تصميم نظام كشف تسلل شبكي باستخدام الشبكات العصبونية العميقة المعقدة

طالب الماجستير: م. ملك فيتروني كلية الهمك – جامعة البعث

اشراف الدكتور: بسيم عمران

ملخص البحث:

مع التطور العلمي الهائل في مختلف المجالات العلمية والصناعية، ونتيجة لاستخدام الشبكات بمختلف أنواعها (حاسوبية – الاتصالات والمعلومات)، ومن أجل حماية هذه الشبكات من الاختراقات، بدأت الدراسات العلمية لكشف التسلل بمختلف أنواعه. في هذا البحث: 1- تم تصميم نظام كشف تسلل شبكي جديد باستخدام الشبكات العصبونية العميقة المعقدة قادراً على اكتشاف الهجمات السيبرانية، 2- كما تم تدريبه واختباره على مجموعة البيانات المعيارية KDDCUP99 على برنامج **pycharm**،3- وتم الحصول على نتائج جيدة، 4- إذ تمت مقارنته مع طرائق كشف التسلل باستخدام الشبكات العصبونية العميقة المشابهة وخوارزميات التعلم الآلي التقليدية.

الكلمات المفتاحية

الأمن السيبراني، نظام كشف التسلل، الشبكات العصبونية العميقة المعقدة، التعلم العميق، مجموعة البيانات KDDCUP99، الشبكة الحاسوبية.

Design of a Network Intrusion Detection System Using Complex Deep Neuronal Networks

D. Basim Oumran Malak Fetaroni

Abstract:

With the tremendous scientific development in various scientific and industrial fields, and as a result of the use of networks of various kinds (computer - communications and information), and in order to protect these networks from penetrations, scientific studies began to detect intrusion of all types. In this research: 1- a new network intrusion detection system has been designed using complex deep neuronal networks capable of detecting cyber-attacks, 2- and it is also trained and tested on the standard dataset KDDCUP99 on pycharm program, 3- good results were obtained, 4- as it was compared with intrusion detection methods using similar deep neuronal networks and traditional machine learning algorithms.

Keywords: Cyber Security, Intrusion Detection System, complex Deep Neural Networks, Deep Learning, KDDCUP99 dataset, Computer Network.

1. مقدمة:

تتعامل شبكات تكنولوجيا المعلومات والاتصالات وأنظمتها مع مختلف بيانات المستخدمين المعرضة لهجمات مختلفة من المتطفلين الداخليين والخارجيين [2]. يمكن أن تكون هذه الهجمات يدوية أو آلية، ولكنها متنوعة، إذ تتطور باستمرار مع تقدم الأجهزة والبرامج وهياكل الشبكات. تطلق الهجمات السيبرانية الخبيثة مشكلات أمنية خطيرة تتطلب الحاجة إلى نظام كشف تسلل Intrusion Detection System (IDS) مرن وموثوق به [2]. يعد IDS تقنية مستخدمة على نطاق واسع للكشف عن التدخلات الداخلية والخارجية التي تستهدف نظامنا، وكذلك الحالات الشاذة. يتضمن نظام IDS مجموعة من الأدوات والآليات لمراقبة نظام الحاسوب وحركة مرور الشبكة. تستخدم تقنيات مختلفة للكشف عن الحالات الشاذة، وفي السنوات الثلاثة الأخيرة تم التحقيق في طرائق التعلم العميق. طرح الباحثون العديد من مناهج التعلم الآلي لكشف التسلل القائم على الشذوذ. مع زيادة استخدام الإنترنت، وظهور سيناريوهات هجوم جديدة أكثر تعقيداً، أصبحت الأساليب التي تعتمد على التعلم الآلي غير فعالة في التعامل مع التحديات الأمنية المتزايدة. أظهرت تقنيات التعلم العميق فعاليتها في استخراج الميزات ومهام التصنيف. يمكن للشبكات العميقة أن تقلل تلقائياً من تعقيد حركة مرور الشبكة بإيجاد الارتباطات بين البيانات دون تدخل بشري، وكذلك يحل مشكلة أنظمة الكشف القائمة على الشذوذ بتخفيض معدل الإيجابيات الكاذبة وزيادة معدل الكشف [1].

2. هدف البحث:

يهدف هذا البحث، إلى تصميم نظام كشف تسلل في الشبكات الحاسوبية وأنظمة تقانة المعلومات والاتصالات، وذلك بالاعتماد على الشبكات العصبونية العميقة المعقدة، للحصول على عملية كشف أفضل.

3. أهمية البحث:

تأمين الشبكات وأنظمة تقانة المعلومات والاتصالات، وحمايتها من الاختراقات والهجمات السيبرانية، وتخفيض الخسائر الناتجة عن الهجمات الإلكترونية والبرمجيات الخبيثة.

4. المواد وطرائق البحث:

يرتكز البحث على ثلاث منظومات أساسية هي: نظم كشف التسلل والشبكات العصبونية العميقة المعقدة وقواعد البيانات.

تم استخدام الآتي:

1. برنامج pycharm ومكتباته لكتابة البرامج اللازمة بلغة python لتصميم النظام المقترح.

2. مجموعة البيانات المعيارية KDD CUP99 لتدريب النموذج المقترح واختباره.

5. الأمن السيبراني ونظام كشف التسلل:

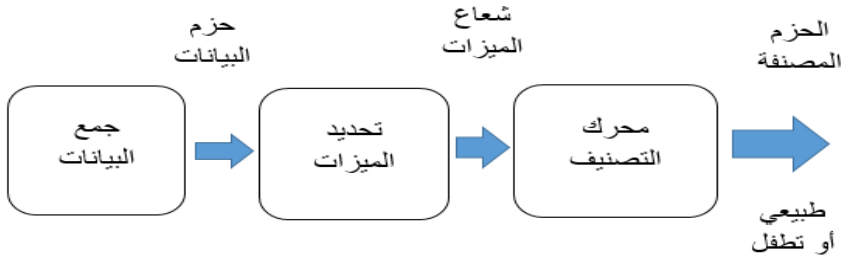
أهم المصطلحات في هذا البحث:

الأمن السيبراني (Cyber Security): هو مفهوم أوسع من أمن المعلومات، ويتضمن تأمين البيانات والمعلومات المتبادلة عبر الشبكات الداخلية أو الخارجية، والتي يتم تخزينها في خوادم داخل أو خارج الشركة من الاختراقات [12].

الشبكة الحاسوبية: عبارة عن شبكة اتصالات حاسوبية مرتبطة ببعضها باستخدام لغات اتصال خاصة تسمى بروتوكولات الشبكة (بروتوكول TCP/IP).

