière classique, ces modèles restent sensibles au déséquilibre des classes.[35,42,43]

C'est dans cette optique que s'inscrit notre étude, qui cherche à répondre à la question suivante : **Comment développer une architecture qui améliore la performance des modèles face aux attaques contradictoires tout en optimisant leur capacité à gérer le déséquilibre des classes ?** Pour y parvenir, nous proposons une méthode de détection d'intrusions par apprentissage supervisé, reposant sur un modèle siamois qui combine CNN et LSTM. Cette architecture permet d'apprendre une fonction de similarité entre les flux réseau, atténuant ainsi l'impact du déséquilibre des données et améliorant la détection des intrusions rares, tout en maintenant une performance globale élevée.

2. Cadre Théorique

Dans le domaine de la détection d'intrusions et de la gestion des classes déséquilibrées, plusieurs approches ont été mises en avant, allant des systèmes basés sur des règles et des modèles formels aux méthodes qui s'appuient sur l'intelligence artificielle et l'apprentissage automatique. Cependant, malgré des progrès significatifs, les travaux qui nous ont précédés présentent des limites qui entravent leur efficacité face aux défis actuels de la cybersécurité. Cela inclut la complexité du trafic réseau, l'évolution rapide des attaques et le déséquilibre des classes dans les ensembles de données. Dans cette optique, une analyse critique nous aide à mieux situer notre contribution et à justifier la pertinence de l'approche que nous proposons.

Ainsi, BREK Bouthaina (2019) a mis au point un système de détection d'intrusions qui repose sur une architecture multi-agents, intégrant des agents mobiles intelligents. Bien que cette méthode présente l'avantage d'une détection décentralisée et d'une surveillance plus large du réseau, elle dépend fortement de l'infrastructure sous-jacente et complique la coordination des agents. De plus, l'absence d'un mécanisme d'apprentissage automatique avancé limite la capacité du système à s'adapter aux nouvelles attaques, ce qui peut diminuer son efficacité dans des environnements en constante évolution. [5]

De son côté, T. Saranya (2020) a mené une étude comparative sur plusieurs algorithmes de machine learning appliqués aux systèmes de détection d'intrusions dans divers contextes, tels que l'IoT, le fog computing, les réseaux 5G et les villes intelligentes. L'auteur a utilisé des techniques comme l'analyse discriminante linéaire, les arbres CART et la forêt aléatoire pour classifier les intrusions. Cependant, ces méthodes traditionnelles de machine learning montrent des limites face à la nature hautement non linéaire et complexe du trafic réseau moderne. De plus, le problème du déséquilibre des classes n'a pas été abordé de manière explicite, ce qui peut entraîner une performance biaisée en faveur du trafic normal, au détriment des attaques rares mais critiques. [38]

En outre, ZITOUNI et BARKA (2024) ont mis au point un système de détection d'intrusions qui s'appuie sur l'apprentissage profond, montrant une nette amélioration de la précision dans la détection des cyberattaques. Cependant, leur méthode ne prend pas vraiment en compte le déséquilibre des classes et ne s'appuie pas sur une architecture axée sur la similarité, ce qui limite sa capacité à distinguer efficacement entre les comportements normaux et anormaux. De plus, comme c'est souvent le cas avec les modèles de deep learning, leur système manque d'interprétabilité, ce qui complique l'analyse des décisions prises par le modèle. [8]

Enfin, le travail de ROMDHANE BEN YOUNES (2007), qui se concentre sur la vérification formelle des modèles pour les réseaux sans fil 802.11, représente une contribution théorique significative. Néanmoins, cette approche repose principalement sur des signatures d'attaques prédéfinies, ce qui la rend peu efficace face aux menaces nouvelles ou inconnues. En outre, son utilisation est limitée aux réseaux Wi-Fi, ce qui restreint son application à d'autres environnements comme l'IoT ou les réseaux 5G. [31]

