Comprehensive Journal of Science
Volume (10), Issue (39), (March, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) ملحق العدد 39 مارس 2026
ردمد: 3014-6266

كشف هجمات حجب الخدمة الموزعة (DDoS) باستخدام نماذج التعلم العميق

الهام يخلف أبوالشواشي
قسم التقنية الالكترونية - كلية التقنية الهندسية زوارة – ليبيا

Detecting Distributed Denial-of-Service (DDoS) Attacks Using Deep Learning Models

Imam Khalaf Abushawashi
Department of Electronic Technology - Faculty of Engineering Technology, Zuwarah – Libya
elham_abuelshwashi@yahoo.com

تاريخ الاستلام:2026/02/11 –تاريخ المراجعة:2026/03/12– تاريخ القبول: 2026/03/13– تاريخ للنشر 2026/04/22

الملخص

تعد هجمات حجب الخدمة الموزعة (Distributed Denial of Service – DDoS) من أخطر التهديدات الأمنية التي تواجه الشبكات الحاسوبية في الوقت الحالي، لما تسببه من تعطيل للخدمات وخسائر تقنية واقتصادية جسيمة. واستنزاف لموارد الشبكة. هناك عدة طرق مستخدمة للكشف عن هذه الهجمات تعتمد هذه الطرق على التواقيع او القواعد الثابتة أو أساليب إحصائية محدودة، مما يقلل من قدرتها على اكتشاف الهجمات الحديثة والمعقدة ذات الأنماط المتغيرة.

يهدف هذا البحث إلى تقديم نهج ذكي لكشف هجمات DDoS بالاعتماد على نماذج التعلم العميق، من خلال تحليل خصائص حركة مرور الشبكة واستخلاص الأنماط الخبيثة بدقة عالية. تم استخدام نموذج الشبكة العصبية العميقة DNN ونموذج الشبكة العصبية المتكررة من نوع الذاكرة طويلة وقصيرة المدى LSTM كما تم استخدام مجموعة بيانات معيارية معتمدة في مجال أمن الشبكات، مع تطبيق عدد من خطوات المعالجة المسبقة، شملت تنظيف البيانات وتطبيعها واختيار الخصائص الأكثر تأثيرًا. ثم جرى تدريب وتقييم النموذجين، ومقارنتهما باستخدام مقاييس تقييم معيارية مثل الدقة، والاستدعاء، ومعدل الإنذارات الخاطئة.

أظهرت النتائج تفوق نموذج LSTM في كشف هجمات DDoS مقارنة بنموذج DNN، حيث حقق دقة أعلى وانخفاضًا في معدلات الإنذارات الخاطئة. تؤكد هذه النتائج فاعلية استخدام التعلم العميق في تعزيز أنظمة كشف التسلل، وتبرز أهميته في دعم أمن الشبكات الحاسوبية ومواجهة التهديدات السيبرانية المتطورة.

الكلمات المفتاحية

أمن المعلومات،هجمات حجب الخدمة, هجمات حجب الخدمة الموزعة، كشف التسلل، التعلم العميق، أمن الشبكات، الشبكات العصبية، DNN، LSTM

1. المقدمة

شهدت الشبكات الحاسوبية تطورًا متسارعًا في السنوات الأخيرة، مما أدى إلى زيادة الاعتماد على الخدمات الرقمية في مختلف المجالات. ومع هذا التطور، برزت تهديدات أمنية متقدمة، وأصبحت الهجمات السيبرانية، وبالأخص هجمات حجب الخدمة الموزعة(DDoS) من أخطر التهديدات الأمنية التي تؤثر على توفر الخدمات واستقرار الأنظمة. تمثل هذه الهجمات تهديدا خطيرا لاستمرارية الاعمال والخدمات الرقمية.

تعتمد الأساليب التقليدية في الكشف عن هذه الهجمات على قواعد ثابتة أو تواقيع معروفة، ومع تطور هذه الهجمات وتغيير أنماطها أصبحت الطرق التقليدية المستخدمة للكشف عن هذه الهجمات غير مجدية حيث تعتمد أنظمة الكشف التقليدية على قواعد ثابتة أو طرق إحصائية، مما يجعلها غير قادرة على اكتشاف الهجمات الحديثة والمعقدة.

ومع التطور في تقنيات الذكاء الاصطناعي برز التعلم الألي كحل فعال لبناء انظمة قادرة على الكشف الاستباقي لمثل هذه الهجمات عبر التعرف على الانماط غير الطبيعية في حركة المرور.

2. مشكلة البحث

تعاني أنظمة كشف التسلل التقليدية من:

- ضعف القدرة على اكتشاف هجمات DDoS المتطورة
- ارتفاع نسبة الإنذارات الخاطئة (False Positives)
- عدم التكيف مع أنماط الهجوم الجديدة

3. أهداف البحث

يهدف هذا البحث إلى:

1. تصميم نموذج تعلم عميق لاكتشاف هجمات.DDoS
2. تقليل معدل الإنذارات الخاطئة.
3. تحسين دقة الكشف في الزمن الحقيقي.
4. تقييم النموذج باستخدام بيانات حقيقية أو شبه حقيقية.