نظام كشف التسلل (IDS): هو برنامج أو تطبيق أمن الحاسوب أو مزيج من كلاهما، والذي يهدف إلى الكشف عن مجموعة واسعة من الانتهاكات الأمنية، إذ يراقب نظاماً أو

شبكة أو أنظمة ضد أي نشاط ضار [4]. تتمثل الوظائف الرئيسة لـ IDSs في مراقبة المضيفين والشبكات وتحليل سلوكيات أنظمة الحاسوب وتوليد التنبيهات والاستجابة للسلوكيات المشبوهة. يتم نشر IDS عادة بالقرب من عقد الشبكة المحمية [2] [3]. يوضح الشكل (1) المكونات الرئيسة لنظام كشف التسلل، إذ تحتوي أنظمة كشف التسلل IDSs على ثلاث مكونات رئيسة كما هو موضح في الشكل (1). بناءً على مصادر المعلومات، يتم تصنيف كشف التسلل إلى نظام كشف التسلل المعتمد على الشبكة (NIDS)ونظام كشف التسلل المعتمد على المضيف (HIDS)، إذ في HIDS يتم جمع ملفات السجل عبر أجهزة الاستشعار المحلية. بينما تفحص NIDS كل حزمة محتويات في تدفقات حركة مرور الشبكة. يتم تحليل تدفقات حركة مرور الشبكة باستخدام طرائق الكشف، وهي طرائق الكشف القائمة على سوء الاستخدام/ التوقيع (Signature based Detection) وطرائق الكشف القائمة على الشذوذ (Anomaly based Detection)[2] .



الشكل (1): المكونات الرئيسة لنظام كشف التسلل.

يستخدم اكتشاف سوء الاستخدام التوقيعات والفلاتر المحددة مسبقًا للكشف عن الهجمات، ويعتمد على تحديث قاعدة بيانات التوقيع باستمرار. هذه الطريقة دقيقة في الهجمات المعروفة، ولكنها غير فعالة في حالة الهجمات غير المعروفة. يستخدم

اكتشاف الشذوذ آليات الكشف عن الأنشطة الخبيثة غير المعروفة. في معظم الأحيان، ينتج عن الكشف عن الشذوذ معدل إيجابي كاذب مرتفع [2].

6. التعلم العميق:

تتكون نماذج التعلم العميق من شبكات عميقة متنوعة، منها خاضع للإشراف مثل الشبكات العصبونية العميقة Deep Neural Networks (DNNs) وشبكات موجزة عميقةDeep Brief Networks (DBNs) والشبكات العصبونية الالتفافية Convolutional Neural Network (CCNs) والشبكات العصبونية التكرارية Recurrent Neural Networks(RNNs)، ومنها غير خاضع للإشراف مثل المشفرات التلقائية (Auto Encoder) وآلات بولتزمان المقيدة Restricted Boltzmann Machine(RBMs) وشبكات الخصومة التوليدية Generative Adversarial Networks (GANs). تتعلم نماذج التعلم العميق مباشرة تمثيلات الميزات من البيانات الأصلية، مثل الصور والنصوص دون الحاجة إلى هندسة الميزات اليدوية، وبالتالي يمكن تنفيذ طرائق التعلم الآلي بطريقة شاملة. بالنسبة لمجموعة البيانات الكبيرة، تتمتع أساليب التعلم العميق بميزة كبيرة في التعامل معها. في دراسة التعلم العميق، إن التركيز الرئيس هو هندسة الشبكة واختيار المعلمة الفائقة واستراتيجية التحسين. يبين الجدول (1) مقارنة بين خوارزميات التعلم العميق المختلفة [4].

الجدول (1): مقارنة بين نماذج التعلم العميق المختلفة.

الخوارزميات	أنواع البيانات المناسبة	خاضع للإشراف أو غير خاضع للإشراف	المهام
Auto encoder	البيانات الخام شعاع الميزات	غير خاضع للإشراف	استخراج الميزة خاصية التخفيض تقليل الضجيج
RBM	شعاع الميزات	غير خاضع للإشراف	استخراج الميزة خاصية التخفيض تقليل الضجيج

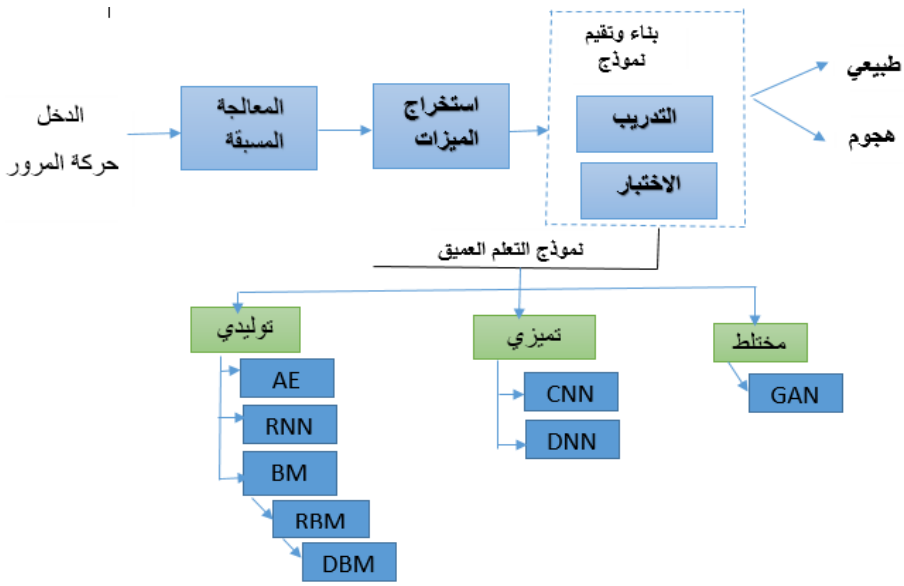
DBN	شعاع الميزات	خاضع للإشراف	استخراج الميزة التصنيف
DNN	شعاع الميزات	خاضع للإشراف	استخراج الميزة التصنيف
CNN	البيانات الخام شعاع الميزات المصفوفات	خاضع للإشراف	استخراج الميزة التصنيف
RNN	البيانات الخام شعاع الميزات بيانات التسلسل	خاضع للإشراف	استخراج الميزة التصنيف
GAN	البيانات الخام شعاع الميزات	غير خاضع للإشراف	زيادة البيانات تدريب الخصومة

7. نظام كشف التسلل القائم على التعلم العميق:

يوضح الشكل (2) نظام الكشف المعتمد على التعلم العميق[1] . حيث يتكون من عدة مراحل هي:

1. الدخل أو حركة المرور: البيانات هي المكون الأساسي عند تقييم أي IDS. يمكن جمع البيانات من مختلف المصادر، بما في ذلك سجلات المضيف وحركة مرور الشبكة.
2. المعالجة المسبقة أو التحضيرية للبيانات: تفيد المعالجة التحضيرية غالبا، في إزالة البيانات المكررة، والبيانات غير الكاملة، وتحويل البيانات إلى شكل موحد. تتضمن في أغلب الأحيان كل من الخطوات التالية: حذف السجلات المتكررة، وتحويل البيانات الرمزية إلى بيانات رقمية.