Face à ces limites, notre recherche intitulée « Identification d'anomalies par apprentissage supervisé à l'aide d'une architecture profonde hybride orientée similarité : une approche pour la gestion des classes déséquilibrées » propose une solution plus robuste et adaptable. En combinant l'apprentissage profond avec une architecture axée sur la similarité, nous cherchons à améliorer la distinction entre le trafic normal et malveillant, tout en intégrant des mécanismes spécifiques pour gérer le déséquilibre des classes. Ainsi, notre travail contribue à faire avancer les systèmes de détection d'intrusions en offrant une méthode plus efficace, généralisable et en phase avec les défis actuels de la cybersécurité.

3. Deep Learning (Apprentissage Profond)

L'apprentissage profond, ou deep learning, est une branche fascinante de l'apprentissage automatique qui s'appuie sur des réseaux de neurones artificiels à plusieurs couches. Cette technologie permet aux machines d'apprendre de manière autonome des représentations complexes à partir de vastes ensembles de données, sans avoir besoin d'une intervention manuelle pour extraire les caractéristiques. Sa capacité à modéliser des relations non linéaires en fait un outil précieux dans des domaines variés comme la vision par ordinateur, le traitement du langage naturel, la reconnaissance vocale, et même la cybersécurité, où il est particulièrement efficace pour détecter des anomalies. [1]

4. Cybersécurité

La cybersécurité englobe toutes les techniques, pratiques et technologies que l'on met en œuvre pour protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les cyberattaques, les accès non autorisés, le vol de données et d'autres menaces numériques. Son objectif est de garantir trois principes fondamentaux : la confidentialité

(protéger les informations), l'intégrité (prévenir toute modification non autorisée) et la disponibilité (s'assurer que les systèmes sont accessibles quand il le faut). [6]

5. Classes Desequilibrees

Le problème des classes déséquilibrées se fait de plus en plus sentir avec l'utilisation des algorithmes de machine learning dans divers domaines, notamment dans les télécommunications pour la détection de fraudes, la bio-informatique, la classification de textes, la reconnaissance vocale, la détection d'intrusions, et bien d'autres. Les données réelles provenant de ces domaines ne sont pas souvent réparties de manière équitable entre les classes. Par exemple, dans un scénario à deux classes, on peut se retrouver avec une classe représentant 98 % des exemples, tandis que l'autre n'en a que 2 %. Dans des cas comme la détection de fraudes téléphoniques, la détection de cartes de crédit frauduleuses et la détection d'intrusions, ce déséquilibre est bien réel. Ignorer ce problème peut entraîner de graves conséquences sur les performances, et cela peut coûter très cher si le classifieur se trompe en classifiant les éléments de la classe minoritaire. Prenons l'exemple de la détection d'intrusions : affirmer qu'une intrusion est un accès normal peut avoir des conséquences très sérieuses. [40]

6. Modèle SIAMOIS, CNN et LSTM

6.1 Modèle SIAMOIS (Siamese Network)

Le modèle SIAMOIS est une architecture qui se compose de deux sous-réseaux identiques, partageant les mêmes paramètres, et qui est conçue pour apprendre à évaluer la similarité entre deux entrées. Les modèles siamois sont particulièrement utiles lorsque les données sont limitées ou déséquilibrées, car ils se concentrent sur la comparaison des échantillons plutôt que sur leur classification directe. [13]

6.2 CNN (Convolutional Neural Network)

Les réseaux de neurones convolutifs sont experts dans l'extraction automatique de caractéristiques à partir de données structurées ou spatiales. Grâce aux opérations de convolution, ils parviennent à capturer des motifs locaux pertinents, ce qui améliore la représentation de données complexes. [7]

6.3 LSTM (Long Short-Term Memory)

Les LSTM sont une variante des réseaux de neurones récurrents, spécialement conçue pour modéliser les dépendances temporelles à long terme. Ils sont particulièrement efficaces pour analyser des données séquentielles, comme le trafic réseau ou les séries temporelles, en atténuant le problème de la disparition du gradient.[9]