4. مفهوم هجمات حجب الخدمة

هجوم حجب الخدمة (DoS) هو نوع من الهجمات السـيبرانية يهدف إلى تعطيل أو إيقاف خدمة إلكترونية عن العمل من خلال اسـتهلاك موارد النظام المسـتهدف، مثل وحدة المعالجة المركزية(CPU) ، الذاكرة، عرض النطاق الترددي(Bandwidth) ، أو جداول الاتصال، مما يؤدي إلى منع المستخدمين الشرعيين من الوصول إلى الخدمة.

يعتمد هذا النوع من الهجمات عادةً على مصـدر واحد يقوم بإرسـال عدد كبير من الطلبات أو الحزم إلى الخادم المستهدف خلال فترة زمنية قصيرة، بحيث يعجز النظام عن معالجتها.

4.1 أنواع هجمات حجب الخدمة(DoS)

4.1.1 هجمات الإغراق بالحزم(Flooding Attacks)

تعتمد هذه الهجمات على إرسال عدد هائل من الحزم إلى النظام المستهدف ومن أنواعها:

✓ SYN Flood

- يستغل آلية المصافحة الثلاثية في بروتوكولTCP
- يرسل المهاجم طلبات اتصال دون إكمال المصافحة
- يؤدي إلى استنزاف جدول الاتصالات في الخادم

✓ ICMP Flood (Ping Flood)

- إرسال عدد كبير من رسائلICMP
- يؤدي إلى استهلاك عرض النطاق الترددي

4.1.2 هجمات استغلال البروتوكولات(Protocol Attacks)

تعتمد على استغلال نقاط الضعف في تصميم بروتوكولات الشبكة ومن أنواعها:

✓ **Smurf Attack**

- إرسال طلبات ICMP بعنوان مصدر مزيف
- تضخيم حجم الهجوم عبر شبكات وسيطة

✓ **Ping of Death**

- إرسال حزم ICMP أكبر من الحجم المسموح
- يؤدي إلى انهيار النظام أو إعادة تشغيله

4.1.3 هجمات الطبقة التطبيقية(Application Layer Attacks)

تستهدف تطبيقات الويب مباشرة ومن أنواعها:

✓ **HTTP Flood**

- إرسال طلبات HTTP مكثفة
- صعب التمييز بينها وبين المستخدمين الحقيقيين

5. مفهوم هجمات حجب الخدمة الموزع

هجوم حجب الخدمة الموزعة (DDoS) هو تطور لهجمات DoS ، حيث يتم تنفيذ الهجوم من خلال عدد كبير من الأجهزة المخترقة تعمل معًا في وقت واحد لاستهداف نظام معين. يتم التحكم في هذه الأجهزة عن بُعد عبر خادم تحكم مركزي وفي هذا النوع من الهجمات:

- يتم التحكم في آلاف أو ملايين الأجهزة المصابة
- تُرسل طلبات متزامنة إلى الهدف
- يصبح من الصعب التمييز بين المستخدم الحقيقي والمهاجم

5.1 آلية عمل هجماتDDoS

تمر هجمات DDoS بعدة مراحل رئيسية:

5.1.1 مرحلة الاختراق(Infection)

يقوم المهاجم بإصابة عدد كبير من الأجهزة ببرمجيات خبيثة.

5.1.2 مرحلة التحكم(Command & Control)

يتم ربط الأجهزة المصابة بخادم تحكم مركزي.

5.1.3 مرحلة الهجوم(Attack Launch)

يتم إرسال أوامر للأجهزة لشن الهجوم بشكل متزامن على الهدف.

5.2 أنواع هجمات حجب الخدمة الموزعة(DDoS)

يتم تصنيف هجمات DDoS بناءاعلى نوع وكمية حركة المرور المستخدمة للهجوم عليه يتم تصنيف هجمات DDoS الى ثلاث فئات

5.2.1 هجمات الحجم الكبير(Volumetric Attacks)

يستخدم هذا النوع من الهجمات كمية هائلة من حركة المرور تهدف إلى استهلاك عرض النطاق الترددي.. من السهل توليد الهجمات الحجمية من خالل استخدام تقنيات تضخيم بسيطة ومن أنواعها:

✓ **UDP Flood**

- إرسال حزم UDP عشوائية
- يؤدي إلى تشبع الشبكة

✓ **DNS Amplification**

- استغلال خوادم DNS مفتوحة
- تضخيم حجم الهجوم عدة مرات

5.2.2 هجمات استنزاف البروتوكولات(Protocol-based Attacks)

يجعل هذا النوع من الهجمات هدفا يمكن الوصــول إليه من خلال اســتغلال نقطة ضــعف في مكدس بروتوكول الطبقة الثالثة والرابعة ومن انواعها:

✓ **SYN Flood الموزع**

- آلاف الأجهزة تنفذ SYN Flood في وقت واحد

✓ **ACK Flood**

- إرسال حزم ACK غير متوقعة
- استنزاف موارد التحقق

5.2.3 هجمات طبقة التطبيقات(Application Layer DDoS)