3. استخراج الميزات: أي تحليل حركة مرور الشبكة باستخدام أدوات محددة، إذ تستخدم أدوات استخراج الميزات لإنشاء مجموعات البيانات، ومن هذه الأدوات Argus.
4. نموذج كشف التسلل: يتم تصميم نموذج كشف التسلل باستخدام أحد خوارزميات التعلم العميق، ومن ثم تدريبه واختباره، ليقوم بتحديد نوع سجل الاتصال هل هو سجل طبيعي أو هجوم.



الشكل (2): نظام الكشف المعتمد على التعلم العميق.

يتم تقييم فعالية IDS من خلال قدرته على التصنيف الصحيح، أي القدرة على تحديد الصنف الذي ينتمي إليه سجل الاتصال طبيعي أم هجومي. عند مقارنة نتيجة تصنيف السجل مع الواقع الفعلي، نجد أربع حالات مختلفة يبينها الجدول (2) الذي يعبر عن مصفوفة الاضطراب التي تعد من أهم الوسائل المستخدمة في عملية تقييم أداء IDS [10].

الجدول (2): مصفوفة الاضطراب.

	تم التنبؤ أن الحدث إيجابي Predicted Positive	تم التنبؤ أن الحدث سلبي Predicted Negative
الحدث بالفعل إيجابي Actual Positive	TP	FN
الحدث بالفعل سلبي Actual Negative	FP	TN

الإيجابيات الصحيحة TP: عدد السجلات المصنفة بشكل صحيح إلى الفئة العادية.
السلبيات الصحيحة TN: عدد سجلات الاتصال المصنفة بشكل صحيح في فئة الهجوم.
الإيجابيات الخاطئة FP: عدد السجلات العادية المصنفة بشكل خاطئ في سجل الهجوم.
السلبيات الخاطئة FN: عدد سجلات اتصال الهجوم المصنفة بشكل خاطئ في سجل الاتصال العادي [2].

استنادًا إلى المصطلحات السابقة، يتم النظر في مقاييس التقييم الأكثر استخدامًا الآتية:
Accuracy: يقدر نسبة سجلات الاتصال المعترف بها بشكل صحيح إلى مجموعة بيانات الاختبار بأكملها، العلاقة (1).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (1)$$

حيث: TP: الإيجابيات الصحيحة، TN: السلبيات الصحيحة، FP: الإيجابيات الخاطئة، FN: السلبيات الخاطئة [2].

Precision: تقدر نسبة سجلات اتصال الهجوم المحددة بشكل صحيح إلى عدد جميع سجلات اتصال الهجوم المحددة، العلاقة (2).

$$Precision = \frac{TP}{TP + FP} \qquad (2)$$

حيث: TP: الإيجابيات الصحيحة،FP : الإيجابيات الخاطئة [2].

المعدل الإيجابي الحقيقي (TPR): يطلق عليه أيضًا Recall. ويقدر نسبة سجلات اتصال الهجوم المصنفة بشكل صحيح إلى العدد الإجمالي لسجلات اتصال الهجوم، العلاقة (3).

$$TPR = \frac{TP}{TP + FN} \qquad (3)$$

حيث: TP: الإيجابيات الصحيحة، FN: السلبيات الخاطئة [2].

المعدل الإيجابي الكاذب (FPR): إنه يقدر نسبة سجلات الاتصال العادية التي تم وضع علامة عليها كمهاجمة إلى العدد الإجمالي لسجلات الاتصال العادية، العلاقة (4).

$$FPR = \frac{FP}{TN + FP} \qquad (4)$$

حيث: FP: الإيجابيات الخاطئة، TN: السلبيات الصحيحة [2].

F1–Score: تسمى أيضاً باسم F1–Measure، وهي عبارة عن محدد يتعلق بكل من Precision و Recall من خلال العلاقة (4).

$$F1 - Score = 2 \times \left(\frac{Precision \times Recall}{Precision + Recall}\right) \qquad (4)$$

حيث Precision: الدقة، Recall: المعدل الإيجابي الحقيقي [2].

8. مجموعة البيانات KDD CUP99:

تم إنشاؤها بسبب الحاجة إلى مجموعة بيانات مناسبة لاختبار أنظمة كشف التسلل بوساطة مختبر MIT Lincon باستخدام 1000 من أجهزة UNIX و 100 من مستخدمي الوصول إلى هذه الأجهزة، وقد تم تصميمها لتكون مجموعة بيانات المحاكاة عام 1998. بشكل عام، تتضمن مجموعة البيانات القياسية KDDCUP99 حوالي 5 ملايين من سجلات الاتصال، تنقسم إلى سجلات تدريب وسجلات اختبار. يتضمن كل سجل اتصال 41 ميزة يمكن تصنيفها على أنها ميزات أساسية، وهي 9 ميزات (1...9)، وميزات محتوى، وهي 13 ميزة (10...22)، وميزات حركة مرور (23...41)، يمكن تصنيف السجلات في مجموعة البيانات هذه إلى 5 فئات رئيسة، 4 منهم هجوم و1 هو عادي.

• عادي: بيانات نوع غير الهجوم.

• أنواع الهجوم: DOS (رفض الخدمة)، والتحقيق (التحقيق الهجمات)، و R2L (الجذر إلى المحلية) و U2R (المستخدم إلى الجذر).

الهجمات هي 22 نوعاً، وكل ينتمي إلى فئة الهجوم أعلاه. تحتوي KDD Cup99 على بيانات رقمية (بتنسيق رقم ثنائي وحقيقي) ومعلومات نصية (محارف) حول فئات الطلب. بالإضافة إلى ذلك، تحتوي هذه البيانات على ميزة إضافية واحدة في النهاية لإظهار تسمية البيانات سواء أكان ذلك من التسلل أم لا [9] [3]. قاعدة البيانات هذه مدروسة بشكل كبير وتفصيلي في المرجع [11].

سجل طبيعي:

0،tcp,http,SF,239,486,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0.00,0.00
,0.00,0.00,1.00,0.00,0.00,19,19,1.00,0.00,0.05,0.00,0.00,0.00,0
.00,0.00,normal.

