

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

م. علاء زكريا جبلاوي * د. أكرم المرعي ** د. وسيم رمضان ***

الملخص

تعدّ هجمات رفض الخدمة الموزعة (DDOS) أحد أبرز التهديدات الأمنية في بيئات الشبكات المعرفة برمجياً (SDN). تزداد صعوبة الكشف عند التعامل مع الهجمات منخفضة المعدل، مما يؤدي إلى ارتفاع معدلات الإيجابيات الكاذبة في العديد من أنظمة الكشف التقليدية التي تهمل الخصائص الزمنية والمكانية لحركة المرور.

يقترح هذا البحث إطار عمل موحد متعدد الفئات موجه نحو SDN يعتمد على دمج الشبكات العصبية الالتفافية (CNN) مع شبكات (BiLSTM) ثنائية الاتجاه، وآلية الانتباه متعددة الرؤوس (Multi Head Attention). تم تدريب النموذج وتقييمه باستخدام مجموعة بيانات هجينة ناتجة عن دمج مجموعتي البيانات CIC-IDS2017 و CIC-IDS2018.

تم تقييم الأداء باستخدام مقاييس (Accuracy, Precision, Recall, F1-score). أظهرت النتائج تفوق نموذج CNN-BiLSTM-MultiAtt على كل من النماذج CNN و BiLSTM و CNN-BiLSTM، وذلك في كشف هجمات DDOS/DOS، حيث سجل النموذج 99.93% وفقاً لمقياس F1-Score.

على عكس الدراسات السابقة، يعالج النموذج هجمات DDOS وهجمات رفض الخدمة DOS ذات المعدل المرتفع والمنخفض ضمن إطار عمل موحد متعدد الفئات موجه نحو SDN، مع تحسين ملحوظ في تخفيف الإنذارات الكاذبة بنسبة 96.34% مقارنةً بـ CNN، و 75.97% مقارنةً بـ BiLSTM، و 70.46% مقارنةً بنموذج CNN-BiLSTM.

الكلمات المفتاحية: الشبكات المعرفة برمجياً، هجمات رفض الخدمة الموزعة، الشبكات العصبية الالتفافية.

*طالب دكتوراه - كلية الهندسة المعلوماتية - هندسة النظم والشبكات الحاسوبية - جامعة حمص

A hybrid spatial-temporal deep learning model for detecting low- and high-rate denial-of-service attacks in Software Defined Networks

Eng. Ala'a Zakaria Jeblawi* Dr. Akram Almarai**

Dr. Wassim Ramadan***

Abstract

Distributed Denial-of-Service (DDoS) attacks are among the most significant security threats in Software-Defined Networking (SDN) environments. Detection becomes increasingly difficult when dealing with low-rate attacks, leading to high false positive rates in many traditional detection systems that neglect the temporal and spatial characteristics of traffic.

This research proposes a unified, multi-class framework for SDN based on the integration of Convolutional Neural Networks (CNN), Bidirectional Networks (BiLSTM), and a Multi-Head Attention mechanism. The model was trained and evaluated using a hybrid dataset resulting from the integration of the CIC-IDS2017 and CIC-IDS2018 datasets. Performance was evaluated using metrics (Accuracy, Precision, Recall, F1-score). The results showed that the CNN-BiLSTM-MultiAtt model outperformed CNN, BiLSTM, and CNN-BiLSTM in detecting DDoS/DoS attacks, achieving an F1-score of 99.93%.

Unlike previous studies, this model simultaneously addresses both high- and low-rate DDoS and DoS attacks within a unified, multi-tiered SDN-oriented framework, significantly improving false positive reduction to 96.34% compared to CNN, 75.97% compared to BiLSTM, and 70.46% compared to CNN-BiLSTM.

KEYWORDS: Software Defined Networks, Distributed Denial of service Attacks, convolutional neural network.

*PhD Student – Faculty of Informatics Engineering – Department of Computer Systems and Networks Engineering – Homs University

** Assistant in Computer Systems and Networks Engineering

Faculty of Informatics Engineering – Homs University

*** Doctor in Agricultural Engineering – Homs University

1. المقدمة

شهدت شبكات الاتصالات خلال السنوات الأخيرة تطوراً ملحوظاً في بنيتها، وذلك مع ظهور الشبكات المعرفة برمجياً (Software-Defined Networking – SDN) كأحد أبرز تقنيات الشبكات الحديثة التي تفصل بين مستوى التحكم (Control Plane) ومستوى البيانات (Data Plane)، مما ساهم في إدارة الموارد بطريقة أكثر مرونة، وتحسين قابلية التوسع مقارنةً بالشبكات التقليدية.

تعتمد الشبكات المعرفة برمجياً على أسلوب التحكم المركزي في إدارة الشبكة وتوجيه الحزم، وتُستخدم على نطاق واسع في مراكز البيانات، والحوسبة السحابية، وإنترنت الأشياء، كما تُعد ركناً أساسياً في بيئات الشبكات المستقبلية لما توفره من قابلية البرمجة والتحكم الديناميكي في حركة المرور [1].

على الرغم من المزايا المتطورة التي تؤمنها الشبكات المعرفة برمجياً، إلا أنها لا تزال عرضة للتهديدات السيبرانية، ولا سيما هجمات رفض الخدمة (Denial of service – DOS) عالية ومنخفضة المعدل وهجمات رفض الخدمة الموزعة (Distributed Denial of service – DDOS)، التي تستهدف إغراق الموارد الشبكية بحركة مرور غير طبيعية لمنع المستخدمين الشرعيين من الوصول إلى الخدمات، مما يجعل دراسة أمن الشبكات المعرفة برمجياً، خصوصاً في سياق هجمات رفض الخدمة (DOS/DDOS)، أمراً بالغ الأهمية. وتمثل هجمات رفض الخدمة الموزعة (DDOS) أكثر الهجمات تعقيداً وانتشاراً في بيئات الشبكات، حيث يمكن أن تسبب شللاً كاملاً للبنى التحتية بسبب تنفيذها مع معدلات حركة مرور عالية، أيضاً تمثل هجمات رفض الخدمة منخفضة المعدل (Low-rate DOS) التي يتم تنفيذها بمعدلات منخفضة صعوبة كبيرة في الكشف عنها بواسطة أساليب الكشف التقليدية [2].

تشير الإحصائيات الحديثة الصادرة عن (Cloudflare Rader) إلى تصاعد ملحوظ في هجمات (DDOS) خلال السنوات الأخيرة، حيث ارتفع العدد الإجمالي للهجمات من حوالي (14) مليون هجمة في عام (2023) إلى (21.3) مليون هجمة في عام (2024)، ثم قفز بشكل حاد ليصل إلى (47.1) مليون هجمة خلال عام (2025)، بزيادة بلغت نحو (236%) مقارنة بعام (2023). ويعكس هذا التصاعد النمو الكبير في قدرة المهاجمين على تنفيذ هجمات واسعة النطاق وأكثر تعقيداً [24].

تعد البنى الشبكية التي تستخدم أسلوب التحكم المركزي في إدارة الشبكة أكثر عرضة لهجمات (DOS/DDOS)، إذ يمكن للهجوم على مستوى التحكم (Control Plane) أن يؤدي إلى تعطيل كامل عمليات التوجيه وإدارة الشبكة. تزداد الخطورة عند قيام هذا النوع من الهجمات باستخدام أسلوب التخفي عبر إرسال التدفقات بمعدل منخفض، الأمر الذي يصعب على آليات الكشف التقليدية التعامل معها [1]، وهذا ما يوضح أهمية البحث في اقتراح حلول تساهم في كشف هذا النوع من الهجمات.

معظم الأبحاث الحالية التي تستهدف الكشف عن هجمات (DOS/DDOS) تركز على الهجمات ذات المعدلات العالية، إذ تبين وجود عدد محدود من الحلول الحالية تتعامل مع الهجمات منخفضة المعدل [3]. غالبيتها تعتمد على التصنيف الثنائي مع إهمال البعد الزمني والاختبار على مجموعة بيانات واحدة. كما أنه لا يوجد إطار موحد قادر على التعامل بكفاءة مع كلا النوعين من الهجمات (منخفضة ومرتفعة المعدل) ضمن بيئة الشبكات المعرفة برمجياً، بحيث تكون قادرة على تحسين معدلات الدقة وتقليل معدلات الخطأ الكاذب، مما يبرهن أهمية استخدام هذا البحث لمنهجية تعتمد على دمج الشبكات العصبية الالتفافية (CNN) بهدف استخراج الخصائص المكانية، وشبكات الذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (BiLSTM) للنقاط الاعتماديات الزمنية [4]، بالإضافة إلى آلية الانتباه متعددة الرؤوس (Multi Head Attention).

أظهرت النتائج التجريبية تفوق النموذج الهجين على بقية نماذج الكشف الأخرى في كشف هجمات (DOS/DDOS)، وقد سجل النموذج 99.93% وفقاً لمقياس F1-Score.

إن دمج الشبكات العصبية الالتفافية (Convolutional Neural Network-CNN) مع شبكات الذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (Bidirectional Long Short-Term -BiLSTM) Memory)، بالإضافة إلى آلية الانتباه متعددة الرؤوس (Multi Head Attention) يمثل حلاً فعالاً للكشف عن الهجمات البطيئة والمعقدة في بيئات الشبكات المعرفة برمجياً.

ساهم البحث في اقتراح نموذج هجين متعدد الفئات للكشف عن هجمات (DDoS/DOS) ذات المعدلات المرتفعة والمنخفضة، حيث أُجريت الاختبارات على مجموعة بيانات هجينة ومتنوعة مع تحسين الأداء وتخفيف الإنذارات الكاذبة بمعدل 0.020% متوقفاً بذلك على CNN بمقدار 96.34%، وعلى BiLSTM بمقدار 75.97%، وبمقدار 70.46% مقارنةً بنموذج CNN-BiLSTM.