يســتغل هذا النوع من الهجمات نقطة ضــعف في حزمة البروتوكولات. هذه الهجمات هي الهجوم الاكثر تعقيدا وهناك صعوبة للتخفيف من حدته ويعتبر أخطر أنواع هجمات حجب الخدمة الموزع ومن أنواعها:

✓ **HTTP GET/POST Flood**

- محاكاة سلوك المستخدم الحقيقي
- يصعب اكتشافها

✓ **Slowloris Attack**

- إبقاء الاتصالات مفتوحة لأطول وقت ممكن
- استنزاف موارد الخادم تدريجيًا

5.3 الطرق التقليدية للحماية من هجمات حجب الخدمة(DoS/DDoS)

5.3.1 التصفية المعتمدة على القواعد

تعتمد هذه الطريقة على تحديد قواعد ثابتة لتصفية حركة المرور الشبكية، مثل:

- حظر عناوين IP المشبوهة
- تحديد حد أعلى لعدد الطلبات في الثانية
- إسقاط الحزم غير المطابقة لمعايير معينة

هذه الطريقة سهلة التنفيذ ولكنها غير فعالة ضد الهجمات المتغيرة وتتطلب تحديثًا مستمرًا للقواعد

5.3.2 أنظمة كشف ومنع التسلل التقليدية(IDS/IPS)

تعتمد هذه الأنظمة على التواقيع(Signatures) وهي فعالة ضــد الهجمات المعروفة ويتم اســتخدامهاعلى نطاق واســع ولكنها:

- غير قادرة على كشف أنواع الهجمات الجديدة
- ارتفاع نسبة الإنذارات الخاطئة
- محدودية الأداء عند الهجمات الضخمة

5.3.3 تحديد المعدل

يتم فرض حد أقصى لعدد الطلبات القادمة من مصدر واحد خلال فترة زمنية معينة وهذا يمكن أن يقلل من الإغراق المفاجئ ولكنه لا يكون فعال ضد DDoS متعددة المصادر وأيضا يمكن أن يؤثر على المستخدمين الشرعيين.

6. حدود الطرق التقليدية

على الرغم من فعالية الأســـاليب التقليدية في الحد من بعض أنواع هجمات حجب الخدمة، إلا أنها تعاني من محدودية واضـحة في مواجهة الهجمات الموزعة والمتطورة، خصـوصًـا تلك التي تسـتهدف الطبقة التطبيقية, ضـعف في التكيف مع أنواع الهجمات الجديدة وصعوبة التمييز بين المستخدم الحقيقي والمهاجم الذكي لذلك، أصبح من الضروري تطوير حلول ذكية تعتمد على تقنيات التعلم الآلي والتعلم العميق القادرة على التكيف مع الأنماط المتغيرة لهجمات حجب الخدمة.

وانطلاقًا من هذه التحديات، تم اقتراح النموذج التجريبي في هذه الدراســة كبديل ذكي يعتمد على تقنيات التعلم العميق، بهدف الى تحليل حركة مرور الشــبكة بطريقة آلية واســتخلاص الأنماط الخفية التي يصــعب اكتشــافها باســتخدام القواعد التقليدية. ويتميز النموذج المقترح بقدرته على التعلم من البيانات مباشرة دون الحاجة إلى تعريف صـريح لقواعد أو تواقيع، مما يمنحه قابلية أعلى للتكيف مع التغيرات المستمرة في سلوك الهجمات.

7. الدراسات السابقة

1- دراسة (Ahmad et al., 2020)

قدمت هذه الدراسة نموذجًا قائمًا على الشبكات العصبية العميقة (DNN) للكشف عن هجمات DDoS باستخدام مجموعة بيانات .CICIDS2017 اعتمد الباحثون على تقنيات المعالجة المسـبقة للبيانات واختيار الخصـائص المهمة لتحسـين أداء النموذج .وأظهرت النتائج أن النموذج حقق دقة تجاوزت 98%، مع قدرة جيدة على التمييز بين حركة المرور الطبيعية والهجمات الخبيثة. وأشـارت الدراسـة إلى أن استخدام الشبكات العصـبية العميقة يسـاعد في استخراج الأنماط المعقدة داخل البيانات الشبكية وتحسين كفاءة أنظمة كشف التسلل.

2- دراسة(Kim et al., 2021)

ركزت هذه الدراســة على اسـتخدام نموذج الذاكرة طويلة وقصـيرة المدى (LSTM) للكشـف عن هجمات DDoS داخل شـبكات إنترنت الأشـياء .(IoT) اعتمدت الدراســة على تحليل التسـلسـل الزمني لحركة المرور الشـبكية، حيث تم تدريب نموذج LSTM على بيانات شــبكية متدفقة تحتوي على أنماط هجومية مختلفة .وأظهرت النتائج أن نموذج LSTM حقق أداءً مرتفعًا في اكتشــاف الهجمات مقارنةً بالنماذج التقليدية، وذلك بســبب قدرته على الاحتفاظ بالمعلومات الزمنية وتحليل العلاقات المتتابعة داخل البيانات.