سجل هجوم:

0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,292,18,1.00,1.00,0.00,0.00,0.06,0.05,0.00,255,18,0.07,0.06,0.00,0.00,1.00,1.00,0.00,0.00,neptune.

الجدول(3): تدريب سجلات الاتصال من مجموعات بيانات KDDCup 99 واختبارها.

Attack category	Description	Data instances - 10 % data			
		KDDCup 99		NSL-KDD	
		Train	Test	Train	Test
Normal	Normal connection records	97,278	60,593	67,343	9,710
DoS	Attacker aims at making network resources down	391,458	229,853	45,927	7,458
Probe	Obtaining detailed statistics of system and network configuration details	4,107	4,166	11,656	2,422
R2L	Illegal access from remote computer	1,126	16,189	995	2,887
U2R	Obtaining the root or super-user access on a particular computer	52	228	52	67
Total		494,021	311,029	125,973	22,544

9. الدراسات السابقة:

1- قدم (Yin ***et all*** ; 2017) [5] نمذجة لنظام كشف تسلل يعتمد على التعلم العميق باستخدام الشبكات العصبونية المتكررة RNN. تم تقييم النموذج على مجموعة البيانات NSL-KDD. حصل النموذج على أعلى دقة عندما كان هناك 80 عقدة مخفية ومعدل التعلم 0.1، حيث وصلت الدقة إلى 81.2 في التصنيف الثنائي، أما في التصنيف لخمس فئات كانت دقة الكشف حوالي 80. من سلبيات هذا النموذج يحتاج إلى وقت تدريب كبير، وتظهر النتائج معدلات اكتشاف أقل لفئات R2L و U2R.

2- اقترح (Lin et all;2018) [6] نظام كشف التسلل باستخدام الشبكات العصبونية التلافيفية CNN بناءً على LeNet-5 لتصنيف هجمات الشبكة. تم تدريب النموذج واختباره على مجموعة البيانات KDD99. أظهرت النتائج أن

معدل دقة الكشف 96%. من سلبيات هذا النموذج، أنه لم يتم أخذ جميع الميزات في مجموعة البيانات (32 من أصل 41 ميزة).

3- استخدم (Vigneswaran et all;2018) [7] الشبكات العصبونية العميقة DNNsللتنبؤ بالهجمات على نظام كشف التسلل إلى الشبكة (N-IDS)، وقد تم استخدام مجموعة بياناتKDDCup-99 . أظهرت النتائج أن بنية DNN من 3 طبقات مخفية أداؤها متفوق على جميع الخوارزميات الكلاسيكية الأخرى وخوارزميات التعلم بعد المقارنة. حيث كانت دقة الكشف 0.92 و 0.91 =Recall و f1-score=0.95.

4- استخدم (VINAYAKUMAR et all;2019) [2] شبكة عصبية عميقة DNN لتطوير IDS لاكتشاف الهجمات السيبرانية وتصنيفها باستخدام مجموعة بيانات KDDCup 99. يقترح هذا العمل بنية DNN تكون من طبقة إدخال و 5 طبقات مخفية وطبقة إخراج. أظهرت معظم طوبولوجيا شبكة DNN دقة التدريب في النطاق من 95٪ إلى 99٪. من سلبيات هذا النموذج، أنه يحتاج إلى وقت تدريب كبير من أجل الحصول على بنينه طوبولوجيا شبكة مثلى.

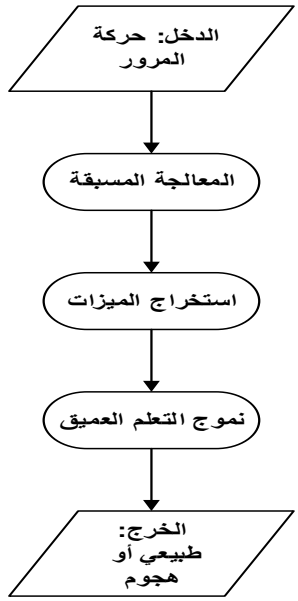
5- استخدم (Alsughayyir ***et all*** ;2019) [8] التعلم العميق لتطوير نظام كشف هجمات الشبكة، إذ استخدم تقنية التشفير التلقائي Auto-encoder لتصنيف السلوك الطبيعي من السلوك الشاذ على الشبكة استناداً إلى مجموعة البياناتNSL-KDD . أظهرت النتائج أن المقترح يتفوق على الأساليب الكلاسيكية بدقة 99% للتدريب و 91.28% لمرحلة الاختبار. هذا المقترح بحاجة إلى محاولة تضمين المزيد من أساليب التعلم العميق وتطبيق خوارزميات التعلم العميق على حركة مرور الشبكة في الوقت الحقيقي.

10. النظام المقترح:

في هذا البحث، تم تصميم شبكة تعلم عميقة معقدة للحصول على عملية كشف تسلل أفضل من شبكات التعلم العميقة العادية، إذ اعتمدت في هذا التصميم على إدخال البيانات حسب أهميتها وتسلسلها إلى شبكات عصبونية عميقة مكونة من مجموعة طبقات خفية بشكل غير متساوٍ لجميع البيانات.

البيانات التي يتم تداولها عبر الشبكة بغض النظر عن نوعها تحتاج إلى معالجة مسبقة، ومن ثم استخراج الميزات منها لتذهب بعدها إلى عملية التصنيف والتقرير ما إذا كانت طبيعة أو شاذة. إن إنشاء قاعدة بيانات لمصنع أو شركة محددة والقيام باستخراج الميزات منها يعتبر قاعدة بيانات لا يمكن الاستفادة منها في أنظمة كشف التسلل العالمية من أجل المقارنة. لذلك، تم القيام بإنشاء قاعدة بيانات ضخمة تحاكي شبكة حاسوبية مكونة من 1000 حاسوباً متصلة عبر بروتوكول TCP/IP تحتوي على كافة أنواع الهجمات التي يمكن أن تهدد الشبكات سواء في مجموعة التدريب منها أو الاختبار. قاعدة البيانات هذه تم استخلاص الميزات منها، وأصبح لكل سجل اتصال 41 ميزة، وكل ميزة تعبر عن نوع مختلف. منها الميزات الأساسية، وهي 9 أنواع ورقمها التسلسلي (1..9)، مثل مدة الاتصال ونوع البروتوكول عدد البايتات المنقولة والعلم الذي يشير إلى الحالة الطبيعية أو حالة الخطأ للاتصال، توفر هذه السمات معلومات لأغراض تحليل البروتوكول. ميزات المحتوى وهي 13 نوعاً ورقمها التسلسلي (10..22)، وهذه السمات تعكس سلوك التطفل مثل عدد حالات فشل تسجيل الدخول، من محتوى البيانات. وميزات حركة المرور المستندة إلى الوقت، وهي 19 نوعاً ورقمها التسلسلي (23..41)، وهذه السمات تعكس الاتصالات بين السجل الحالي والسجل في الفترات الزمنية السابقة. تعتبر هذه المعلومات مهمة بالنسبة لإرسال البيانات، لذلك عملية استخلاص الميزات مهمة جداً قبل مرحلة التصنيف / الكشف التي تتم باستخدام نموذج