2. الدراسة المرجعية

بعد مراجعة أدبيات الدراسات السابقة تبين لدينا أنه يمكن تصنيف الدراسات المرجعية وفقاً لثلاثة اتجاهات. الاتجاه الأول: يمثل نماذج (ML) التقليدية، الاتجاه الثاني: يمثل نماذج مثل (LSTM/GRU)، الاتجاه الثالث: يمثل إضافة آليات متقدمة مثل (Attention).

1. الاتجاه الأول:

يمثل هذا التوجه الدراسات التي اعتمدت على نموذج واحد أو على بنية كشف مباشرة نسبياً، دون دمج عميق بين عدة معماريات أو توظيف آليات متقدمة للانتباه واستخراج الميزات. في هذا السياق، جاءت الدراسة [20] التي اقترح فيها Marcos V.O. Assis وآخرون نظاماً للكشف يهدف إلى تخفيف أثر هجمات DDoS على متحكم SDN، بالاعتماد على خوارزمية GRU داخل وحدة الكشف. وقد جرى تقييم الخوارزمية بمقارنتها مع سبعة نماذج أخرى، مثل DNN و CNN و LSTM و SVM و LR و KNN و GD، باستخدام مجموعتي البيانات: CIC-2019 و CIC-IDS2018. وأظهرت النتائج تفوق GRU من حيث التوازن بين مؤشرات الأداء المختلفة. ومع ذلك، اقتصرَت الدراسة على اكتشاف الشذوذ دون الانتقال إلى تصنيف نوع الهجوم، وهو ما يحد من شمولية النموذج في البيئات العملية.

2. الاتجاه الثاني:

يمثل التوجه الأحدث في الدراسات، حيث لا يكفي بدمج نماذج التعلم العميق فقط، بل يضيف طبقات تصنيف نهائية أكثر ذكاءً، بما يعزز القدرة على التعميم في بيانات بيئات متعددة. ومن أبرز أمثلة هذا الاتجاه الدراسة [18] التي اقترح فيها Azhar F. Al Zubidi وآخرون خوارزمية هجينة ثلاثية المراحل CNN-LSTM-XGBoost للتنبؤ بهجمات DDOS و DOS؛ إذ تُستخدم CNN لاستخراج الأنماط المكانية، و LSTM لانتقاط الاعتماد الزمني، بينما يعمل XGBoost

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

كطريقة تصنيف نهائية قادرة على التعامل مع الضجيج وعدم التوازن في البيانات. وقد تم تقييم النموذج على ثلاث مجموعات بيانات هي CIC-IDS001 و CIC-IDS2017 و CIC-IDS2018، وحقق دقة مرتفعة بلغت 98.3% و 99.2% و 99.3% على التوالي. وتمثل هذه الدراسة تطوراً مهماً نحو التكامل بين التعلم العميق والتعلم الآلي المعزز في أنظمة الكشف.

كما تتدرج ضمن هذا الاتجاه أيضاً الدراسة [17] التي قدّم فيها Ahmed M. Elshewey وآخرون تقييماً لعدة نماذج من التعلم العميق، مع اقتراح نموذج هجين CNN-GRU لتصنيف حركة المرور إلى فئتين: طبيعية وهجومية. وقد عولج عدم توازن البيانات باستخدام تقنية SMOTE، بعد أن كانت مجموعة البيانات الأصلية غير متوازنة، ثم جرى تطبيق خطوات معالجة مسبقة شملت تعويض القيم المفقودة وتوحيد القياس عبر Standard Scaler. ورغم أن النموذج حقق نتائج مثالية في مؤشرات الأداء، إلا أن الاعتماد على حجم بيانات محدود مع تضخيم اصطناعي للعيبة يجعل النتائج بحاجة إلى مزيد من التحقق، فضلاً عن أن الدراسة اعتمدت على التصنيف الثنائي فقط ولم تتناول التصنيف متعدد الفئات.

3. الاتجاه الثالث:

يمثل هذا التوجه مرحلة أكثر تطوراً، حيث انتقلت فيه الدراسات من النماذج الأحادية إلى الدمج بين بنى متعددة للتعلم العميق، مع الاعتماد على آليات الانتباه (Attention) أو تقنيات اختيار الميزات لتعزيز الأداء والحد من الإنذارات الكاذبة.

في هذا الإطار، قدّم Ashfaq Ahmad Najar وآخرون في الدراسة [16] نموذجاً هجيناً يجمع بين CNN و BiLSTM و Attention بهدف تعزيز استخراج الميزات وتحسين أداء التصنيف في كشف هجمات DDOS. وقد تم اختبار النموذج على مجموعتي البيانات CIC-DDOS2019 و Edge-IloT، وحقق دقة مرتفعة بلغت 99.78% و 98.84% على التوالي. وتؤكد نتائج المقارنة أن هذا النموذج يتمتع بمتانة جيدة وملاءمة للتطبيق في البيئات محدودة الموارد. ومع ذلك، اقتصرَت هذه الدراسة على هجمات DDOS مرتفعة المعدل دون معالجة الهجمات منخفضة المعدل.

وتتدرج الدراسة [19] ضمن هذا الاتجاه أيضاً، حيث اقترح Junjie Zhao وآخرون نموذجاً يجمع بين CNN و BiLSTM و Attention لمعالجة مشكلتي انخفاض دقة التصنيف وارتفاع معدل الإنذارات الكاذبة. وقد دعموا النموذج بمرحلة اختيار ميزات باستخدام الغابة العشوائية وتحليل ارتباط بيرسون،

يهدف تقليل التكرار في المدخلات وتحسين جودة البيانات الداخلة للنموذج. ثم استُخدمت CNN لاستخراج الأنماط المكانية، و BiLSTM لتمثيل الاعتماديات الزمنية، بينما تولت Attention إبراز السمات الأكثر أهمية، قبل أن يُستخدم SoftMax لإخراج نتائج التصنيف. وأظهرت التجارب على CIC-IDS2017 و CIC-DDOS2019 تفوق النموذج المقترح على النماذج الأخرى في مؤشرات الأداء المختلفة، سواء في التصنيف الثنائي أو المتعدد.

وبالتالي تتحدد الفجوة البحثية في غياب نموذج هجين متعدد الفئات، مدعوم بدمج بيانات متنوعة وضبط للمعاملات الفائقة، وقادر على كشف الهجمات منخفضة وعالية المعدل بكفاءة عالية ضمن بيئة الشبكات المعرفة برمجياً. وهذا ما يوضحه الجدول (1) مقارنة بين الدراسة الحالية والدراسات السابقة.

الجدول (1): مقارنة مع الدراسات السابقة

Study	Model	Dataset	Attack Type	Metrics			
				Accuracy	Precision	Recall	F1 Score
[16] 2025	CNN-BiLSTM-AT	CIC-DDOS2019	DDOS	99.78	99.77	99.77	99.70
		Edge IIoT		98.84	98.83	98.83	98.81
[17] 2025	CNN-GRU	InSDN	DDOS	100	100	100	100
[18] 2023	CNN-LSTM-XGBOOST	CIC-IDS001	DDOS & Low-Rate DOS & High-Rate DOS	98.4	98.2	98.2	98.2
		CIC-IDS2017		98.6	98.8	99	99
		CIC-IDS2018		98.7	99	98.7	98.7
[19] 2023	CNN-Att-BiLSTM	CIC-IDS2017	DDOS	95.6	95.8	95.9	95.8

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

[20] 2021	GRU	CIC- DDoS2019	DDoS	99.94	99.94	99.94	99.94
		CIC-IDS 2018		97.09	97.09	97.09	97.09
Actual Study	CNN- BiLSTM- MultiAtt	CIC-IDS1718	DDoS & Low-Rate DOS & High-Rate DOS	99.93	99.93	99.93	99.93

3. هدف البحث

يهدف هذا البحث إلى تطوير نموذج هجين متعدد الفئات مخصص لبيئات الشبكات المعرفة برمجياً (SDN)، وذلك للكشف عن هجمات رفض الخدمة (DOS) عالية ومنخفضة المعدل وهجمات رفض الخدمة الموزعة (DDoS)، ضمن إطار تصنيفي موحد يضمن التعامل بفعالية مع مختلف أنماط الهجوم. من خلال تحقيق الأهداف الفرعية الآتية:

- استخراج الخصائص المكانية من بيانات المرور الشبكية باستخدام الشبكات العصبية الالتفافية (CNN).
- استخراج الخصائص الزمنية والاعتماديات التسلسلية باستخدام الشبكات المنكررة ثنائية الاتجاه (BiLSTM).
- تعزيز آلية التركيز على الخصائص الأكثر أهمية من خلال وحدة التركيز متعددة الرؤوس (Multi Head Attention).
- تحسين قدرة النموذج على التمييز بين الحركتين الطبيعية والهجومية، بما يساهم في الحد من الإنذارات الكاذبة.

- مقارنة أداء النموذج المقترح مع نماذج CNN و BiLSTM و CNN-BiLSTM لتقييم أثر الدمج المكاني-الزمني وآلية الانتباه على جودة الكشف.
- بناء مجموعة بيانات هجينة من CIC-IDS2017 و CIC-IDS2018 وإعادة تصنيف سجلاتها ضمن فئات سلوكية مناسبة لهجمات (DOS/DDOS).

4. الدراسة النظرية

نستعرض في هذا القسم أبرز الأفكار النظرية والتقنيات التي ارتكز عليها هذا البحث.