3- دراسة(Vinayakumar et al., 2019)

هدفت هذه الدراسة إلى مقارنة عدة نماذج من التعلم العميق في مجال كشف التسلل، مثل:

- DNN
- CNN
- LSTM

واستخدم الباحثون مجموعة بيانات CICIDS2017 لتقييم أداء النماذج المختلفة .وأظهرت النتائج أن نموذج LSTM حقق نتائج أفضـل في التعامل مع البيانات الزمنية، بينما أظهر نموذج DNN سـرعة أكبر في التدريب والتنفيذ .وأكدت الدراسـة أن اختيار النموذج المناسب يعتمد على طبيعة البيانات وحجمها ونوع الهجمات المستهدفة.

8. الجانب العملي

8.1 مجموعة البيانات(Dataset)

تم الاعتماد في هذه الدراسة على مجموعة بيانات واقعية تُعرف باسم **CICIDS2017**، والتي تُعد من أشهر قواعد البيانات المستخدمة في أبحاث الأمن السيبراني. حيث تحتوي مجموعة البيانات على حركة مرور شبكية حقيقية تشمل عدة أنواع من الهجمات :

- DDoS
- DoS
- Brute Force
- Port Scan

وتتضمن عددًا كبيرًا من السمات (Features) التي تصف خصائص حركة الشبكة الموضحة بالجدول (8.1).

جدول 8.1 خصائص البيانات

الخاصية (Feature)	الوصف
Flow Duration	مدة الاتصال
Total Fwd packets	عدد الحزم المرسلة
Total Backward packets	عدد الحزم المستلمة
Flow Bytes/s	معدل نقل البيانات
Flow Packets/s	معدل الحزم
Packet Length Mean	متوسط طول الحزمة
Packet Length Std	الانحراف المعياري
SYN Flag Count	عدد إشاراتSYN
ACK Flag Count	عدد إشاراتACK
Idle Mean	متوسط زمن الخمول
Active Mean	متوسط زمن النشاط

8.2 بيئة التنفيذ والأدوات المستخدمة

تم تنفيذ الجانب العملي باستخدام لغة البرمجة Python لما توفره من مكتبات متخصصة في مجالات التعلم العميق وتحليل البيانات. وقد تم الاعتماد على عدد من المكتبات العلمية القياسية، من أبرزها:

- مكتبة NumPy لتنفيذ العمليات الرياضية ومعالجة البيانات العددية.
- مكتبة Pandas لتنظيم البيانات والتعامل معها في شكل جداول.
- مكتبة Scikit-learn لتنفيذ عمليات تقسيم البيانات وحساب مؤشرات الأداء.
- مكتبة TensorFlow / Keras لبناء وتدريب نموذج الشبكة العصبية العميقة.
- مكتبة Matplotlib لتمثيل النتائج بيانيًا عند الحاجة.

وقد تم تنفيذ جميع التجارب على حاسوب شخصي يعمل بنظام تشغيلWindows ، دون الحاجة إلى بنية حوسبية متقدمة، مما يعزز قابلية إعادة تطبيق التجربة.

8.3 المعالجة المسبقة للبيانات(Data Preprocessing)

تُعد مرحلة المعالجة المسبقة من أهم المراحل في بناء نموذج تعلم عميق فعال، حيث تؤثر بشكل مباشر على جودة النتائج.

8.3.1 تنظيف البيانات

- إزالة القيم المفقودة (Missing Values)
- حذف السجلات غير الصالحة

8.3.2 تحويل البيانات

- تحويل القيم النصية إلى رقمية (Encoding)
- تصنيف البيانات إلى :
  - ✓ 0 بيانات طبيعية (Benign)
  - ✓ 1 هجوم (Attack)

8.3.3 تطبيع البيانات(Normalization)

تم استخدام تقنية StandardScalerلتوحيد نطاق القيم، مما يساعد على تحسين سرعة ودقة التدريب.

8.3.4 تقسيم البيانات

تم تقسيم البيانات إلى:

- 80%بيانات تدريب (Training Set)
- 20%بيانات اختبار(Testing Set)

8.4 تصميم الدراسة

تعتمد هذه الدراسة على استخدام نموذجين من نماذج التعلم العميق، الشبكة العصبية العميقة (Deep Neural Network - DNN) والشبكة العصبية المتكررة من نوع الذاكرة طويلة وقصيرة المدى (Long Short-Term Memory - LSTM). يُستخدم نموذج DNNلاستخلاص الأنماط من البيانات الثابتة، بينما يتميز نموذج LSTM بقدرته على معالجة البيانات الزمنية وتحليل التسلسل الزمني لحركة المرور الشبكية، مما يجعله أكثر كفاءة في كشف هجمات حجب الخدمة الموزعة.(DDoS) . تم تدريب كلا النموذجين على نفس مجموعة البيانات لضمان عدالة المقارنة، مع استخدام نفس خطوات المعالجة المسبقة.

8.4.1 نموذج الشبكة العصبية العميقة (Deep Neural Network – DNN)

يتكون هذا النموذج من عدة طبقات متصلة بالكامل(Fully Connected Layers) ، حيث يتم تمرير البيانات عبر هذه الطبقات لاستخلاص الأنماط.