7. Methodologie

7.1. Données Experimentales

Nous avons décidé d'utiliser les données CICIDS2018 pour cette étude, car il présente plusieurs raisons convaincantes qui justifient son choix dans ce contexte. Tout d'abord, il est essentiel de souligner que le CICIDS2018 n'a, jusqu'à présent, pas été largement exploité avec un algorithme de type réseau siamois associé à des CNN et LSTM. Cette nouveauté représente une véritable opportunité de recherche, car elle permet d'explorer l'efficacité des réseaux siamois dans la détection des intrusions, surtout pour des données à haute dimensionnalité avec des caractéristiques complexes, comme celles du CICIDS2018.

De plus, le CICIDS2018 présente des défis supplémentaires qui rendent son utilisation encore plus intéressante. En effet, cet ensemble de données est déséquilibré, ce qui signifie que les différentes classes de données (attaques contre trafic normal) ne sont pas réparties de manière égale. Cela pose un défi majeur pour la détection des intrusions, car un modèle d'apprentissage supervisé classique pourrait être biaisé vers la classe majoritaire, rendant la détection des attaques, surtout celles moins fréquentes, plus difficile.

L'utilisation d'un réseau siamois, qui est particulièrement adapté à la comparaison de paires d'échantillons, pourrait offrir une solution efficace à ce problème d'équilibrage.

Category	Attack Type	Flow Count	Training	Test
Brute-force	SSH-Bruteforce	230	184	46
	FTP-BruteForce	611	489	122
Web attack	Brute Force -XSS	187589	7504	1876
	Brute Force -Web	193360	15469	3867
	SQL Injection	87	70	17
DoS attack	DoS attacks-Hulk	466664	18667	4667
	DoS attacks-SlowHTTPTest	139890	55956	13989
	DoS attacks-Slowloris	10990	4396	1099
	DoS attacks-GoldenEye	41508	16603	4151
DDoS attack	DDOS attack-HOIC	686012	27441	6860
	DDOS attack-LOIC-UDP	1730	1384	346
	DDOS attack-LOIC-HTTP	576191	23048	5762
Botnet	Bot	286191	11448	2862
Infilteration	Infilteration	161934	6478	1620
Benign	/	12697719	50791	12698
Total	/	15450706	231127	57782

***Figure 1** : Extrait du Dataset CICIDS2018*

7.2. Architecture De La Solution Proposee

Notre approche s'articule autour d'une architecture de traitement organisé en cinq étapes complémentaires. Dans un premier temps, les données sont nettoyées pour les valeurs manquantes, les doublons et les anomalies pour garantir leur qualité. Puis, un équilibrage des classes est mis en œuvre, notamment grâce à des méthodes comme SMOTE, pour corriger les déséquilibres et améliorer la représentativité des données. Au cours de la troisième étape, plusieurs d'algorithmes sont entraînés et évalués en utilisant les données prétraitées. La quatrième étape implique l'utilisation d'attaques adverses pour introduire une contamination des données, dans le but d'évaluer la performance des modèles face à ces manipulations. Enfin, les algorithmes sont de nouveau appliqués sur les données empoisonnées et comparés selon des critères prédéfinis, afin d'identifier les modèles les plus performants et les plus résilients.