1.4 الشبكات المعرفة برمجياً (SDN - Software-Defined Networking)

تُعد الشبكات المعرفة برمجياً تحولاً معمارياً في تصميم الشبكات، إذ تفصل مستوى التحكم (Control Plane) عن مستوى البيانات (Data Plane)، مما يتيح إدارة مركزية ذكية وقابلة للبرمجة. يسهم هذا الفصل بين التحكم والبيانات في تعزيز مرونة إدارة الشبكة، وتحسين قابلية التوسع، وتسريع نشر الخدمات. إلا أن المركزية التي تمنح SDN هذه المرونة تجعلها في الوقت ذاته أكثر حساسية للهجمات التي تستهدف مستوى التحكم، إذ يمثل المتحكم نقطة اختناق حرجية يمكن أن يؤدي استنزافها إلى تعطيل الشبكة بالكامل.

من منظور أمني، يؤدي تدفق عدد كبير من الحزم غير المعروفة إلى المتحكم بهدف إنشاء قواعد تدفق جديدة إلى استهلاك موارده الحسابية، مما يجعل هجمات رفض الخدمة الموزعة (DDOS) ذات تأثير مضاعف في بيئة SDN مقارنة بالبنى التقليدية [27].

طُرِح بروتوكول OpenFlow كأحد أوائل المعايير المفتوحة التي سعت إلى توفير آلية موحدة للتحكم في أجهزة الشبكة، والذي تم تقديمه لتجاوز القيود التي فرضتها الحلول التقليدية [5].

تظهر خطورة هجمات رفض الخدمة منخفضة المعدل (Low-Rate DOS) ضمن بيئة SDN في اعتمادها على تدفقات منقطعة ومنخفضة المعدل تستغل انقضاء المهلة الزمنية في البروتوكولات قبل اتخاذ إجراء معين وحالات عدم التطابق في جداول التدفق، مما يدفع المبدلات إلى إرسال رسائل Packet-In متكررة إلى المتحكم. ونتيجة لذلك، يزداد الحمل على مستوى التحكم، ويتأخر تثبيت قواعد التدفق، وتعرض قناة OpenFlow بين المبدلات والمتحكم إلى ضغط مستمر، وهو ما قد يحول المتحكم إلى نقطة اختناق تؤثر في أداء الشبكة ككل، مما يفسر الحساسية العالية لبنية SDN تجاه هذا

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

النمط من الهجمات، وبالتالي يستدعي ذلك الاعتماد على نماذج كشف أكثر حساسية للأنماط الزمنية الدقيقة داخل بيئات SDN [24].

2.4 مفهوم OpenFlow ودوره في SDN

يُعد من أكثر البروتوكولات استخداماً في بيئات الشبكات المعرفة برمجياً، يمثل واجهة برمجة التطبيقات المتجهة جنوباً التي تتيح التواصل بين طبقة التحكم وطبقة البيانات. تتولى مؤسسة الشبكات المفتوحة (Open Networking Foundation – ONF) مسؤولية إدارة وتطوير معايير هذا البروتوكول. يُعتبر OpenFlow 1.5.0 أحدث إصدار رسمي معتمد من هذا البروتوكول [6].

تعتمد العديد من هجمات DDOS في بيئات SDN على استغلال آلية عمل OpenFlow ذاتها. فعند وصول حزمة لا تطابق أي قاعدة موجودة في جدول التدفق (Flow Table)، يقوم المبدل بإرسال رسالة (Packet-In) إلى المتحكم لطلب قرار بشأن كيفية معالجتها. في حال قيام المهاجم بإغراق الشبكة بعدد هائل من التدفقات الجديدة ذات رؤوس مختلفة، فإن ذلك يؤدي إلى:

- استنزاف موارد المتحكم نتيجة الكم الكبير من رسائل (Packet-In).
- زيادة زمن الاستجابة بسبب الضغط على قناة الاتصال بين المبدلات والمتحكم.
- امتلاء جداول التدفق داخل المبدلات، مما يؤدي إلى إسقاط حزم شرعية.
- احتمالية تعطيل المتحكم أو انهياره نتيجة الحمل الزائد.

انطلاقاً من ذلك، تكمن الحاجة إلى أطر كشف ذكية قادرة على تحليل الأنماط الزمنية والمكانية لحركة المرور، بما يمكن من اكتشاف سلوكيات الإغراق مبكراً قبل أن تؤثر على المتحكم أو جداول التدفق، وهو ما يتم العمل عليه في هذا البحث.

3.4 تعلم الآلة وأهميته في أمن الشبكات

يُعد تعلم الآلة أحد الفروع الأساسية للذكاء الاصطناعي، إذ يركز على تمكين الأنظمة الحاسوبية من اكتساب المعرفة من البيانات وتحسين أدائها تلقائياً دون الحاجة إلى برمجة واضحة. وتعتمد هذه التقنيات على تحليل الأنماط والعلاقات الكامنة داخل البيانات، مما يجعلها مناسبة للتعامل مع البيانات الديناميكية والمعقدة مثل حركة المرور الشبكية، مع قدرتها على كشف السلوك غير الطبيعي والتكيف مع الهجمات الجديدة وغير المعروفة [7].

واجهت الأساليب التقليدية لكشف التسلل المعتمدة على القواعد اليدوية والتوقع الثابتة قصوراً واضحاً في كشف الهجمات الحديثة، خاصة هجمات حجب الخدمة منخفضة المعدل، والتي غالباً ما تتخفي ضمن السلوك الطبيعي للشبكة. وقد أظهرت عدة دراسات أن هذه الأساليب تعاني من ضعف التكيف مع الهجمات الجديدة وتتطلب تحديثاً مستمراً للقواعد، مما جعل تقنيات التعلم الآلي ضرورة أساسية في بيئات الشبكات المعرفة برمجياً [8], [9], [10].

يُعدّ التعلم العميق أحد الفروع المتقدمة لتعلم الآلة، ويعتمد على الشبكات العصبية العميقة متعددة الطبقات القادرة على التعلم التلقائي للميزات ذات الصلة مباشرة من البيانات الخام، دون الحاجة إلى هندسة ميزات يدوية. وتمكّن هذه البنية الهرمية من تمثيل العلاقات المعقدة وغير الخطية بكفاءة عالية، فضلاً عن قدرتها على التعامل مع البيانات عالية الأبعاد [11].

تكتسب تقنيات التعلم العميق أهمية خاصة في مجال تحليل حركة المرور الشبكية، نظراً للطبيعة الديناميكية والمعقدة لهذا النوع من البيانات، والتي تتميز بتعدد الأبعاد، والاعتمادية الزمنية، وعدم الخطية، إضافة إلى احتوائها على مستويات مرتفعة من الضوضاء. وفي هذا السياق أثبتت نماذج التعلم العميق قدرتها على معالجة السلاسل الزمنية بكفاءة، واستخراج تمثيلات عالية المستوى، وتحقيق أداء متفوق من حيث الدقة والاستقرار مقارنة بالأساليب التقليدية [12][28].

وفي هذا السياق، تُستخدم الشبكات العصبية الالتفافية (CNN) لاستخراج الأنماط المحلية والعلاقات المكانية بين ميزات تدفقات الشبكة. وفي سياق كشف هجمات (DOS/DDOS)، تساعد CNN على النقاط العلاقات المميزة بين مؤشرات التدفق مثل مدة التدفق، ومعدل الحزم، وأحجام الحزم، والإحصاءات المرتبطة بالاتجاهين الأمامي والخلفي.

كما تُعد شبكات الذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (BiLSTM) من النماذج المناسبة لتحليل السلاسل الزمنية، إذ تعالج التسلسل في الاتجاهين الأمامي والخلفي، مما يسمح بالتقاط الاعتماديات السابقة واللاحقة داخل البيانات. وتكتسب هذه الخاصية أهمية خاصة في تحليل حركة المرور الشبكية، لأن بعض الهجمات، ولا سيما منخفضة المعدل، لا تظهر من خلال قيمة منفردة أو حزمة واحدة، بل من خلال نمط زمني متدرج ومتكرر.

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

تُستخدم آلية الانتباه (Attention Mechanism) لتعزيز قدرة النموذج على التركيز على الأجزاء الأكثر أهمية داخل التمثيلات المستخرجة. وفي حالة آلية الانتباه متعددة الرؤوس (Multi-Head Attention)، يتم توزيع عملية الانتباه على عدة رؤوس مستقلة. وتبرز أهمية هذه الآلية في كشف الهجمات منخفضة المعدل، لأن مؤشراتها قد تكون دقيقة ومتباعدة زمنياً، ولا تظهر بوضوح في كامل التدفق. لذلك تساعد Multi-Head Attention على إبراز السمات الأكثر دلالة وتقليل تأثير الضوضاء والخصائص الأقل ارتباطاً بالتصنيف.

5. أدوات البحث ومنهجيته

1.5 البيانات البحثية

تم دمج مجموعتي البيانات المرجعيتين CIC-IDS2017 و CIC-IDS2018 [22] [21]، اللتين تُعتبران من أشهر مجموعات البيانات العامة الشائعة في أبحاث كشف التسلسل، وهما ليستا مخصصتين لبيئات SDN، لكنهما مناسبتان لبناء وتقييم نموذج كشف يمكن تكيفه للعمل داخل شبكات SDN نظراً لاعتمادهما على بيانات تدفق مرورية واحتوائهما على أنماط هجمات متنوعة. تم توحيد البنية الهيكلية للسمات المشتركة بين المجموعتين، ثم:

- إزالة السمات غير المتوافقة.
- معالجة القيم المفقودة.
- توحيد أسماء الفئات.
- إعادة ترميز التسميات لتلائم التصنيف متعدد الفئات.