- طبقة إدخال
- ثلاث طبقات مخفية باستخدام دالة تنشيط ReLU
- طبقة إخراج باستخدام Sigmoid

8.4.2 نموذج الشبكة العصبية المتكررة من نوع الذاكرة طويلة وقصيرة المدى – Long Short-Term Memory (LSTM)

يعد نموذج LSTM من النماذج المتقدمة القادرة على التعامل مع البيانات الزمنية، وهو مناســـب لتحليل حركة المرور الشبكية. حيث لديه القدرة على حفظ المعلومات السابقة وتحليل التسلسل الزمني للبيانات وتحسين دقة الكشف ويتكون من:

- طبقة LSTM أولى (64 وحدة)
- طبقة Dropout لتقليل الإفراط في التعلم (Overfitting)
- طبقة LSTM ثانية (32 وحدة)
- طبقة كثيفة (Dense)
- طبقة إخراج

9. تقييم الأداء

بعد الانتهاء من مرحلة التدريب، تم تقييم أداء النموذج باستخدام مجموعة الاختبار غير المستخدمة في التدريب. وقد تم الاعتماد على مجموعة من المقاييس الإحصائية الشائعة في مجال كشف التسلل، وتُعد هذه المقاييس معيارًا معتمدًا في تقييم أنظمة كشف التسلل، حيث توازن بين دقة الكشف وتقليل الإنذارات الخاطئة وهي:

9.1 الدقة الكلية(Accuracy)

تشـير الدقة الكلية إلى نسـبة العينات التي تم تصـنيفها بشـكل صـحيح من إجمالي العينات. أي كم مرة كان قرار النموذج صـــحيحًا مقارنة بجميع القرارات التي اتخذها وعلى الرغم من أهميتها كمؤشـــر عام لأداء النموذج، إلا أنها لا تُعد كافية بمفردها في تقييم أنظمة كشـــف هجمات حجب الخدمة الموزعة، نظرًا لاحتمالية عدم توازن البيانات وخطورة حالات عدم اكتشاف الهجوم.

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN}$$

9.2 الدقة النوعية(Precision)

تمثل الدقة النوعية نسـبة الهجمات الحقيقية من إجمالي الحالات التي صـنفها النموذج كهجمات. وتُعد مؤشـرًا على موثوقية إنذارات النظام، حيث يشـير انخفاضــها إلى ارتفاع معدل الإنذارات الكاذبة، وهو ما قد يؤثر سـلبًا على كفاءة أنظمة كشـف هجمات حجب الخدمة.

$$\boldsymbol{Precision = \frac{TP}{TP+FP}}$$

9.3 الاسترجاع(Recall)

يقيس الاسترجاع قدرة النموذج على اكتشاف الهجمات الفعلية من إجمالي الهجمات الموجودة في مجموعة البيانات، ويعكس كفاءة النظام في عدم تفويت الهجمات. وتشير قيمة الاسترجاع المتوسطة إلى أن النموذج تمكن من اكتشاف جزء معتبر من الهجمات، إلا أن نسبة غير قليلة منها ما زالت تمر دون كشف.

$$\boldsymbol{Recall = \frac{TP}{TP+FN}}$$

9.4 مقياسF1

يمثل مقياس F1-Score المتوسط التوافقي بين الدقة النوعية والاسترجاع، ويعد من أهم مؤشرات تقييم أداء نماذج كشـف هجمات حجب الخدمة الموزعة، خاصـــة في ظل عدم توازن البيانات. وتشـــير القيمة المحققة إلى أن النموذج يوفر توازنًا معقولًا بين اكتشاف الهجمات وتقليل الإنذارات الخاطئة.

$$\boldsymbol{F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}}$$

حيث أن :

- **TP (True Positive):** عدد الهجمات التي تم اكتشافها بشكل صحيح
- **TN (True Negative):** عدد البيانات الطبيعية المصنفة بشكل صحيح
- **FP (False Positive):** بيانات طبيعية تم تصنيفها كهجوم
- **FN (False Negative):** هجمات لم يتم اكتشافها

10 النتائج وتحليل الاداء

بعد الانتهاء من تدريب ;كلا النموذجين باستخدام مجموعة بيانات CICIDS2017 الخاصة بكشف هجمات حجب الخدمة الموزعة(DDoS) ، تم اختبار النموذجين على بيانات لم تُستخدم أثناء عملية التدريب بهدف تقييم قدرة هذه النماذج على التعميم وكفاءة الكشف عن الهجمات.