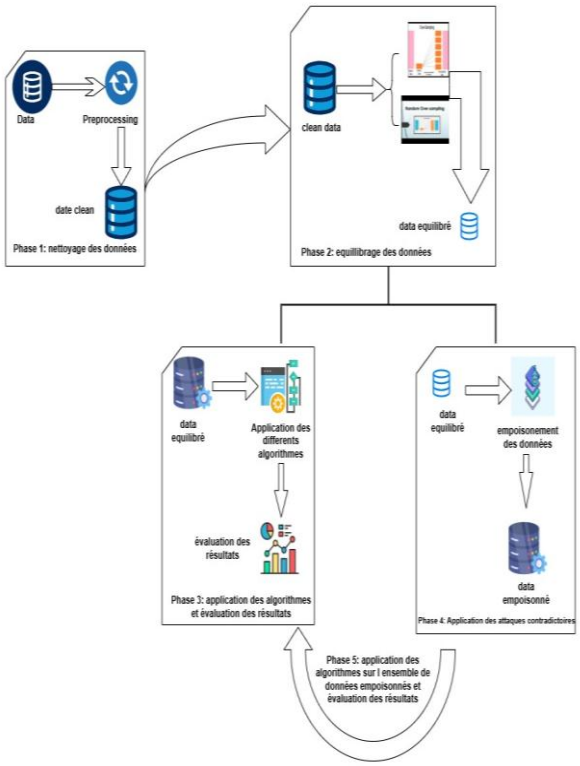


***Figure 2** : Architecture de la solution prosée*

7.3. Pretraitement des Données [12,13,26]

Dans notre contexte, voici les principales étapes de prétraitement que nous avons mises en œuvre :

• **Filtrage des Données** : Nous avons d'abord filtré l'ensemble de données pour éliminer toutes les lignes redondantes représentant les instances de classe. Ensuite, nous avons effectué une analyse pour identifier toute valeur 'NAN' (Not A Number) ou 'INF' (Infinite Value). Ces valeurs, considérées comme des données manquantes, peuvent sérieusement affecter les performances des modèles d'apprentissage automatique ou profond. Dans notre cas, la colonne "Flow Bytes" contenait plusieurs valeurs 'NAN'. Étant donné que nous avons un volume de données suffisant, nous avons décidé de supprimer les lignes avec des valeurs 'NAN' ou 'INF'.

• **Suppression des Colonnes Non Informatives** : Les statistiques descriptives ont montré que certaines colonnes étaient vides (avec des valeurs constamment égales à 0) et n'apportaient donc aucune information utile pour distinguer les classes d'attaque. Au contraire, elles pourraient mener à des résultats erronés. Des colonnes comme 'Bw PSH Flag', 'Fw URG Flag', 'Bw URG Flag', 'FIN Count', 'PST Count', 'ECE Count', 'Fw Avg Bytes/Bulk', 'Fw Avg Packets/Bulk', 'Fw Avg Bulk Rate', 'Bw Avg Bytes/Bulk', 'Bw Avg Packets/Bulk', et 'Bw Avg Bulk Rate' ont été supprimées. D'autres colonnes catégorielles, telles que les adresses IP et les horodatages ('Timestamp'), ont également été retirées, car ces informations ne sont pas directement liées aux caractéristiques des attaques. Des éléments comme 'Flow ID', 'Source IP', 'Destination IP', et 'Timestamp' ont été éliminés pour ne garder que les caractéristiques pertinentes du trafic réseau.

• **Encodage des Caractéristiques Catégorielles :** Certaines caractéristiques catégorielles dans notre ensemble de données nécessitaient un encodage. Par exemple, la colonne 'Flow Packets/s' a été transformée en une colonne numérique.

• **Encodage de la Colonne 'Label' :** La colonne 'Label', qui représente la classe de chaque instance, a été encodée grâce à une méthode bien connue appelée "One-Hot-Encoding". Cette technique convertit les catégories en colonnes distinctes, où une valeur de 1 signifie que l'instance appartient à cette classe, tandis qu'une valeur de 0 indique qu'elle n'y appartient pas.

• **Normalisation des Données :** Dans notre cas, nous avons utilisé StandardScaler de la bibliothèque Scikit-learn pour normaliser nos données. StandardScaler fonctionne en centrant et en réduisant chaque variable en appliquant la transformation suivante :

$$Xnormalisé = \frac{X - \mu}{\sigma}$$

où μ représente la moyenne de chaque caractéristique et σ son écart-type. Cela permet de transformer les données de manière à ce qu'elles soient centrées autour de 0, avec un écart-type de 1, assurant ainsi une échelle uniforme entre toutes les variables.