يهدف دمج المجموعتين إلى تعزيز تنوع البيانات (Data Diversity) وزيادة قدرة النموذج على التعميم، حيث تتضمن كل منهما توزيعات متفاوتة للهجمات، وأحجام تدفقات مختلفة. وبما أن الهدف الأساسي لهذا البحث يتمثل في كشف هجمات رفض الخدمة (DOS) بمختلف أنماطها، سواء ذات المعدلات المرتفعة أو المنخفضة، وهجمات رفض الخدمة الموزعة (DDOS)، فقد تم استخراج السجلات التي تمثل هذا النوع من الهجمات من كلتا المجموعتين، بما يضمن توفير تمثيل واقعي ومتوازن لسيناريوهات الهجوم المختلفة. كما جرى تضمين السجلات التي تمثل حركة المرور الطبيعية (BENIGN)، وذلك بهدف تمكين النموذج من تعلم الفروق الجوهرية بين السلوك الشبكي الطبيعي والنشاط الخبيث وتعزيز قدرته على التمييز الدقيق بينهما. يعرض الجدول (2) عدد السجلات

ضمن مجموعتي البيانات CICIDS2017 و CICIDS2018 ومجموعة البيانات CICIDS-1718 الناتجة بعد الدمج.

الجدول (2): توزيع سجلات مجموعة البيانات قبل وبعد الدمج

نوع الهجوم	CIC-IDS2017	CIC-IDS2018	نوع الهجوم بعد التصنيف	قبل المعالجة CICIDS-1718	بعد المعالجة CICIDS-1718
BENIGN	2273097	6876913	BENIGN	2273097	350000
DoS Hulk	231073	461912	High-Rate DOS	744786	369740
DOS GoldenEye	10293	41508			
DDOS	128027	1262203	DDOS	1390230	902241
DOS slowloris	5796	10990	Low-Rate DOS	162175	20573
DOS Slowhttptest	5499	139890			

وفقاً للجدول (2)، تم تجميع البيانات ضمن أربعة فئات رئيسية قائمة على التشابه السلوكي والخصائص الإحصائية لتدفقات الشبكة، بدلاً من الاعتماد على اسم أداة الهجوم فقط كما يلي:

- BENIGN : تمثل حركة المرور الطبيعية.

- DDOS : تشمل الهجمات الموزعة عالية الكثافة مثل HOIC و LOIC ، والتي تتميز بمعدلات حزم مرتفعة وأنماط إغراق مروري موزعة.

- High-Rate DOS : تشمل هجمات الإغراق أحادية المصدر ذات المعدل العالي مثل Hulk وGoldenEye، والتي تتميز بارتفاع كبير في معدل الحزم ضمن فترات زمنية قصيرة.
- Low-Rate DOS : تشمل هجمات الإغراق أحادية المصدر ذات المعدل المنخفض والبطيئة مثل Slowloris وSlowHTTPTest، والتي تعتمد على استنزاف الموارد تدريجياً عبر اتصالات طويلة منخفضة المعدل.

حيث تم دمج مجموعتي البيانات في مجموعة واحدة بهدف تكوين مجموعة بيانات أكثر توازناً وملاءمة لعملية التدريب. تم تنفيذ خطوة إعادة تصنيف (Label Reclassification) لتوحيد المسميات بين القاعدتين ومعالجة التباين في تسمية الهجمات، إذ أن بعض الهجمات تظهر بأسماء مختلفة رغم تشابهها السلوكي. وقد تم اعتماد استراتيجية إعادة تصنيف قائمة على التشابه السلوكي والخصائص الإحصائية لتدفقات الشبكة، بدلاً من الاعتماد على اسم أداة الهجوم فقط.

يهدف هذا التصنيف إلى تحقيق توازن بين الدقة التفصيلية للهجمات من جهة، وتقليل تجزئة حدود القرار (Decision Boundary Fragmentation) من جهة أخرى، مما يسمح للنموذج بتعلم أنماط سلوكية أكثر استقراراً وتمييزاً. كما يسهم توحيد الفئات في تقليل التباين داخل الفئة الواحدة (Intra-Class Variance) وتعزيز قابلية التعميم عند اختبار النموذج على بيانات غير مرئية.

تعاني مجموعة البيانات من عدم توازن واضح في توزيع فئات الهجمات، إذ يفوق عدد سجلات حركة المرور الطبيعية (BENIGN) عدد سجلات الهجمات الأخرى بفارق كبير. وقد أُجريت جميع عمليات المعالجة المسبقة، بما في ذلك تنظيف القيم الشاذة، وحذف السجلات المكررة، وتوحيد الميزات المشتركة بين القاعدتين، قبل إدخال البيانات إلى نموذج التعلم العميق وتشمل هذه الخطوات:

- ❖ إزالة السجلات المكررة: بلغ إجمالي عدد السجلات 4570288 سجل، بعد إزالة السجلات المكررة بلغ الإجمالي 3182475 سجل، حيث بلغت نسبة السجلات المحذوفة 30.4% من إجمالي البيانات.
- ❖ معالجة القيم المفقودة والشاذة: من خلال التعامل مع القيم اللانهائية أو القيم الناقصة، وذلك بتحويل جميع القيم اللانهائية (∞ ، $-\infty$) إلى Nan ثم تعويضها بمتوسط كل ميزة. وبالتالي أصبحت جميع البيانات صالحة رياضياً للتدريب.

❖ توحيد القياس باستخدام (Standard Scaler): وذلك عبر تطبيق عملية التطبيق

القياسي للميزات بحيث تصبح جميع القيم ضمن نطاق موحد، وهو أمر ضروري لضمان

كفاءة التعلم داخل الشبكات العصبية. جميع الميزات أصبحت ضمن توزيع قياسي (μ

$\sigma = 1$, $= 0$). الأمر الذي يساهم في تحسين سرعة التدريب وزيادة استقرار النموذج.

تم تطبيق Standard Scaler بعد تقسيم مجموعة البيانات الى ثلاث مجموعات

(تدريب، واختبار، وتحقق) وليس قبله، وتم ضبطه على بيانات التدريب فقط.

كما تم تطبيق تقنية Under Sampling بهدف تخفيف العبء الحسابي وتحسين التوازن دون

إدخال بيانات مزيفة (مولدة اصطناعياً)، والمحافظة على طبيعة البيانات الحقيقية، فتم تطبيق هذه التقنية

على سجلات Benign فقط لأنها: الأكبر حجماً وتحتوي على تكرار معلوماتي عالٍ (redundancy)

ولا تمثل حالة نادرة، كما تم الاحتفاظ بفئات الهجوم لأنها تحمل معلومات هجوم مهمة وتخفيفها قد

يؤدي إلى فقدان أنماط هجوم حرجية وضعف قدرة التعميم.

نلاحظ تحسن نسبة التوازن بين الفئات حيث بلغت النسب بعد المعالجة بشكل تقريبي كما يلي:

(Low-Rate $\approx 1\%$, BENIGN $\approx 20\%$, High-Rate $\approx 21\%$, DDOS $\approx 52\%$)

لكن لا تزال Low-Rate تمثل فئة نادرة ونسبتها منخفضة جداً، تم التعامل مع عدم التوازن المتبقي

باستخدام class weights حيث يتم إعطاء وزن أكبر للفئات الصغيرة أثناء التدريب (Low-Rate

DOS) بحيث يصبح الخطأ في هذه الفئة أكثر تكلفة، وهذا يؤدي إلى تحسين Recall للفئات النادرة.

كما تم الاستفادة من خوارزمية المعلومات المتبادلة (Mutual Information) لاختيار أهم الميزات

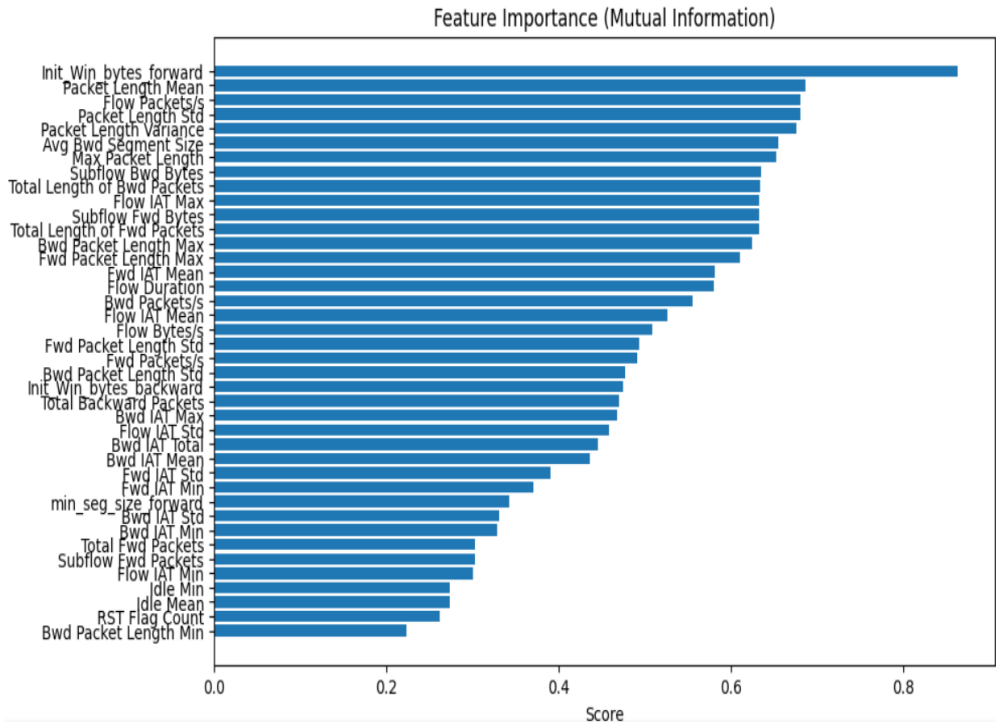
بالاعتماد على بيانات التدريب فقط، الأمر الذي مكّن من تقليل الأبعاد وإزالة الضوضاء وتحسين أداء

النموذج. وبعد تطبيق منهجية اختيار الميزات، تم تحديد 40 ميزة فقط من أصل 79 ميزة، وهي الميزات

الأكثر تأثيراً في التمييز بين حركة المرور العادية وحركة مرور هجمات (DOS/DDOS) بأنماطها

المختلفة. يظهر الشكل (1) أهم 40 ميزة تم اختيارها بواسطة خوارزمية المعلومات المتبادلة.