10.1 نتائج نموذج DNN

تم تدريب نموذج الشبكة العصبية العميقة (Deep Neural Network - DNN) باستخدام مجموعة بيانات CICIDS2017بهدف كشف هجمات حجب الخدمة الموزعة(DDoS) ، حيث تم إجراء المعالجة المسبقة للبيانات وتطبيع الخصائص قبل عملية التدريب. وبعد الانتهاء من تدريب النموذج واختباره، تم تقييم أدائه باستخدام مجموعة من المقاييس الإحصائية، وكانت النتائج كما موضحة بالجدول (10.1)

جدول 10.1 نتائج نموذج DNN

المقياس	القيمة
Accuracy	99.20%
Precision	99.40%
Recall	98.90%
F1-Score	99.10%

10.2 تحليل نتائج نموذج DNN

تشير النتائج السابقة إلى أن نموذج DNN حقق أداءً مرتفعًا في عملية تصنيف البيانات الشبكية، حيث بلغت الدقة الكلية حوالي:

Accuracy=99.20%

مما يدل على قدرة النموذج على التمييز بين حركة المرور الطبيعية والهجمات الإلكترونية بدرجة عالية من الكفاءة .كما حقق النموذج قيمة Precision مرتفعة بلغت:

Precision=99.40%

وهو ما يشير إلى انخفاض عدد الإنذارات الكاذبة التي يصدرها النظام أثناء عملية الكشف .أما قيمة الاسترجاع Recall فقد بلغت:

Recall=98.90%

مما يدل على قدرة النموذج على اكتشاف معظم الهجمات الموجودة داخل البيانات .في حين بلغت قيمة F1-Score حوالي:

F1=99.10%

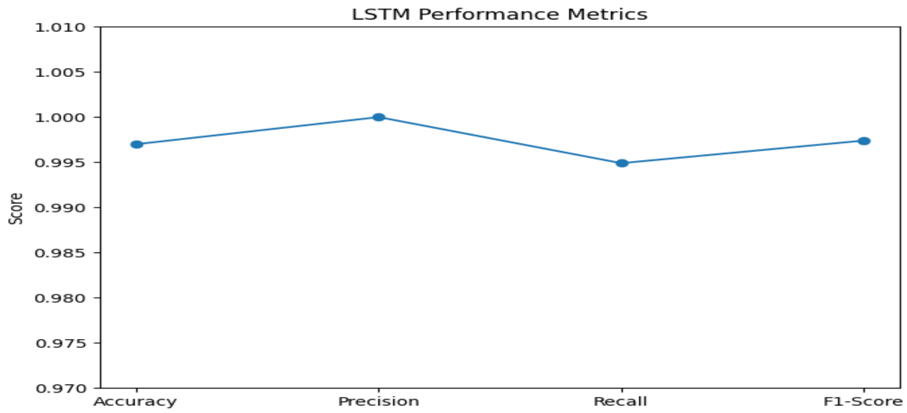
وهو ما يعكس وجود توازن جيد بين الدقة والاسترجاع. وتوضح هذه النتائج أن نموذج DNN يُعد نموذجًا فعالًا في كشف هجماتDDoS

10.3 نتائج نموذجLSTM

الجدول 10.2 يوضح قيم مقاييس الأداء الخاصة بالنموذج LSTM

جدول (10.2) نتائج نموذج LSTM

المقياس	القيمة
Accuracy	99.70%
Precision	100%
Recall	99.49%
F1-Score	99.74%



شكل 10.1 مقاييس أداء نموذجLSTM

يوضح الشكل السابق أداء نموذج الذاكرة طويلة وقصيرة المدى (LSTM) باستخدام مقاييس التقييم المختلفة، حيث حقق النموذج قيمًا مرتفعة جدًا في جميع المقاييس الإحصائية المستخدمة في الدراسة.

وقد بلغت الدقة الكلية (Accuracy) حوالي 99.70%، مما يدل على قدرة النموذج العالية في تصنيف حركة المرور الشبكية بصورة صحيحة. كما حقق النموذج قيمة Precision بلغت 100%، وهو ما يشير إلى انخفاض الإنذارات الكاذبة بشكل كبير.

كذلك أظهرت نتائج الاسترجاع (Recall) ومقياس F1-Score أداءً مرتفعًا، مما يؤكد كفاءة نموذج LSTM في اكتشاف هجمات DDoS وتحقيق توازن جيد بين دقة التصنيف واكتشاف الهجمات الفعلية.

10.4 تحليل النتائج LSTM

تشير النتائج السابقة إلى أن نموذج LSTM استطاع تحقيق كفاءة عالية جدًا في كشف هجماتDDoS ، ويُعزى ذلك إلى قدرة النموذج على تحليل الأنماط الزمنية لحركة المرور الشبكية والتعرف على السلوك غير الطبيعي داخل البيانات.

- ✓ **الدقة الكلية(Accuracy)**

حقّق النموذج دقة كلية بلغت 99.70، وهي نسبة مرتفعة تشير إلى نجاح النموذج في تصنيف معظم البيانات بشكل صحيح. ويعكس ذلك قدرة نموذج LSTM على تعلم الأنماط المعقدة الموجودة داخل البيانات الشبكية.

- ✓ **الدقة النوعية(Precision)**

بلغت قيمة الدقة النوعية 100%، مما يعني أن جميع الاتصالات التي صنفها النموذج كهجمات كانت بالفعل هجمات حقيقية، أي أن النموذج لم ينتج أي إنذارات كاذبة.(False Positives)

وتُعد هذه النتيجة مهمة جداً في أنظمة كشف التسلل، لأن تقليل الإنذارات الكاذبة يساعد في رفع كفاءة النظام وتقليل العبء على مسؤولي الشبكات.