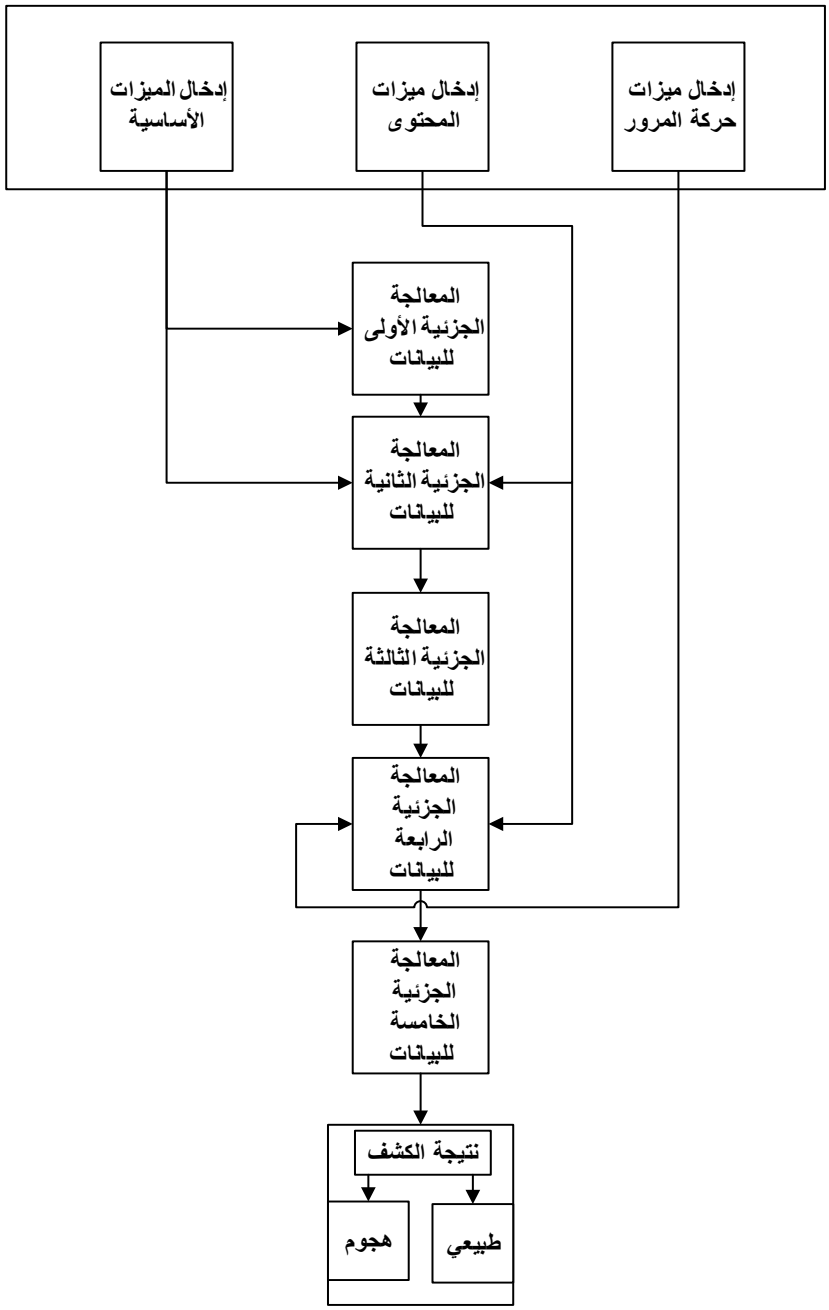
التعلم العميق كما هو موضح في الشكل (3). لذلك، لتقييم نماذج التصنيف / الكشف يجب اختبارها على مجموعة البيانات المعيارية نفسها، وهي KDD CUP99.



الشكل (3): المخطط الصندوقي لنظام كشف التسلل.