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً



الشكل (1): الميزات المختارة المستخدمة في التدريب

تم اختيار Mutual Information لأنها طريقة Filter-based، وقادرة على التقاط الاعتماديات الإحصائية غير الخطية بين خصائص تدفق الشبكة وفئة الهجوم، كما أنها أقل كلفة من طرق Wrapper التي تتطلب تدريب النموذج بشكل متكرر.

إن هذا الإعداد الدقيق لمجموعة البيانات، بالإضافة إلى الدمج بين مجموعتي CIC-IDS2017 وCIC-IDS2018، أدى إلى إنتاج مجموعة بيانات قوية ومتوازنة قادرة على تمثيل سيناريوهات الهجمات الحديثة، ومناسبة تماماً لتدريب النموذج الهجين المستخدم.

2.5 الحزم والمكتبات المستخدمة

اعتمد هذا البحث على مكتبات برمجية رائدة في مجالي تعلم الآلة والتعلم العميق، حيث استُخدمت Scikit-learn للمعالجة المسبقة وتقييم النماذج، و TensorFlow.Keras لبناء وتدريب الشبكات

العصبية، بينما استُخدمت Keras Tuner لتحسين المعاملات الفائقة بشكل منهجي، مما يضمن دقة أعلى وقابلية أفضل لإعادة إنتاج النتائج. يعرض الجدول (3) الإصدارات الخاصة بالمكتبات المستخدمة في إعداد البحث.

الجدول (3): إصدارات المكتبات المستخدمة

الإصدار	اسم المكتبة
2.13.0	TensorFlow
1.3.0	Scikit-learn
3.10.6	Matplotlib
2.3.2	Pandas
1.24.3	NumPy
3.10.18	Python

6. مقاييس الأداء

تم حساب وزن لكل فئة من الفئات الأربع الرئيسية ضمن مجموعة البيانات الهجينة -CICIDS 1718 باستخدام (compute_class_weight) من خلال (scikit-learn)، بعدها تم تمرير هذه الأوزان إلى (model.fit) عبر (class_weight) عملياً، هذا يعني أن كل عينة تأخذ وزن فئتها أثناء حساب دالة الخسارة في التدريب فقط، وليس أثناء الاختبار. المعادلة المستخدمة في الوضع (balanced) هي [26]:

$$W_c = \frac{N}{K \times n_c} \quad (1)$$

حيث:

- N : عدد عينات التدريب الكلي

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

• K : عدد الفئات

• n_c : عدد عينات الفئة c داخل بيانات التدريب

وفيما يلي المقاييس المعتمدة لتقييم أداء النظام المقترح لمقارنة نتائج النظام مع القيم المتوقعة أو الحقيقية، وذلك بهدف قياس مقدار الأخطاء أو الفروقات بينهما [15]:

❖ الدقة الإيجابية (Precision): ويُعبّر عن هذا المقياس رياضياً كما يأتي:

$$precision = \frac{TP}{TP+FP} \quad (2)$$

حيث:

- TP (True Positive): النموذج توقع أن العينة إيجابية، وكانت إيجابية بالفعل.
- FP (False Positive): النموذج توقع أن العينة إيجابية، لكنها في الحقيقة سلبية.
- ❖ الاسترجاع (Recall): ويُعبّر عن هذا المقياس رياضياً كما يأتي:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

حيث:

- FN (False Negative): النموذج توقع أن العينة سلبية، لكنها في الحقيقة إيجابية.
- ❖ درجة F1 (F1-Score): ويُعبّر عن هذا المقياس رياضياً كما يأتي:

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

❖ الدقة الكلية (Accuracy): ويُعبّر عن هذا المقياس رياضياً كما يلي:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (5)$$

حيث:

- TN (True Negative): النموذج توقع أن العينة سلبية، وكانت سلبية بالفعل.

7. النتائج والمناقشة

تم تنفيذ البحث باستخدام بيئة حاسوبية مخصصة لدعم نماذج التعلم العميق ومعالجة البيانات كبيرة الحجم، ثم اختبار النماذج ضمن بيئة Jupyter Notebook [13]. واستخدام برنامج [14] Microsoft Visio لرسم المخططات التدفقية وذلك بهدف دعم الشرح النظري ضمن سياق البحث. يوضح الجدول (4) الأدوات المستخدمة لإعداد التجارب.

الجدول (4): أدوات إعداد التجارب

الإصدار	الأداة
6.30.1	Jupyter
2019	Microsoft Visio
10 PRO	Windows
Intel i5-8400H (8 CPUs)	CPU
32GB	RAM

تم إعداد البحث وفق خطوات المنهجية العامة لتطوير نظام كشف تسلل فعال يعتمد على نموذج هجين يجمع بين شبكات (CNN)، والشبكات المتكررة ثنائية الاتجاه (BiLSTM)، بالإضافة إلى آلية الانتباه متعددة الرؤوس (Multi Head Attention). تم تصميم هذه المنهجية بشكل متسلسل ومنظم لضمان تحقيق أعلى مستويات الدقة والكفاءة في اكتشاف الهجمات السيبرانية ضمن بيئة الشبكات المعرفة برمجياً.

وفي المرحلة اللاحقة تم تقسيم مجموعة البيانات الناتجة إلى ثلاث مجموعات فرعية، حيث خُصّصت نسبة (70%) من البيانات لأغراض التدريب، في حين استُخدمت النسبة المتبقية (15%) لاختبار النموذج وتقييم أدائه و (15%) لأغراض التحقق.

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

بعد إجراء عملية التحسين عبر اختيار أفضل قيم للمعاملات الفائقة باستخدام Bayesian Optimization تم تقييم أداء النموذج الهجين باستخدام مقاييس الأداء الأربعة المعتمدة، ثم مقارنته مع بعض النماذج لدراسة تأثير إضافة بعض الطبقات الى النموذج، يعرض الجدول (5) مقارنة تفصيلية لكل فئة مدروسة (حميدة أو مهاجمة) وأداء النماذج وفقاً لمعايير الأداء التالية (Precision, Recall, F1-Score)، وذلك باستخدام مجموعة البيانات الهجينة CICIDS-1718.

الجدول (5): مقارنة أداء عدة نماذج على مجموعة البيانات CICIDS-1718

Model	Attack Type	Precision	Recall	F1-Score	Support
CNN	BENIGN	99.13	96.32	97.70	52500
	DDOS	99.58	98.98	99.28	135337
	High-Rate DOS	94.97	98.76	96.83	55461
	Low-Rate DOS	95.61	98.80	97.18	3086
BiLSTM	BENIGN	99.50	99.46	99.48	52500
	DDOS	99.96	99.85	99.91	135337
	High-Rate DOS	99.53	99.77	99.65	55461
	Low-Rate DOS	98.65	99.74	99.19	3086
	BENIGN	99.73	99.44	99.59	52500
	DDOS	99.97	99.89	99.93	135337

CNN-BiLSTM	High-Rate DOS	99.44	99.84	99.64	55461
	Low-Rate DOS	98.72	99.77	99.24	3086
CNN-BiLSTM-MultiAtt	BENIGN	99.89	99.82	99.85	52500
	DDOS	99.99	99.98	99.98	135337
	High-Rate DOS	99.88	99.93	99.91	55461
	Low-Rate DOS	99.13	99.77	99.45	3086

حيث تم تقييم أداء النماذج الأربعة وفقاً لخمس مراحل بهدف الوصول إلى النموذج المقترح:

المرحلة الأولى: تقييم نموذج CNN

وفقاً للجدول (6) نلاحظ أن نموذج (CNN) أعطى أداءً جيداً في الهجمات الواضحة، وضعفاً نسبياً في اكتشاف هجمات (High-Rate) و (Low-Rate)، وهذا يُفسَّر بأن نموذج (CNN) جيد في استخراج الأنماط المحلية، لكنه لا يفهم التسلسل الزمني. وبالتالي هناك حاجة إلى نموذج قادر على فهم الاعتماديات الزمنية داخل حركة المرور الشبكية.

الجدول (6): تقييم نموذج CNN

F1-Score	الهجوم
97.70	BENIGN
99.28	DDOS
96.83	High-Rate DOS
97.18	Low-Rate DOS

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

المرحلة الثانية: إضافة BiLSTM

وفقاً للجدول (7) نلاحظ تحسن واضح وهذا يعني أن العلاقات الزمنية مهمة جداً. الهجمات البطيئة تعتمد على أنماط تسلسلية. نموذج (BiLSTM) حسن فهم السياق الزمني. خفّض الإخفاقات. حسن Recall و F1-Score. لكن ما تزال هناك مشكلة: فقدان بعض الخصائص المكانية المحلية.