- ✓ **الاسترجاع(Recall)**

حقق النموذج قيمة استرجاع بلغت 99.49%، مما يدل على قدرة عالية في اكتشاف الهجمات الفعلية وتقليل عدد الهجمات غير المكتشفة.

وتشير هذه النتيجة إلى كفاءة نموذج LSTM في تحليل التسلسل الزمني لحركة المرور الشبكية واكتشاف الأنماط المرتبطة بهجمات.DDoS

- ✓ **مقياسF1-Score**

بلغت قيمة F1-Score حوالي 99.74% وهي قيمة مرتفعة تعكس وجود توازن ممتاز بين الدقة النوعية والاسترجاع، مما يؤكد استقرار النموذج وكفاءته العالية في التصنيف.

10.5 تحليل مصفوفة الالتباس(Confusion Matrix)

كانت مصفوفة الالتباس للنموذج كما يلي:

$$\begin{bmatrix} 417 & 0 \\ 3 & 580 \end{bmatrix}$$

ويُفسَّر ذلك كما يلي:

- تم تصنيف 417 اتصالاً طبيعياً بشكل صحيح .
- تم اكتشاف 580 هجمة DDoS بشكل صحيح .
- لم يتم تسجيل أي إنذار كاذب .
- أخفق النموذج في اكتشاف 3 هجمات فقط .

وتؤكد هذه النتائج كفاءة النموذج المقترح في كشف هجمات DDoS بدقة مرتفعة جداً.

11 المقارنة

11.1 المقارنة بين نموذج DNN ونموذجLSTM

لإظهار كفاءة نماذج التعلم العميق في كشف هجمات حجب الخدمة الموزعة(DDoS) ، تم إجراء مقارنة بين نموذج الشبكة العصبية العميقة (DNN) ونموذج الذاكرة طويلة وقصيرة المدى (LSTM) باستخدام نفس مجموعة البيانات ونفس معايير التقييم.

أظهرت النتائج الموضـــحة في الجدول (11.1) أن كلا النموذجين حقق أداءً مرتفعًا في عملية التصـــنيف، إلا أن نموذج LSTMتفوق بشـكل طفيف على نموذج DNN في معظم المقاييس، ويرجع ذلك إلى قدرة LSTM على تحليل البيانات الزمنية والتسلسلات المتعاقبة لحركة المرور الشبكية، وهو ما يجعله أكثر ملاءمة لاكتشاف الأنماط الديناميكية المرتبطة بهجمات.DDoS

جدول (11.1) مقارنة نتائج DNN وLSTM

المقياس	DNN	LSTM
الدقة الكلية(Accuracy)	0.9920	0.9970
الدقة النوعية(Precision)	0.9940	1.0000
الاسترجاع(Recall)	0.9890	0.9949
مقياسF1	0.9910	0.9974

11.2 تحليل المقارنة

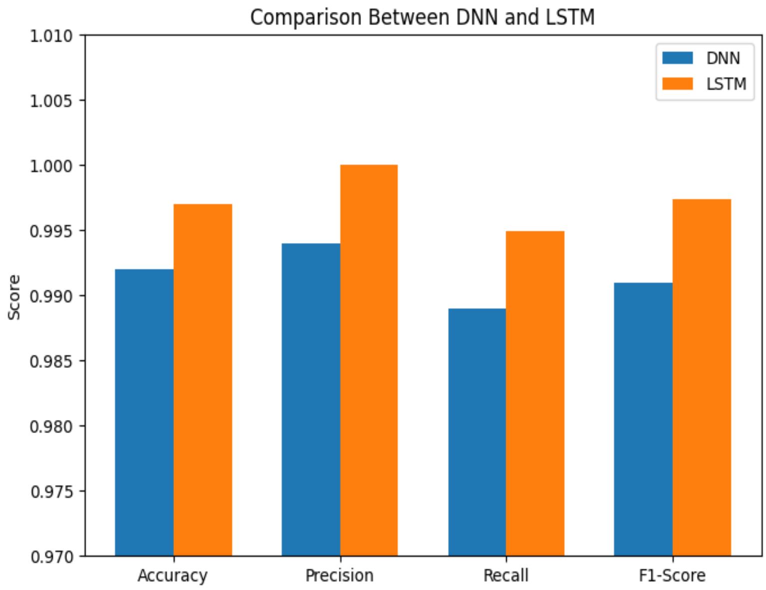
تشير النتائج الواردة في الجدول السابق إلى أن نموذج LSTM حقق أفضل أداء مقارنةً بنموذجDNN ، حيث بلغت الدقة الكلية للنموذج حوالي 99.70%، وهي نســبة مرتفعة تدل على قدرة النموذج على التمييز بين حركة المرور الطبيعية والهجمات الإلكترونية بكفاءة عالية.

كما حقق نموذج LSTM قيمة Precision بلغت 100%، مما يعني أن جميع العينات التي تم تصـنيفها كهجمات كانت صحيحة فعليًا، دون وجود إنذارات كاذبة تقريبًا، وهو أمر بالغ الأهمية في أنظمة كشف التسلل والشبكات الأمنية.