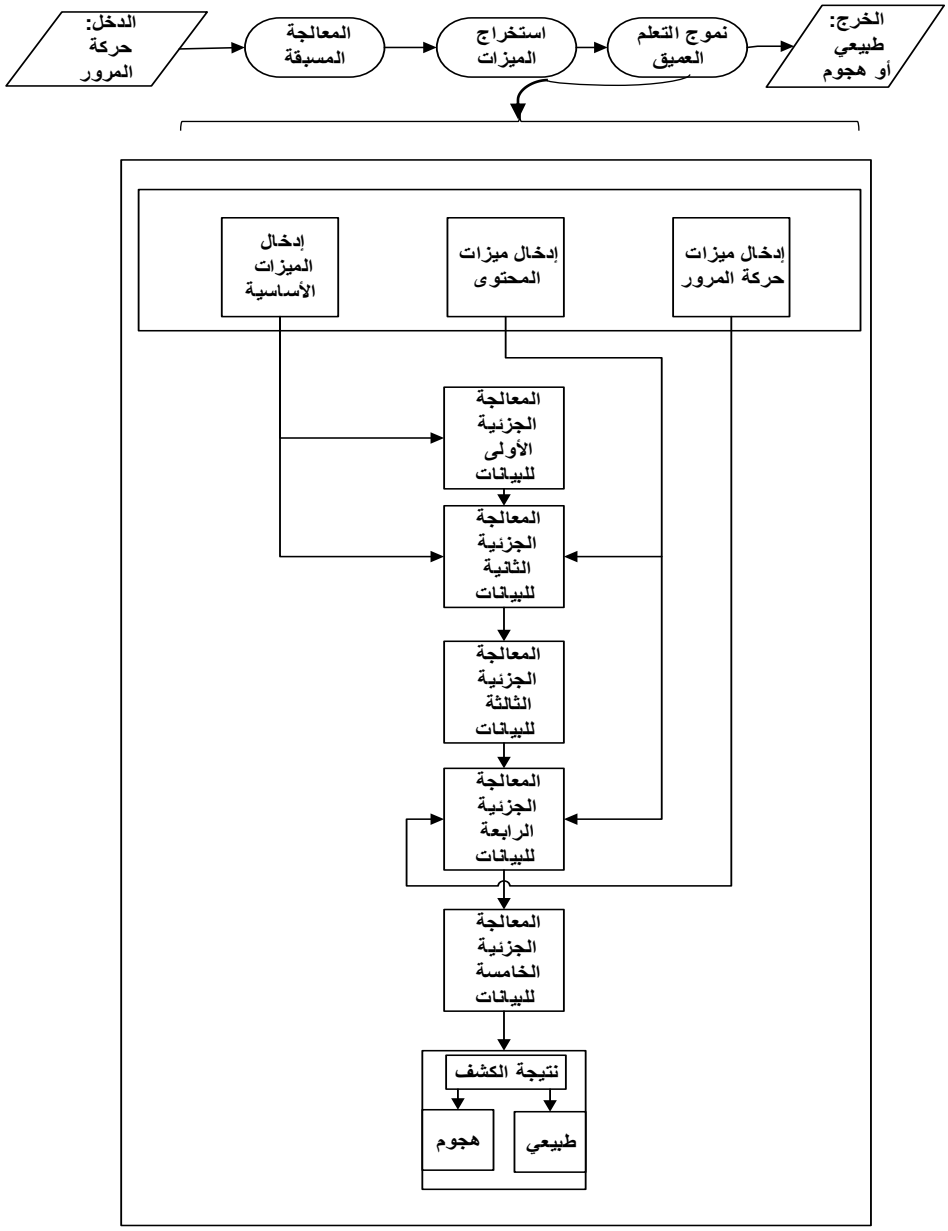
في مرحلة الكشف باستخدام التعلم العميق، تم في هذا البحث تصميم نظام كشف تسلل جديد باستخدام الشبكات العصبونية العميقة اعتماداً على قاعدة البيانات KDD CUP99 التي تحتوي على الميزات، إذ تبعاً لميزاتها التي هي عبارة عن 41 ميزة مقسمة إلى ميزات أساسية (1...9) وميزات محتوى (10...22) وميزات حركة المرور (23....41) بدلاً من إدخال كامل الميزات إلى نظام التعلم العميق دفعة واحدة. تم اقتراح طريقة جديدة للتصميم، تتم فيها عملية الإدخال على مراحل. بما أن الميزات مقسمة إلى ثلاثة أقسام تم الاقتراح على أن يتم إدخالها على ثلاث مراحل تبعاً لتسلسل الميزات وأهميتها. تعتبر الميزات الأساسية هي الأهم، لذلك يتم إدخالها أولاً إلى النظام ليتم معالجتها بشكل جزئي في مرحلة المعالجة الأولى للبيانات، والتي هي عبارة عن الطبقات الخفية (1 و 2) المكونة من (16,64) عصبوناً على التوالي. في مرحلة

المعالجة الجزئية الثانية للبيانات، والتي هي عبارة عن الطبقة الخفية الثالثة، يتم إدخال ميزات المحتوى، وكذلك الميزات الأساسية قبل المعالجة الجزئية الأولى وبعدها، لتصبح الطبقة المخفية طبقة مدخلات أيضاً مكونة من 86 عصبون، إذ خرج مرحلة المعالجة الجزئية الثانية يكون دخلاً لمرحلة المعالجة الجزئية الثالثة، والتي هي عبارة عن الطبقات الخفية (5 , 4) المكونة من (86,128) عصبوناً على التوالي وفي مرحلة المعالجة الجزئية الرابعة، والتي هي عبارة عن الطبقة الخفية السادسة يتم إدخال ميزات حركة المرور، وكذلك الميزات القادمة من مرحلة المعالجة الجزئية الثالثة وميزات المحتوى وهي مكونة من 160 عصبوناً، إذ خرج مرحلة المعالجة الجزئية الرابعة هو دخل لمرحلة المعالجة الجزئية الخامسة، والتي عبارة عن الطبقات الخفية (7,8) المكونة من (256,128) عصبوناً على التوالي، والتي تعتبر آخر عملية معالجة بهذه الحالة تكون قد اكتملت عملية معالجة البيانات لتذهب إلى مرحلة التصنيف في طبقة الخرج المكونة من عصبون يقرر النتيجة إما أن يكون تسللاً أو هجوماً كما هو موضح في الشكل (4). يكون خرج كل عصبون في أية مرحلة معالجة عبارة عن قيم الدخل لهذا العصبون مضروبة بالأوزان، فإذا كان المجموع الموزون لقيم الدخل أكبر من قيمة معينة تدعى العتبة فإنه يتفعل العصبون (حسب تابع التفعيل المستخدم) ويرسل إشارة.



الشكل (4): مخطط تفصيلي لنظام كشف التسلل المعتمد على التعلم العميق.

وبالتالي يكون المخطط الصندوقي لنظام كشف التسلل المقترح كما في الشكل (5).