الجدول (7): تأثير إضافة BiLSTM على النتائج

الهجوم	CNN	BiLSTM
High-Rate DOS	96.83	99.65
Low-Rate DOS	97.18	99.19

المرحلة الثالثة: الدمج بين CNN و BiLSTM

يوضح الجدول (8) أهمية الاستفادة من الميزات المكانية والزمنية ممثلة بنموذج واحد (CNN) ممتاز مكانياً و BiLSTM ممتاز زمنياً). أنتج الدمج تمثيلاً أكثر شمولية. حسن جميع الفئات تقريباً. قدم أداء إجمالي أفضل من استخدام النموذج الزمني او المكاني بشكل منفرد.

الجدول (8): تأثير الدمج بين CNN و BiLSTM.

الهجوم	BiLSTM	CNN-BiLSTM
DDOS	99.91	99.93
High-Rate	99.65	99.64
Low-Rate	99.19	99.24

المرحلة الرابعة: إضافة آلية الانتباه Attention

وهنا أهم نقطة في السرد البحثي. رغم تفوق CNN-BiLSTM: ما تزال الهجمات منخفضة المعدل أصعب كشفاً. بعض السمات ليست مهمة. يوجد تشابه مع الحركة الطبيعية. لذلك نحن بحاجة إلى آلية

تركز على السمات المهمة. تقلل الضوضاء. تعزز الأنماط الخفية. وهنا يصبح Multi-Head Attention إضافة منطقية جداً.

المرحلة الخامسة: تقييم Attention

الجدول (9): تقييم إضافة Attention.

الهجوم	CNN-BiLSTM	CNN-BiLSTM-ATT
DDOS	99.93	99.98
High-Rate	99.64	99.91
Low-Rate	99.24	99.45

يوضح الجدول (9) تحسن الأداء العام. وتحسن أيضاً بالنسبة للهجمات منخفضة المعدل Low-Rate DOS وهذه نقطة ممتازة. إضافة آلية الانتباه متعددة الرؤوس ساهمت في تحسين كشف الهجمات منخفضة المعدل، مما يشير إلى قدرة آلية الانتباه على التركيز على الأنماط الدقيقة والخفية داخل البيانات الشبكية.

وبالتالي وفقاً لما سبق اعتماد CNN-BiLSTM-MultiAtt كنموذج رئيسي (لأنه: الأفضل في تحقيق أعلى معدل كشف للهجمات منخفضة وعالية المعدل. ساهم في تخفيف الإنذارات الكاذبة بشكل كبير).

مما يؤكد فعالية الدمج بين استخراج الخصائص المكانية والنمذجة الزمنية. ومع ذلك، فقد ساهمت إضافة آلية Multi-Head Attention في تحسين أداء الكشف بالنسبة للهجمات منخفضة المعدل، والتي تمثل التحدي الأكبر بسبب طبيعتها المتخفية وتشابهها مع حركة المرور الطبيعية.

يعرض الجدول (10) مقارنة الأداء الإجمالي للنماذج المدروسة، وذلك باستخدام مجموعة البيانات التي تم تجميعها ودمجها CICIDS-1718.

نموذج هجين للتعلم العميق المكاني-الزمني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

الجدول (10): مقارنة الأداء الإجمالي للنماذج

Model	Accuracy	Precision	Recall	F1-Score	FPR (%)	FP	Parameter	Training Time (min)	Memory Used (MB)
CNN	98.35	98.39	98.35	98.36	0.547	4045	21060	47	4982
BiLSTM	99.74	99.74	99.74	99.74	0.083	616	299524	1109	4987
CNN-BiLSTM	99.78	99.78	99.78	99.78	0.068	501	396548	540	1593
CNN-BiLSTM-Multi Att	99.93	99.93	99.93	99.93	0.020	148	593924	1246	1797

وفقاً للجدول (10)، أظهرت النتائج التجريبية وجود توازن واضح بين الأداء التصنيفي والكلفة الحسابية بين النماذج. فقد حقق نموذج CNN أقل زمن تدريب وأقل عدد من المعاملات مقارنة ببقية النماذج، إلا أن ذلك انعكس على الأداء التصنيفي الذي سجل أقل قيمة F1-Score بلغت (98.36). ويعود ذلك إلى محدودية قدرة CNN على تمثيل الاعتماد الزمني طويل المدى داخل تدفقات الشبكة، إذ يركز بصورة أساسية على استخراج الأنماط المحلية فقط.

في المقابل، حقق نموذج BiLSTM تحسناً ملحوظاً في الأداء، حيث ارتفع F1-Score إلى (99.74) نتيجة قدرته على تحليل العلاقات الزمنية وتسلسل الحزم الشبكية بشكل ثنائي الاتجاه، إلا أن هذا التحسن ترافق مع ارتفاع كبير في زمن التدريب الذي تجاوز (1109 دقيقة)، بسبب الطبيعة التكرارية لحسابات LSTM والتي تتطلب معالجة تسلسلية للبيانات، مما يزيد الكلفة الزمنية بصورة كبيرة رغم أن استهلاك الذاكرة بقي ضمن حدود مقبولة نسبياً.

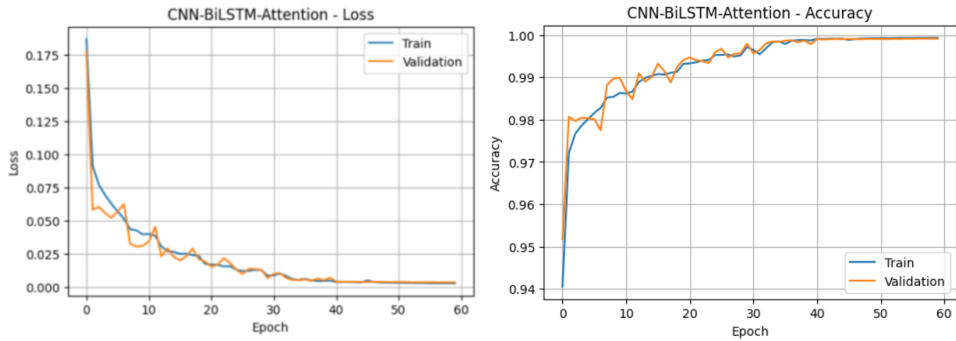
أما نموذج CNN-BiLSTM فقد حقق توازناً أفضل بين الكفاءة والأداء، حيث جمع بين قدرة CNN على استخراج الخصائص المكانية المحلية وقدرة BiLSTM على تمثيل السلوك الزمني للتدفقات الشبكية. وقد أدى هذا الدمج إلى رفع الأداء التصنيفي إلى (99.78) مع تقليل زمن التدريب إلى (540 دقيقة)، وهو أقل بكثير من نموذج BiLSTM، مما يشير إلى أن دمج CNN قبل BiLSTM يساعد على تقليل التعقيد الزمني عبر ضغط التمثيلات الأولية للبيانات قبل معالجتها زمنياً.

حقق نموذج CNN-BiLSTM-MultiAtt أعلى أداء بين جميع النماذج (99.93)، مما يدل على فعالية آلية Multi-Head Attention في تحسين التركيز على الأنماط الخفية والاعتماديات الزمنية الدقيقة المرتبطة بالهجمات ذات السلوك المتخفي. إلا أن هذا التحسن ترافق مع أعلى كلفة حسابية، حيث ارتفع عدد المعاملات إلى (593924) مما يساهم في تعلم علاقات أكثر تعقيداً لأنه يحتوي على عدد أكبر من الأوزان القابلة للتعلم. وأعلى استهلاك RAM وصل إليه البرنامج أثناء تنفيذ النموذج (1797 MB)، إضافة إلى زيادة زمن التدريب إلى (1246 دقيقة). ويعود ذلك إلى أن طبقة Attention تضيف إسقاطات خطية متعددة، فضلاً عن الاحتفاظ بالتسلسل الكامل للمخرجات الزمنية من BiLSTM، مما يزيد من حجم التمثيلات الوسيطة والعمليات الحسابية أثناء التدريب.

حقق نموذج CNN-BiLSTM-MultiAtt أدنى عدد من الإنذارات الكاذبة (FP) بلغ 148 حالة فقط، مقارنةً بـ 4045 حالة في نموذج CNN، و616 حالة في نموذج BiLSTM، و501 حالة في نموذج CNN-BiLSTM. ويعادل ذلك انخفاضاً في الإنذارات الكاذبة بنسبة 96.34% مقارنةً بـ CNN، و75.97% مقارنةً بـ BiLSTM، و70.46% مقارنةً بـ CNN-BiLSTM. كما انخفض معدل الإنذار الكاذب (FPR) إلى 0.020% فقط، مقابل 0.547% في CNN، مما يؤكد أن آلية Multi-Attention حسّنت بشكل ملحوظ قدرة النموذج على التمييز بين الحركة الطبيعية والهجومية وتقليل التنبهات الخاطئة.

بناءً على ذلك، يمكن اعتبار نموذج CNN-BiLSTM-MultiAtt النموذج الأكثر دقة وفعالية للكشف عن الهجمات مرتفعة ومنخفضة المعدل، في حين يُعد نموذج CNN-BiLSTM الخيار الأكثر توازناً بين الأداء والكلفة الحسابية، مما يجعله مناسباً أكثر للتطبيقات العملية داخل بيئات SDN التي تتطلب استجابة سريعة واستهلاكاً محدوداً للموارد الحاسوبية. يوضح الشكل (2) منحني الخسارة والدقة لكل من بيانات التدريب والاختبار للنموذج CNN-BiLSTM-MultiAtt.