أما بالنسبة لمقياس Recall فقد بلغ 99.49%، مما يشير إلى قدرة النموذج على اكتشاف معظم الهجمات الموجودة داخل البيانات، مع فقدان عدد محدود جدًا من العينات الضارة. كذلك حقق النموذج قيمة F1-score مرتفعة بلغت 99.74%، مما يعكس التوازن الممتاز بين الدقة والاسترجاع.

في المقابل، حقق نموذج DNN نتائج جيدة أيضًـــا، إلا أن أداءه كان أقل قليلًا من نموذجLSTM ، ويرجع ذلك إلى أن DNNيعالج البيانات بصورة ثابتة دون الاستفادة الكاملة من العلاقات الزمنية بين الحزم الشبكية المتتابعة.

وبناءً على النتائج السـابقة، يمكن الاسـتنتاج أن نموذج LSTM يُعد أكثر كفاءة وملاءمة لكشـف هجمات DDoS مقارنةً بنموذجDNN ، خصوصًا في البيئات الشبكية التي تعتمد على تدفقات بيانات متسلسلة ومتغيرة مع الزمن.



شكل 11.1 مقارنة أداء نموذج DNN ونموذج LSTM

12 الخلاصة

تناولت هذه الدراسـة تطوير نموذج ذكي للكشـف عن هجمات حجب الخدمة الموزعة (DDoS) اعتمادًا على تقنيات التعلم العميق، وذلك من خلال بناء إطار تجريبي قائم على مقارنة أداء نموذجين رئيسيين هما الشبكة العصـبية العميقة (DNN)

والشبكة العصبية المتكررة .(LSTM) وقد تم استخدام مجموعة بيانات واقعية (CICIDS2017) مع تطبيق مجموعة متكاملة من خطوات المعالجة المسبقة، شملت تنظيف البيانات، وتحويلها، وتطبيعها، وتقسيمها إلى بيانات تدريب واختبار .
أظهرت النتائج النموذج LSTM حقق نتائج متقدمة على نموذج DNN في جميع مقاييس التقييم المعتمدة، بما في ذلك الدقة الكلية، والدقة النوعية، والاسترجاع، ومعاملF1 ، مما يعكس كفاءة عالية في اكتشاف الهجمات وتقليل الأخطاء .
وتبرز هذه النتائج أهمية اعتماد النماذج القائمة على تحليل التسلسل الزمني في معالجة بيانات الشبكات، لما لها من قدرة على التقاط الأنماط الديناميكية المعقدة المرتبطة بسلوك الهجمات الإلكترونية.

13 الخاتمة

خلصت هذه الدراسة إلى أن تقنيات التعلم العميق تمثل أحد أهم الاتجاهات الحديثة في مجال الأمن السيبراني، خاصة في كشف هجمات حجب الخدمة الموزعة .(DDoS) وقد أثبت نموذج LSTM تفوقه الواضح على نموذجDNN ، وذلك بفضل قدرته على تحليل البيانات الزمنية واستيعاب العلاقات المتتابعة بين الأحداث داخل حركة المرور الشبكية .
كما أظهرت النتائج أن جودة البيانات وفعالية مراحل المعالجة المسبقة تلعب دورًا حاسمًا في تحسين أداء النماذج، إلى جانب أهمية اختيار الخصائص المناسبة وبنية النموذج الملائمة.
وبناءً على ذلك، يمكن التأكيد على أن دمج نماذج التعلم العميق، وخاصة النماذج الزمنية، في أنظمة كشف التسلل يسهم بشكل فعّال في تعزيز أمن الشبكات، ورفع كفاءة الأنظمة الدفاعية في مواجهة التهديدات السيبرانية المتزايدة.

14 المراجع

1. عبد الله، محمد أحمد.(2021) "استخدام تقنيات التعلم العميق في كشف الهجمات السيبرانية"، *المجلة العربية لتقنية المعلومات* .
2. الحربي، خالد بن سعود.(2020) "أمن الشبكات وهجمات حجب الخدمة"، دار النشر الأكاديمي .
3. عمر سلام، "تحسين كشف وتخفيف هجمات DDoS باستخدام تقنيات التعلم العميق"، رسالة ماجستير، جامعة ديالى، العراق، 2024 .
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
5. S. M. Mousavi and M. St-Hilaire (2018). "Early detection of DDoS attacks against SDN controllers using machine learning techniques," *Journal of Network and Computer Applications*, 104, 61–74.
6. M. Roopak, G. Y. Tian, and J. Chambers (2019). "Deep learning models for cyber security in IoT networks," *IEEE Access*, 7, 47374–47384.
7. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), pp. 108–116, 2018.
8. M. Ahmad, A. Shahid, and S. Khan, "Deep Neural Network Based DDoS Detection System Using CICIDS2017 Dataset," International Journal of Computer Networks and Communications, vol. 12, no. 4, pp. 55–67, 2020.
9. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
10. J. Kim, H. Kim, and M. Shim, "LSTM-Based DDoS Detection for IoT Networks," Journal of Information Security and Applications, vol. 58, pp. 102–115, 2021.
11. R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating Deep Learning Approaches for Network Intrusion Detection Systems," IEEE Access, vol. 7, pp. 41520–41535, 2019.