7.4. Equilibrage des Données avec SMOTE [20,21,26]

Nous avons utilisé la technique SMOTE (Synthetic Minority Over-sampling Technique) pour rétablir l'équilibre entre les classes dans notre ensemble d'entraînement. Avant d'appliquer SMOTE, nous avons constaté un déséquilibre marqué dans la distribution des classes, certaines étant clairement sous-représentées. Grâce à SMOTE, nous avons pu créer des exemples synthétiques pour les classes minoritaires, ce qui a permis d'atteindre un équilibre parfait.

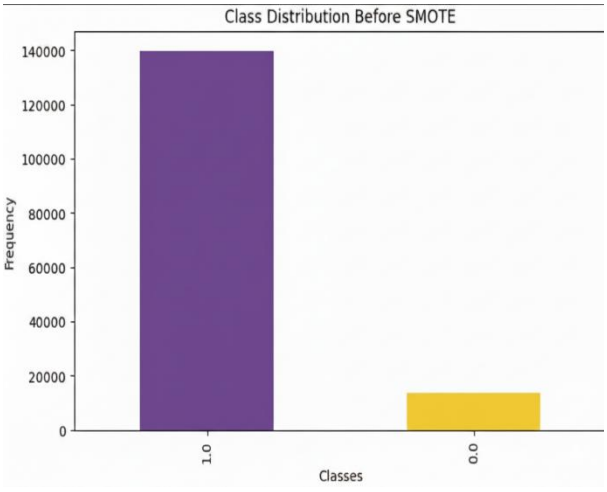


***Figure 3** : Distribution des classes avant SMOTE*

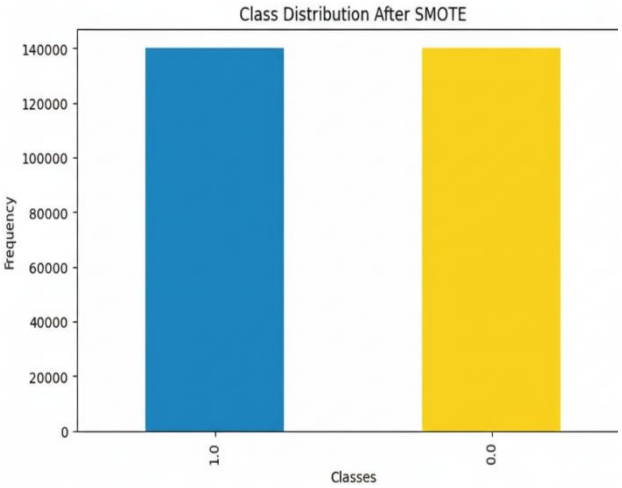


***Figure 4** : Distribution des classes après SMOTE*

8. Résultats [17,21,24, 36,44]

8.1 Entrainement des Modèles et Test de Performance

Cette section examine les performances de cinq algorithmes de classification appliqués à un jeu de données équilibré : l'arbre de décision, la forêt aléatoire, le CNN, le LSTM et le réseau siamois CNN-LSTM. Les résultats révèlent que l'arbre de décision obtient la meilleure précision, tandis que le modèle siamois CNN-LSTM propose le meilleur équilibre entre précision, rappel et score F1. Le CNN et le modèle siamois affichent un rappel élevé, ce qui indique une bonne capacité à identifier les comportements anormaux. En revanche, le LSTM montre des performances globalement inférieures, surtout en ce qui concerne la précision et le score F1.