نموذج هجين للتعلم العميق المكاني-الزماني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً



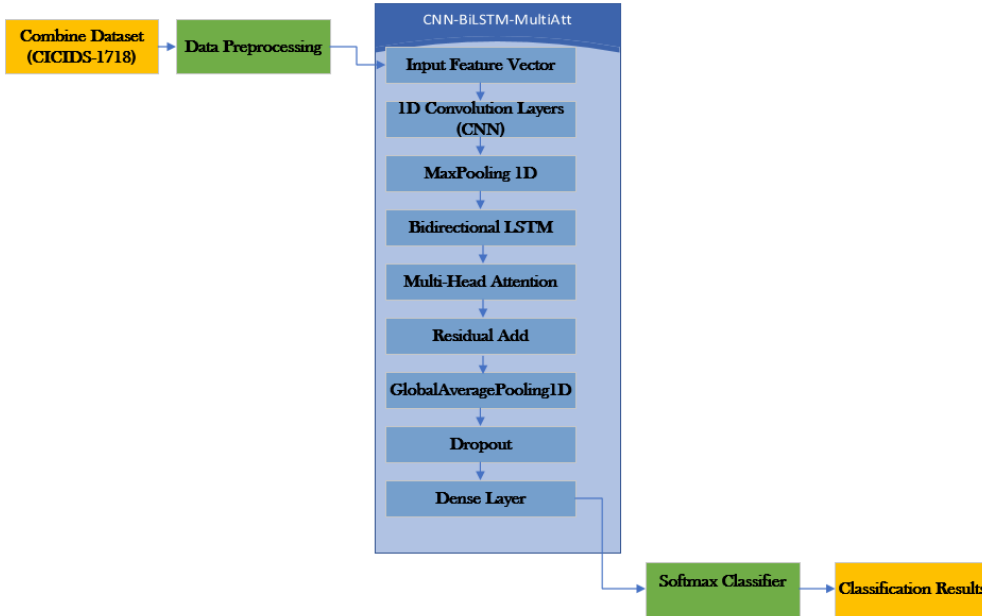
الشكل (2) منحنيات الأداء للنموذج CNN-BiLSTM-MultiAtt

يُظهر منحنى الخسارة في الجزء الأيمن من الشكل انخفاضاً حاداً في قيمة الخسارة خلال مرات التدريب الأولى، حيث تبدأ خسارة التدريب بقيمة مرتفعة (0.185) ثم تتخفّف تدريجياً وبسرعة كبيرة لتصل في نهاية التدريب إلى (0.0026) وهذا يشير إلى أن النموذج استطاع في المراحل المبكرة التقاط الأنماط الأساسية والخصائص المميزة لحركة المرور الشبكية بكفاءة عالية. كما نلاحظ أن خسارة التحقق (Validation Loss) تتخفّف أيضاً بشكل متوازي مع خسارة التدريب، مما يدل على أن النموذج لا يقتصر على حفظ بيانات التدريب فقط، بل ينجح في تعميم المعرفة على بيانات جديدة غير مرئية أثناء التدريب. الأهم من ذلك هو عدم وجود فجوة كبيرة بين منحنى خسارة التدريب والتحقق، مما يشير إلى أن النموذج لا يعاني من مشكلة (Overfitting)، وهو تحدٍ شائع في نماذج كشف التسلسل.

في الجزء الأيسر من الشكل (2)، نلاحظ أن دقة التدريب تبدأ بنسبة مقبولة منذ فترات التدريب الأولى، حيث تتجاوز (94.05)، ثم تستمر بالارتفاع تدريجياً حتى تصل إلى ما يقارب (99.94). بالمثل، فإن دقة التحقق تتبع نفس الاتجاه تقريباً، وتبقى قريبة جداً من دقة التدريب طوال فترة التدريب. هذا التقارب العالي بين المنحنيين يُعد مؤشراً قوياً على أن النموذج يتمتع بقدرة ممتازة على التعميم، وليس فقط تحقيق أداء مرتفع على بيانات التدريب. كما أن وصول دقة التحقق إلى مستويات شبه مثالية يدل على أن النموذج قادر على التمييز بدقة بين حركة المرور الطبيعية والهجمات المختلفة، بما في ذلك الهجمات منخفضة المعدل التي غالباً ما تكون أكثر صعوبة في الكشف.

8. معمارية النموذج المقترح

بناءً على ما تقدم وما تم التوصل إليه من خلال التجارب المعروضة ونتائجها تم اعتماد نموذج CNN-BiLSTM-MultiAtt. يستخدم النموذج المقترح في هذا البحث كلاً من CNN و BiLSTM حيث يجمع هذا الدمج بين القوة المكانية ل CNN والعمق الزمني BiLSTM، بالإضافة إلى آلية الانتباه متعددة الرؤوس Multi Head Attention. مما يمنح النموذج قدرة فائقة على التمييز بين الحركة الطبيعية وحركة الهجوم حتى في حالات التخفي، ويساهم بفاعلية في تقليل الإنذارات الكاذبة. يوضح الشكل (3) معمارية النموذج المقترح.



الشكل (3): معمارية النموذج المقترح

يتكون دخل النموذج من متجه ميزات أحادي البعد بحجم (40,1)، والذي يمثل الخصائص المختارة لتدفقات الشبكة. في المرحلة الأولى، يستخدم النموذج طبقة التفاف أحادية البعد (Conv1D) تحتوي على 64 مرشحاً (Filters) وبحجم نواة (Kernel Size) يساوي 3. تعمل هذه الطبقة على استخراج الأنماط المحلية من خلال تعلم العلاقات المكانية بين الميزات المتجاورة. بعد ذلك، يتم تمرير المخرجات

نموذج هجين للتعلم العميق المكاني-الزماني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات المعرفة برمجياً

إلى طبقة MaxPooling1D بحجم تجميع يساوي 2، مما يؤدي إلى تقليل الأبعاد من 40 إلى 20 مع الحفاظ على أهم الميزات.

بعد ذلك، يتم إدخال التمثيل المختزل إلى طبقة Bidirectional LSTM التي تحتوي على 192 وحدة. تقوم هذه الطبقة بمعالجة البيانات في الاتجاهين الأمامي والخلفي، مما يسمح للنموذج بالنقاط الاعتماديات طويلة المدى والتفاعلات المعقدة بين الميزات. تم الاحتفاظ بكامل التسلسل الزمني وليس آخر حالة فقط، وهذا ضروري لأن طبقة Attention اللاحقة تحتاج إلى جميع الحالات المخفية لتقييم أهمية كل جزء من التسلسل.

تم تطبيق آلية الانتباه متعددة الرؤوس حيث يقوم النموذج بتوزيع الانتباه على ثمانية رؤوس مستقلة، وكل رأس يتعلم نمطاً مختلفاً من الاعتماد داخل التسلسل. الفكرة الأساسية هنا أن الهجمات، خاصة Low-Rate DDOS، لا تكون دائماً واضحة في كل جزء من التدفق، بل قد تظهر على شكل تغيرات دقيقة ومتباعدة. لذلك، فإن attention يسمح للنموذج بإعطاء وزن أكبر للأجزاء الأكثر دلالة في التسلسل.

للمحد من مشكلة فرط التكيف (Overfitting)، تم استخدام طبقة Dropout بنسبة 0.2. وأخيراً، يتم استخدام طبقة (Dense) متصلة بالكامل مع دالة تفعيل Softmax لإنتاج توزيع احتمالي على أربع فئات (Low-Rate DOS، High-Rate DOS، DDOS، BENIGN).

تم استخدام Bayesian Optimization لتحسين أداء النموذج وضبط أفضل القيم الممكنة للمعاملات الفائقة (Hyperparameters) مثل: (عدد المرشحات في CNN، وعدد الوحدات في BiLSTM، ومعدل الإسقاط Dropout، ومعدل التعلم Learning Rate). يوضح الجدول (11) قيم المعاملات الفائقة للنموذج المقترح والتي تساهم في تحقيق أفضل أداء للنموذج

الجدول (11): المعاملات الفائقة للنموذج باستخدام Bayesian Optimization

Hyperparameter	Value
CNN conv_filters_1	64
CNN Activation Function	ReLU
Number of heads	8

Optimization Function	Adam
Epochs	60
Learning Rate	0.0005
Batch Size	128
BiLSTM Units	192
Dropout Rate	0.2

9. الخاتمة

في هذه الدراسة، تم تناول واحدة من أبرز المشكلات التي تواجه أنظمة كشف التسلل الحديثة ضمن بيئات الشبكات المعرفة برمجياً (SDN)، والمتمثلة في صعوبة التمييز الدقيق بين حركة المرور الطبيعية والهجمات السيبرانية، لا سيما هجمات (DOS/DDOS) ذات المعدلات العالية والمنخفضة. اقترح البحث نموذجاً هجيناً يعتمد على دمج الشبكات الانتقافية (CNN) لاستخراج الأنماط المكانية من بيانات المرور الشبكي، وشبكات الذاكرة طويلة وقصيرة المدى ثنائية الاتجاه (BiLSTM) لالتقاط الاعتمادية الزمنية وتسلسل الأحداث، مع إضافة طبقة Attention للنموذج لتساهم في التركيز على الميزات الأكثر تمييزاً في الهجمات الخفية Low-Rate DOS. وقد ساهم هذا الدمج في بناء إطار كشف قوي قادر على تمثيل خصائص البيانات الشبكية بصورة أكثر شمولية ودقة.