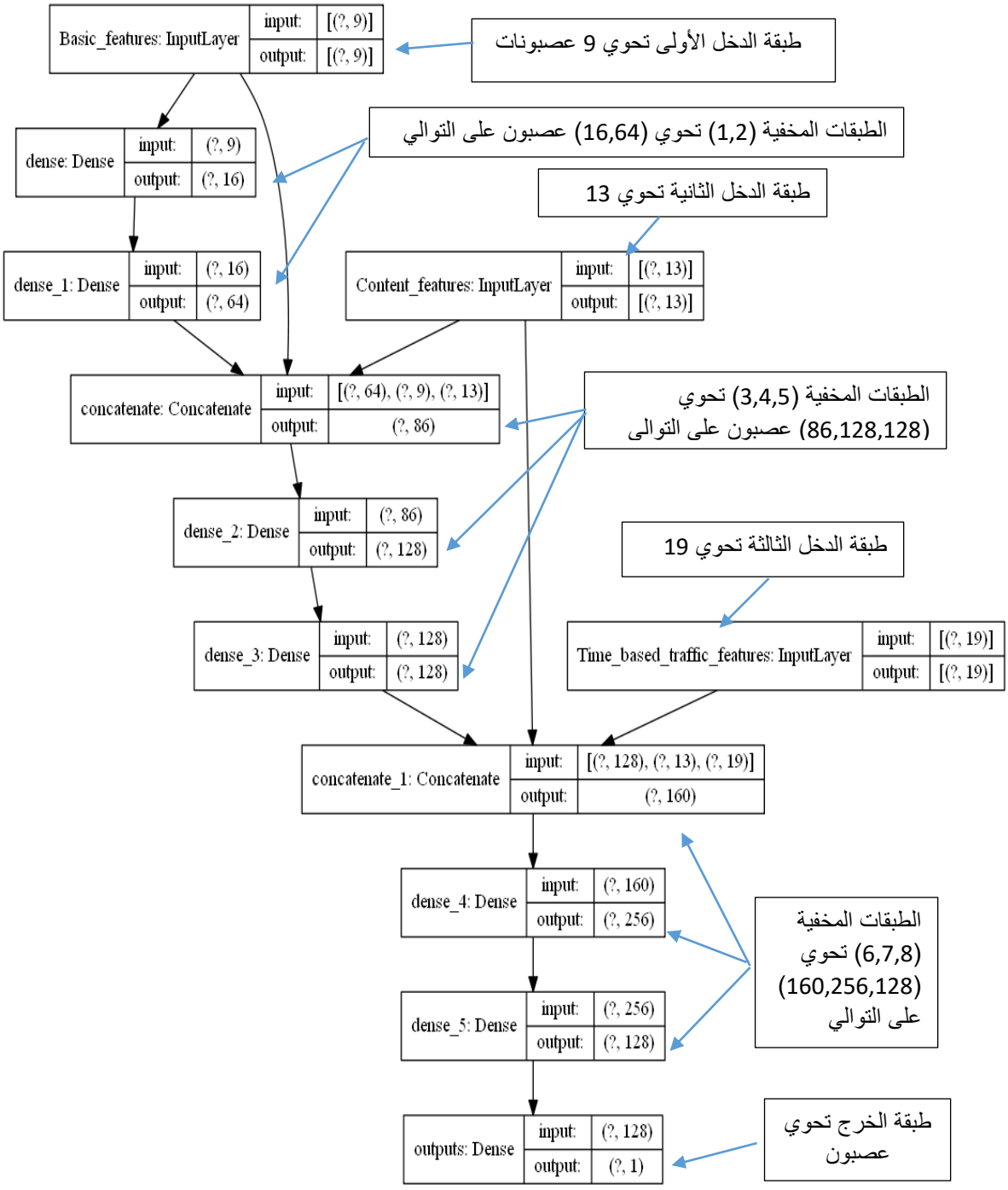


الشكل (5): المخطط الصندوقي لنظام كشف التسلل المقترح

بما أن عصبونات،

فقد تم استخدام برنامج pycharm المصمم للتعامل مع التعلم العميق لتصميم البنية

المقترحة. يوضح الشكل (6) بنية الشبكة العصبونية العميقة المعقدة المقترحة وعدد العصبونات في كل طبقة ودخل وخرج كل طبقة، إذ تم استخدام تابع التشيط relu في الطبقات الخفية لأنها أكثر كفاءة ولديها القدرة على تسريع عملية التدريب بالكامل، وتابع التنشيط sigmoid في طبقة الخرج، وذلك لطبيعته المستخدمة في الفصل الثنائي، حيث يرجع بخرجه 0 أو 1. نظراً لأن الميزات الأساسية يبلغ عددها 9 ميزات، فقد تم مضاعفة عدد العصبونات في الطبقة الخفية 16 عصبوناً، وهو أقرب عدد بالاس الثنائي 2^n، ولتقليل تعقيد الشبكة ووقت التدريب، فقد اختصرنا طبقة خفية من الطبقات، لذلك تم مضاعفة عدد العصبونات في الطبقة الخفية التالية إلى 64 عصبوناً مباشرة، وتم اختصار طبقة 32 عصبون، إذ أنه في البداية تم اختصار طبقة 64 عصبوناً، لكن النتائج لم تكن مرضية، وبالمثل لباقي الطبقات الخفية. تم الحفاظ على التعلم ثابتاً عند0.01، بينما يتم تحسين البارامترات الأخرى. وتم تدريب المقترح 10 مرات واستغرقت عملية التدريب ساعة واحدة تقريباً على معالج CORE i3. إشاره الاستفهام في البنية المقترحة تعني النموذج قبل إدخال البيانات إليه و Input Layer هي طبقة الدخل وDense، هي طبقة مخفية وOutput هي طبقة الخرج.



الشكل 6: بنية الشبكة العصبونية العميقة.

11. النتائج والمقارنة:

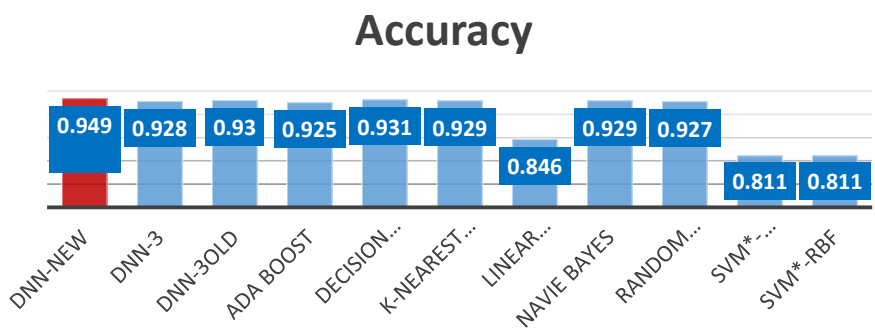
لتقييم النموذج المقترح، تم إعادة تطبيق الخوارزميات الكلاسيكية وتدريب الشبكة العصبونية العميقة العادية، وكذلك الشبكة العصبونية العميقة المعقدة المصممة على مجموعة البيانات KDDCup-99، وبعد اكتمال التدريب تم إعادة مقارنة جميع النماذج. يوضح الجدول (4) نتائج اختبار النموذج الجديد المقترح بعد التدريب ومقارنته مع نتائج الخوارزميات الأخرى التي تم إعادة تطبيقها.

الجدول (4): نتائج اختبار النموذج الجديد ومقارنته مع الخوارزميات الأخرى.

Algorithm	Accuracy	Precision	Recall	f1score	FPR
DNN-New	0.949	0.999	0.915	0.955	0.001
DNN-3	0.928	0.999	0.915	0.956	0.001
Ada Boost	0.925	0.995	0.911	0.951	0.005
Decision Tree	0.931	0.999	0.915	0.955	0.001
K-Nearest Neighbour	0.929	0.998	0.913	0.954	0.002
Linear Regression	0.846	0.988	0.819	0.896	0.012
Navie Bayes	0.929	0.988	0.923	0.955	0.012
Random Forest	0.927	0.999	0.910	0.953	0.001
SVM-Linear	0.811	0.994	0.770	0.868	0.006
SVM-rbf	0.811	0.992	0.772	0.868	0.008