Tableau 1 : **Performance des algorithmes sur l'ensemble des données équilibrées**

Algorithmes	accuracy	précision	rappel	F1 score
Random forest	96.8%	97%	95%	96%
Decision tree	98.2%	94%	96%	95%
CNN	97%	95%	97.4%	96.19%
LSTM	95.68%	90%	94.3%	92.10%
Siamois(CNN)	96.54%	96.25%	92%	94.08%
Siamois (CNN+LSTM)	97.7%	97%	97%	97%

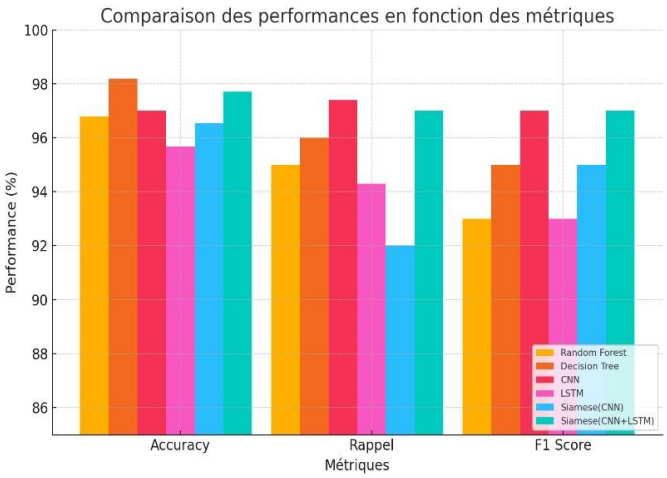


***Figure 5** : Le graphe de performance pour tous les algorithmes utilisés*

8.2 Amélioration de la Performance Globale des Modèles

Pour améliorer la performance de nos modèles, nous avons choisi d'utiliser la méthode FGSM (Fast Gradient Sign Method) pour générer des exemples adversaires, plutôt que la méthode PGD (Projected Gradient Descent). Ce choix est justifié par le fait que FGSM est largement reconnue comme une méthode de référence pour évaluer la performance des modèles face aux attaques adversariales, ce qui permet une comparaison claire et cohérente des performances des différentes architectures que nous avons étudiées.

Tableau 2 : **Performances des algorithmes réévaluées après intégration des attaques**

Algorithmes	accuracy	précision	rappel	F1 score
Random forest	97.3%	97.23%	97%	97.12%
Decision tree	98.3%	98%	96.71%	97.36%
CNN	97.15%	97.08%	97%	97.04%
LSTM	97.37%	96.12%	97.19%	96.65%
Siamois(CNN)	97.12%	96.78%	97.02%	96.9%
Siamois (CNN+LSTM)	98.9%	98%	98.43%	98.22%

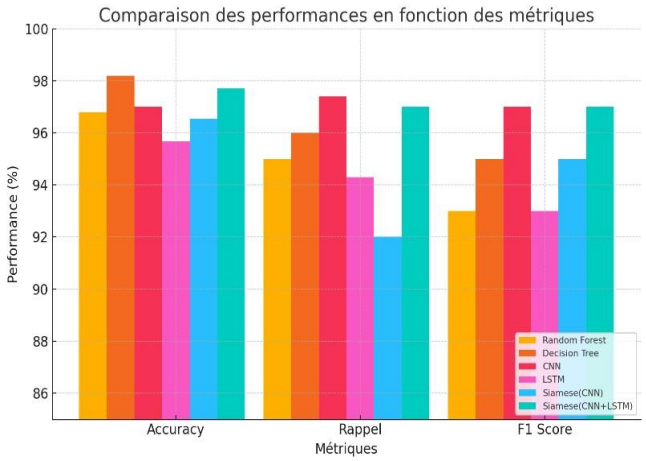


Figure 5 : **Le graphique de performance des algorithmes testés sur les données, à la fois équilibré et altéré.**