أظهرت النتائج أن نموذج CNN عانى من محدودية في تمثيل العلاقات الزمنية والسياقية (Contextual)، وهو ما انعكس في انخفاض أدائه مقارنة بالنماذج العميقة الأخرى، خاصة في High-Rate DOS و Low-Rate DOS في المقابل، حسن BiLSTM الأداء بشكل ملحوظ من خلال قدرته على نمذجة الاعتماديات التسلسلية، حيث ارتفع F1-score في High-Rate DOS من (96.83) إلى (99.65)، وفي Low-Rate DOS من (97.18) إلى (99.19). بالنسبة لنموذج CNN-BiLSTM فقد حقق توازناً أفضل بين الكفاءة والأداء، حيث جمع بين قدرة CNN على استخراج الخصائص المكانية المحلية وقدرة BiLSTM على تمثيل السلوك الزمني للتدفقات الشبكية. وقد أدى هذا الدمج إلى رفع الأداء التصنيفي إلى (99.78) مع تقليل زمن التدريب إلى (540 دقيقة)، وهو أقل بكثير من نموذج BiLSTM.

حقق نموذج CNN-BiLSTM-MultiAtt أعلى أداء بين جميع النماذج (99.93)، مما يدل على فعالية آلية Multi-Head Attention في تحسين التركيز على الأنماط الخفية والاعتماديات الزمنية الدقيقة المرتبطة بالهجمات ذات السلوك المتخفي. إلا أن هذا التحسن ترافق مع أعلى كلفة حسابية، حيث ارتفع عدد المعاملات إلى (593924)، إضافة إلى زيادة زمن التدريب إلى (1246 دقيقة). ويعود ذلك إلى أن طبقة Attention تضيف إسقاطات خطية متعددة، فضلاً عن الاحتفاظ بالتسلسل الكامل للمخرجات الزمنية من BiLSTM، مما يزيد من حجم التمثيلات الوسيطة والعمليات الحسابية أثناء التدريب.

وفقاً لما سبق يوصي البحث بما يأتي:

1. اعتماد النموذج CNN-BiLSTM كخط كشف أولي، ثم تفعيل Attention بشكل انتقائي فقط عند الحاجة. هذا مهم جداً لأن النتائج أظهرت أن Attention يرفع الأداء، لكنه يزيد الكلفة. لذلك يمكن جعل CNN-BiLSTM مرحلة أولى سريعة، ثم تمرير فقط التدفقات المشبوهة أو منخفضة الثقة إلى CNN-BiLSTM-MultiAtt.
 2. اعتماد بنية IDS هرمية، حيث يعمل النموذج الهجين CNN-BiLSTM كمرحلة فرز أولى، بينما يُخصص النموذج المقترح المعزز بالانتباه لمعالجة التدفقات ذات السلوك الخفي أو منخفضة الثقة، بما يحقق أفضل توازن بين سرعة الاستجابة ودقة الكشف.
 3. التأكيد على أن كشف هجمات رفض الخدمة منخفضة المعدل يحتاج نماذج زمنية وسياقية (Contextual)، النتائج أوضحت أن هذا النوع من الهجمات هو الأصعب، وأن النماذج التي تتعامل مع الاعتماديات الزمنية مثل BiLSTM والهجينة كانت الأفضل. لذلك يُنصح على أن الهجمات منخفضة المعدل لا تكفي معها الخصائص المحلية فقط.
- وفي الأعمال المستقبلية، يمكن توسيع النموذج المقترح من خلال اختباره على مجموعات بيانات إضافية، وتحسين كفاءة التنفيذ في الزمن الحقيقي، إضافة إلى دمجها ضمن وحدات التحكم في SDN لتوفير نظام كشف واستجابة أكثر ذكاءً وتكيفاً مع التهديدات المستجدة.

- [1] S. Batool, M. Aslam, and E. Akpokodje, 'A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives', *Electron.* 2025, 2025, doi: <https://doi.org/10.3390/electronics14214222>.
- [2] J. Singh and S. Behal, 'Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions', *Comput. Sci. Rev.*, vol. 37, p. 100279, Aug. 2020, doi: 10.1016/j.cosrev.2020.100279.
- [3] A. Jain, H. Shukla, and D. Goel, 'A comprehensive survey on DDoS detection, mitigation, and defense strategies in software-defined networks', *Clust. Comput.*, vol. 27, pp. 13129–13164, Jun. 2024, doi: 10.1007/s10586-024-04596-z.
- [4] A. Najar and M. Naik S, 'DDoS attack detection using CNN-BiLSTM with attention mechanism', *Telemat. Inform. Rep.*, vol. 18, p. 100211, May 2025, doi: 10.1016/j.teler.2025.100211.
- [5] N. McKeown *et al.*, 'OpenFlow: enabling innovation in campus networks', *SIGCOMM Comput Commun Rev*, vol. 38, no. 2, pp. 69–74, Mar. 2008, doi: 10.1145/1355734.1355746.
- [6] Y. Zhang, L. Cui, W. Wang, and Y. Zhang, 'A survey on software defined networking with multiple controllers', *J. Netw. Comput. Appl.*, vol. 103, pp. 101–118, Feb. 2018, doi: 10.1016/j.jnca.2017.11.015.
- [7] T. M. Mitchell, *Machine Learning*. McGraw-Hill Science/Engineering/Math, 1997.
- [8] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, 'Deep learning approach for Network Intrusion Detection in Software Defined Networking', in *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Oct. 2016, pp. 258–263. doi: 10.1109/WINCOM.2016.7777224.
- [9] R. Sommer and V. Paxson, 'Outside the Closed World: On Using Machine Learning for Network Intrusion Detection', in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 305–316. doi: 10.1109/SP.2010.25.
- [10] A. Kuzmanovic and E. W. Knightly, 'Low-rate TCP-targeted denial of service attacks and counter strategies', *IEEEACM Trans. Netw.*, vol. 14, no. 4, pp. 683–696, Aug. 2006, doi: 10.1109/TNET.2006.880180.

-
- [11] Y. LeCun, Y. Bengio, and G. Hinton, 'Deep learning', *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
- [12] A. Casolaro, V. Capone, G. Iannuzzo, and F. Camastra, 'Deep Learning for Time Series Forecasting: Advances and Open Problems', *Information*, vol. 14, no. 11, p. 598, Nov. 2023, doi: 10.3390/info14110598.
- [13] 'Download Anaconda Distribution', Anaconda. Accessed: Jan. 29, 2026. [Online]. Available: <https://www.anaconda.com/download>
- [14] 'Microsoft Visio - Download'. Accessed: Jan. 29, 2026. [Online]. Available: <https://microsoft-visio.en.softonic.com/>
- [15] 'Optimization System Based on Convolutional Neural Network and Internet of Medical Things for Early Diagnosis of Lung Cancer'. Accessed: Jan. 29, 2026. [Online]. Available: <https://www.mdpi.com/2306-5354/10/3/320>
- [16] A. A. Najar and S. Manohar Naik, 'DDoS attack detection using CNN-BiLSTM with attention mechanism', *Telemat. Inform. Rep.*, vol. 18, p. 100211, Jun. 2025, doi: 10.1016/j.teler.2025.100211.
- [17] A. M. Elshewey, S. Abbas, A. M. Osman, E. A. Aldakheel, and Y. Fouad, 'DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network', *Sci. Rep.*, vol. 15, no. 1, p. 29122, Aug. 2025, doi: 10.1038/s41598-025-13754-1.
- [18] A. al-zubidi, A. Farhan, and S. Towfek, 'Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model', *J. Intell. Syst.*, vol. 33, Apr. 2024, doi: 10.1515/jisys-2023-0195.
- [19] J. Zhao, Y. Liu, Q. Zhang, and X. Zheng, 'CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM', *IEEE Access*, vol. 11, pp. 136308–136317, 2023, doi: 10.1109/ACCESS.2023.3334916.
- [20] M. V. O. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença, 'A GRU deep learning system against attacks in software defined networks', *J. Netw. Comput. Appl.*, vol. 177, p. 102942, Mar. 2021, doi: 10.1016/j.jnca.2020.102942.
- [21] Mohamed. Abdisalam, CSE-CIC-IDS2018, doi: 10.17632/29hdbdxx2r.1, accessed: 2026-02-08, url: <https://data.mendeley.com/datasets/29hdbdxx2r/1>
- [22] Network Intrusion dataset (CIC-IDS- 2017), accessed: 2026-02-08, url: <https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset>

- [23] A. Lara, A. Kolasani, and B. Ramamurthy, "Network Innovation using OpenFlow: A Survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 493–512, 2014.
- [24] 'DDoS threat report for 2025 Q4 | Cloudflare Radar'. Accessed: May 16, 2026. [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q4?utm_source=chatgpt.com
- [25] '(PDF) When SDN Meets Low-rate Threats: A Survey of Attacks and Countermeasures in Programmable Networks', ResearchGate, Jan. 2026, doi: 10.1145/3704434.
- [26] 'compute_class_weight', scikit-learn. Accessed: Jun. 09, 2026. [Online]. Available: https://scikit-learn/stable/modules/generated/sklearn.utils.class_weight.compute_class_weight.html
- [27] معاينة كشف هجمات حجب الخدمة الموزعة على الشبكات المعرفة برمجياً باستخدام التعلم العميق'. Accessed: Jun. 14, 2026. [Online]. Available: <https://journal.homs-univ.edu.sy/index.php/Engineering/article/view/8370/3630>
- [28] معاينة تحديد عتبة التصنيف المثلى ديناميكياً في أنظمة الكشف المبكر عن الشذوذ القائمة على التعلم العميق'. Accessed: Jun. 14, 2026. [Online]. Available: <https://journal.homs-univ.edu.sy/index.php/Engineering/article/view/1112/1044>

نموذج هجين للتعلم العميق المكاني-الزماني للكشف عن هجمات رفض الخدمة منخفضة وعالية المعدل في الشبكات
المعرفة برمجياً