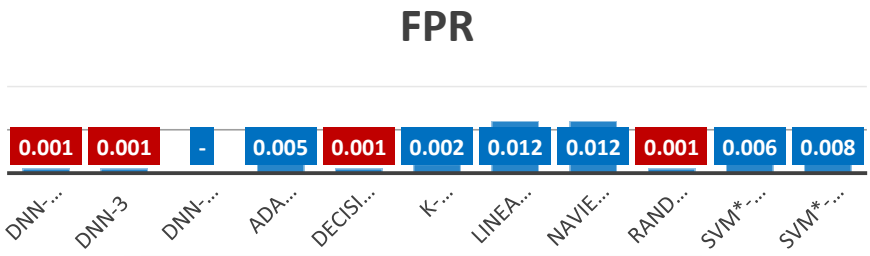
من الجدول (4)، نجد أن خوارزمية أشجار القرار أفضل من حيث الدقة من الشبكة العصبونية العميقة العادية، بالرغم أن عدد مرات التدريب ذاتها المستخدمة في الدراسة السابقة[7] ، ولكن نلاحظ تفوق الشبكة العميقة الجديدة على الشبكة العميقة العادية وجميع خوارزميات التعلم الآلي الكلاسيكية الأخرى. هذا بسبب قدرة DNNs على

استخراج البيانات والميزات ذات التجريد العالي، بالإضافة إلى توزيع الدخل الذي يخفف العبء على الشبكة. عدم الخطية للشبكات يضاف إلى الميزة عند مقارنته بالخوارزميات الأخرى. أعطت أفضل دقة على الرغم من عدد مرات التدريب قليلة (10)، أي استغرقت زمناً أقل، في حين تم تدريب الشبكة العصبونية العميقة العادية 1000 للحصول على دقة 0.93 مع زمن تدريب كبير. مع العلم أن الشبكة المصممة احتمالية انهيارها ضئيل مهما زاد عدد مرات التدريب بسبب توزيع الدخل. توضح المخططات الآتية مقارنة كل متغير من المتغيرات، الشكل (7).



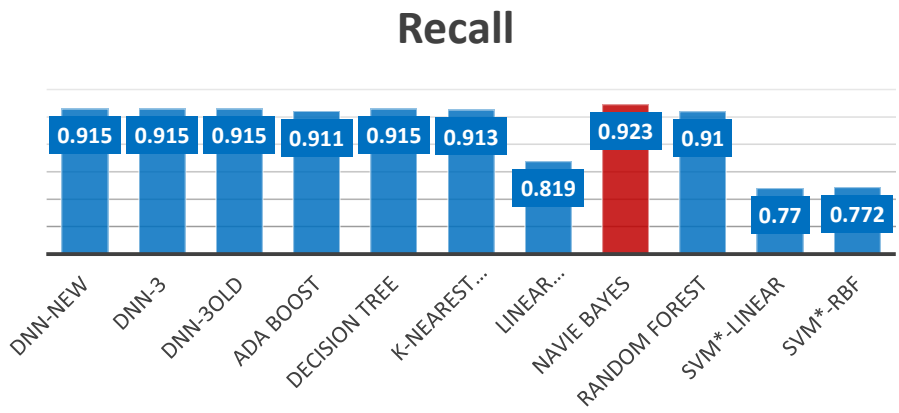
الشكل (7): مقارنة الدقة Accuracy.

نلاحظ من الشكل (7)، أن النموذج المقترح حصل على أفضل دقة 0.949 مقارنة بالخوارزميات الأخرى.



الشكل (8): مقارنة معدل الإيجابيات الكاذبة.

نلاحظ من الشكل (8)، النموذج المقترح حصل على معدل إيجابيات كاذبة 0.001 تعتبر قيمة منخفضة جدا ولكن هناك خوارزميات قامت بتحقيقها.



الشكل (9): مقارنة معدل الإيجابيات الحقيقية.

تفوقت خوارزمية Navie Bayes في الحصول على أعلى معدل إيجابيات حقيقة، وهي 0.923 ولكن النموذج المقترح حقق قيمة 0.915.

13. الخاتمة والمقترحات:

شبكات التعلم العميق أثبتت فعاليتها في أنظمة كشف التسلل لاكتشاف الهجمات على الشبكة، إذ حققت دقة كشف عالية مقارنة مع طرائق التعلم الآلي. يعتبر نظام الكشف القائم على الشبكة العميقة المعقدة الذي تم اقتراحه في هذا البحث أفضل إلى حد ما من حيث قدرته على تمييز حركة المرور العادية عن الشاذة. لزيادة الدقة يجب تدريب النموذج المقترح أكثر.

14. المراجع:

[1] ALDWEESH.A, DERHAB.A, EMAM.A.Z,2019-"Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues". Knowledge-Based Systems, VOL.189.19, P.37.https://doi.org/10.1016/j.knosys.2019.105124

[2] VINAYAKUMAR.R, ALAZAB.M, SOMAN.K.P, 2019 -"Deep Learning Approach for Intelligent Intrusion Detection System", IEEE ACCESS VOL.7.197, pp. 41525-41550.

https://doi.org/10.1109/ACCESS.2019.2895334

[3] KARATAS.G, DEMIR.O, SAHINGOZ.O.K, 2018-"Deep Learning in Intrusion Detection Systems", IEEE International Congress on Big Data, Deep Learning and Fighting Cyber Terroris VOL..32, PP.113-116. doi: 10.1109/IBIGDELFT.2018.8625278

[4] LIU.H and LANG.B,2019 - "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey", Applied Sciences , VOL.9(20), PP.4396

[5] YIN.CH, ZHU.Y, FEI.J, HE. X, 2017-"A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", IEEE ACCESS , VOL.5.551, PP. 21954- 21961.

https://doi.org/10.1109/ACCESS.2017.2762418

[6] HUI LIN.W, CHUNG LIN. H. WANG. P, HUA WU. B, YING TSAI. J,2018- Using Convolutional Neural Networks to Network

Intrusion Detection for Cyber Threat, IEEE computer science, VOL..32,PP.11071110.https://doi.org/10.1109/ICASI.2018.8394474

[7] VIGNESWARA. R, KP. S, POORNACHANDRAN. P, 2018- Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security, IEEE Communications and Informatics(ICACCI),VOL..34,p.6.https://doi.org/10.1109/ICACCI.2018.8494096

[8] ALSUGHAYYIR.B, QAMAR.A.M, KHAN.R, 2019- Developing a Network Attack Detection System Using Deep Learning, IEEE computer science , VOL..32, P.5.

https://doi.org/10.1109/ICCISCI.2019.8716389

[9]DDCup1999Data.2001
https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[10] DR.ALAHMAD.H,IBRAHIME.R,2017-"Using Neural Networks to Build an Intrusion Detection System based on Standard Dataset (KDD99)",Engineering Sciences Series Vol. (93) No. (5),pp 287-310.

[11]https://www.arabicprogrammer.com/article/7432839791/#KDD_CUP_67 12\1\20021.

[12] DR. SUMEET DUA AND DR. XIAN DU, 2011- Data Mining and Machine Learning in Cybersecurity. New York, p.248.