Les résultats de l'amélioration de performance révèlent que tous les algorithmes évalués atteignent des performances remarquables, avec des scores dépassant 96 % en termes d'accuracy, de précision, de rappel et de F1-score. Parmi eux, le modèle siamois qui combine CNN et LSTM se distingue clairement, affichant les meilleures performances globales : une accuracy de 98,9 %, une précision de 98 %, un rappel de 98,43 % et un F1-score de 98,22 %. Cela montre une excellente capacité à identifier correctement les cas positifs tout en minimisant les erreurs. L'arbre de décision présente également des résultats très encourageants, avec une accuracy de 98,3 %, bien que son rappel légèrement inférieur indique une sensibilité réduite face à certains cas. Les autres méthodes, comme la forêt aléatoire, le CNN, le LSTM et le modèle siamois basé uniquement sur CNN, affichent des performances homogènes autour de 97 % pour toutes les métriques, ce qui confirme leur robustesse. En somme, ces résultats suggèrent que tous les modèles sont efficaces, mais que l'approche siamoise hybride CNN-LSTM offre le meilleur équilibre entre précision et rappel, entraînant une amélioration globale des performances.

9. Conclusion

Cette étude s'est concentrée sur l'identification d'anomalies à l'aide de l'apprentissage supervisé, en utilisant une architecture profonde hybride axée sur la similitude, dans un contexte où les classes sont déséquilibrées. Pour équilibrer les classes, les données ont été prétraitées avec SMOTE. Les performances ont été comparées entre des algorithmes classiques tels que l'arbre de décision, la forêt aléatoire, le CNN et le LSTM, ainsi que des modèles siamois basés sur le CNN et le LSTM. L'analyse initiale sur des données équilibrées a révélé que l'arbre de décision affichait la meilleure précision globale avec 98,2 %, suivi du modèle siamois CNN+LSTM à 97,7 %. Cela indique que ces modèles réussissent à classer correctement la majorité des anomalies et du trafic normal. Après l'intégration des attaques, tous les modèles ont montré des performances élevées, avec des scores dépassant 96 % en termes d'exactitude, de précision, de rappel et de F1-score. Le modèle siamois hybride CNN-LSTM se démarque par ses performances exceptionnelles : une exactitude de 98,9 %, une précision de 98 %, un rappel de 98,43 % et un F1-score de 98,22 %. Cela démontre sa capacité à détecter efficacement les anomalies tout en minimisant les faux positifs. L'arbre de décision et les autres modèles (forêt aléatoire, CNN, LSTM, Siamese CNN) maintiennent des performances autour de 97 %, mais l'approche hybride CNN-LSTM offre le meilleur équilibre entre précision et rappel, garantissant une identification fiable des anomalies et renforçant la sécurité des systèmes face aux attaques.

10. Références

[1] A. Buda, A. Maki, and M. A. Mazurowski, "A systematic study of the class imbalance problem in convolutional neural networks," *Neural Networks*, 2018.
[2] A. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv*, 2019.
[3] A. Rakotomamonjy et F. Renaud, "Apprentissage automatique : concepts et algorithmes," *Hermès Science*, 2016.
[4] A. Zimek, E. Schubert, and H.-P. Kriegel, "A survey on unsupervised outlier detection," *Statistical Analysis and Data Mining*, 2012.
[5] B. Brek, *Système de détection d'intrusions basé sur les systèmes multi-agents*, mémoire de master, Université Larbi Tébessi, Tébessa, Algérie, 2019.
[6] B. Schölkopf et al., "Support vector method for novelty detection," *Advances in Neural Information Processing Systems*, 2000.
[7] D. M. Chickering and D. Heckerman, "Efficient Bayesian network classifiers," *Machine Learning*, 1997.
[8] D. Zitouni et A. Barka, "Un système de détection d'intrusion basés sur l'apprentissage profond pour la cybersécurité," Mémoire, Université Kasdi Merbah Ouargla, 2024.
[9] F. Provost and T. Fawcett, "Robust classification for imprecise environments," *Machine Learning*, vol. 42, pp. 203–231, 2001.
[10] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *CVPR*, 2015.
[11] G. Batista, R. C. Prati, and M. Monard, "A study of the behavior of several methods for balancing machine learning training data," *SIGKDD Explorations*, 2004.
[12] H. Ahmed, A. Mahmood, and M. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, 2016.
[13] H. Shi, X. Li, and H. Lu, "Deep similarity learning for image classification," *Pattern Recognition*, 2019.
[14] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
[15] J. Bromley et al., "Signature verification using a 'Siamese' time delay neural network," *ICANN*, 1993.
[16] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed., Morgan Kaufmann, 2011.
[17] J.-H. Hwang et al., "An ensemble classification algorithm for imbalanced data," *IEEE Trans. Knowl. Data Eng.*, 2014.
[18] K. Q. Weinberger and L. K. Saul, "Distance metric learning for large margin nearest neighbor classification," *J. Mach. Learn. Res.*, 2009.
[19] L. Fernández et al., "Learning from imbalanced data sets," *Springer*, 2018.

[20] L. Yang et al., "Hybrid deep learning for anomaly detection," *IEEE Access*, 2020.
[21] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PloS ONE*, 2016.
[22] M. Lin, Q. Chen, and S. Yan, "Network in network," *ICLR*, 2014.
[23] M. Oussalah, *Détection d'anomalies dans les séries temporelles*, *Hermès*, 2019.
[24] M. Z. Alom et al., "A state-of-the-art survey on deep learning in medical image analysis," *Comput. Med. Imag. Graph.*, 2019.
[25] N. V. Chawla et al., "SMOTE: Synthetic minority over-sampling technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.
[26] O. Russakovsky et al., "ImageNet large scale visual recognition challenge," *IJCV*, 2015.
[27] P. Baldi, *Deep Learning in Science*, Cambridge University Press, 2021.
[28] P. Branco, L. Torgo, and R. Ribeiro, "A survey of predictive modeling on imbalanced domains," *ACM Comput. Surv.*, 2016.
[29] P. Dolla and A. Mourot, "Réseaux de neurones profonds pour la reconnaissance de formes," *Revue d'Intelligence Artificielle*, 2020.
[30] P. García, F. Sánchez, and R. Mollineda, *Apprentissage automatique et fouille de données*, Dunod, 2017.
[31] R. Ben Younes, "Étude et mise en œuvre d'une méthode de détection d'intrusions dans les réseaux sans-fil 802.11 basée sur la vérification formelle de modèles," Mémoire de maîtrise, Université du Québec à Montréal, Montréal, QC, Canada, 2007.
[32] S. Ahmed and B. Mahmood, "Network intrusion detection with deep learning," *Neurocomputing*, 2016.
[33] S. Chopra, R. Hadsell, and Y. LeCun, "Learning a similarity metric discriminatively," *CVPR*, 2005.
[34] S. Raschka and V. Mirjalili, *Python Machine Learning*, 3rd ed., Packt, 2019.
[35] T. Islam et al., "Credit card fraud detection using machine learning," *IEEE Access*, 2020.
[36] T. Liu, "Anomaly detection techniques and applications," *Roceedings of the International Conference on Computer Science and Electronics Engineering*, 2012.
[37] T. N. Sainath et al., "Deep convolutional neural networks for LVCSR," *ICASSP*, 2013.
[38] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung et M. K. A. Ahamed Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," *Procedia Computer Science*, vol. 171, pp. 1251–1260, Jan. 2020, doi: 10.1016/j.procs.2020.04.133.
[39] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, Jul. 2009.
[40] V. Lemaire, M.-L. Zhang, and X. Ruiz, "Apprentissage supervisé en présence de classes déséquilibrées : méthodes et enjeux," *Revue Française de Reconnaissance des Formes et Intelligence Artificielle*, 2017.
[41] X. Wang, Z. Han, and S. Wang, "Deep learning for anomaly detection: A review," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 7, pp. 2533–2553, 2020.
[42] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," *IEEE Trans. Pattern Anal. Mach. Intell.*, 2013.
[43] Y. LeCun, *Apprentissage profond et réseau de neurones*, Presses Universitaires de France, 2020.
[44] Y. Sun, Y. Chen, and N. Wang, "Deep metric learning with angular loss," *ICCV*, 2017.