



جامعة دمشق

كلية العلوم

قسم الرياضيات

شعبة الرياضيات التطبيقية والمعلوماتية

دراسة تحليل سلوك المستخدم باستخدام خوارزميات الذكاء الصناعي لكشف الشذوذ الشبكي

دراسة أعدت لنيل درجة الماجستير في الرياضيات التطبيقية والمعلوماتية

إعداد الطالبة: مانويلا صفر

إشراف: أ.م. د محمد فراس الحلبي

2024-2025

الشكر والإهداء

إلى من سارت معي هذا الدرب وتحملت وصبرت ووهبتني من حبها وحنانها ما لا يُقاس

أُمي الغالية

إلى من لم يفارق طيفه مخيلتي يوماً وكان حضوره في قلبي رغم الغياب

والذي رحمه الله

إلى من أنار لي دربي بعلمه وتوجيهه وكان نعم المشرف والداعم

الدكتور محمد فراس الحلبي

إلى من خفف الطريق وأضأن لحظاته شكراً لكن على الدعم رفيقات الدرب وصديقات القلب

شذى الهويدي وبراءة الخالد

إلى الذين كان لهم دوراً فاعلاً في رحلتي العلمية ولم يبخلوا يوماً بعلمهم وخبراتهم. فكانت محاضراتهم، ونقاشاتهم وتوجيهاتهم حجر الأساس في بناء معرفتي وتوسيع مداركي

جميع الدكاترة الأجلاء

إلى من سيقراً هذه الرسالة، ويجعل من كلماتي امتداداً لعلمه وبحثه عسى أن تجدوا بين السطور ما ينفع الباحثين وطلاب الدراسات العليا

وأخيراً لكل من ساندني بكلمة، دعاء أو تشجيع، وكان له في هذا الإنجاز أثر... شكراً من القلب.

الفهرس

الشكر والإهداء

IV	 الملخص باللغة العربية
V	 قائمة الأشكال (List of Figures)
VI	 قائمة الجداول (List of Table)
1	 1. الفصل الأول: مقدمة عامة
1	 1.1. تمهيد (Introduction)
1	 2.1. مشكلة البحث
1	 3.1. الهدف من البحث
2	 4.1. أهمية البحث
2	 5.1. بنية الرسالة
3	 2. الفصل الثاني: الذكاء الصناعي
3	 1.2. مقدمة
3	 2.2. مفهوم الذكاء الصناعي (Artificial Intelligence Concept)
4	 3.2. أنواع الذكاء الصناعي (Types of Artificial Intelligence)
4	 1.3.2. القائم على القدرات (Capabilities Based)
4	 2.3.2. القائم على الوظيفة (Functionality Based)
5	 4.2. فروع الذكاء الصناعي (Branches of Artificial Intelligence)
5	 1.4.2. تعلم الآلة (Machine Learning)
6	 1.1.4.2. بعض خوارزميات تعلم الآلة
7	 2.4.2. التعلم العميق (Deep Learning)
8	 1.2.4.2. أنواع الشبكات العصبية (Types of Neural Networks)
10	 5.2. خلاصة الفصل
11	 3. الفصل الثالث: الأمن السيبراني
11	 1.3. مقدمة

11	2.3	مفهوم الأمن السيبراني (Cyber Security Concept)
12	1.2.3	الفرق بين الامن السيبراني وأمن المعلومات
13	3.3	أنواع الأمن السيبراني (Types of Cyber Security)
14	4.3	الشبكة (Network)
16	1.4.3	طبقات الشبكة (النموذج المرجعي OSI)
22	2.4.3	أمن الشبكة (Network Security)
24	5.3	الشذوذ (Anomaly)
25	1.5.3	أنواع الشذوذ (Types of Anomaly)
25	2.5.3	طرائق كشف الشذوذ (Anomaly Detection Methods)
26	6.3	خلاصة الفصل
27	4	الفصل الرابع: تحليلات الأمان
27	1.4	مقدمة
27	2.4	مفهوم تحليلات الأمان (Security Analytics Concept)
28	3.4	تحليل سلوك المستخدم (User Behavior Analysis)
29	1.3.3	الركائز الثلاث لتحليل سلوك المستخدم
30	2.3.3	مكونات تحليل سلوك المستخدم
32	3.3.4	التهديدات التي تحددها التقنية
33	4.3.4	سلبيات وإيجابيات التقنية
34	4.4	خلاصة الفصل
35	5	الفصل الخامس: الخوارزميات المستخدمة في تقنية الـ UBA
35	1.5	مقدمة
35	2.5	آلة شعاع الدعم SVM
35	1.2.5	مفهوم خوارزمية الـ SVM
37	2.2.5	تحليل سلوك المستخدم باستخدام الـ SVM
38	3.5	الشبكة العصبية المتكررة RNN

38	 1.3.5 الشبكات العصبية
48	 2.3.5 مفهوم شبكة الـ RNN
51	 3.3.5 تحليل سلوك المستخدم باستخدام الـ RNN
54	 4.5 خلاصة الفصل
55	 6. الفصل السادس: النموذج المقترح
55	 1.6 مقدمة
55	 2.6 الخوارزمية الجينية (Genetic Algorithm)
58	 3.6 مجموعة البيانات (Dataset)
58	 4.6 النموذج المقترح
68	 5.6 النتائج
75	 6.6 خلاصة الفصل
76	 7. الفصل السابع: الخاتمة والرؤى المستقبلية

قائمة المصطلحات (List of Terms)

قائمة الاختصارات (List of Acronyms)

المراجع

الملاحق

الملخص باللغة الإنكليزية

الملخص

كما هو معروف فقد أصبح من المستحيل تقريباً تخيل العالم دون شبكة الإنترنت. وفقاً لـ Statista، كان هناك 4.66 مليار مستخدم نشط على مستوى العالم لعام 2021، وهو ما يمثل 59.9% من سكان العالم.

عندما يستخدم مليارات الأشخاص شبكة الإنترنت، ينتقل كمية هائلة من البيانات بين عناوين الـ IP، الأنظمة، الشبكات والأجهزة المختلفة. من بين هؤلاء الأشخاص مجرمي الإنترنت والمتسللين القادرين على تعريض النظام الأمني لأي مؤسسة للخطر. أصبح من الصعب تحديد التهديدات الأمنية نظراً لأن الأساليب التقليدية مثل التحقق اليدوي من إداخلات السجل قد أصبحت قديمة. خصوصاً مع التطور الكبير والتوسع السريع لشبكة الإنترنت وقيم البيانات التي تحويها والتي أصبحت أكثر استغلالاً من قبل المهاجمين. زادت الحاجة لأنظمة الحماية، عندها بدأت طرق الحماية المتطورة في الظهور مثل أنظمة كشف وتصنيف الشذوذ الشبكي عندها تبلور معنى الأمن السيبراني. توجد العديد من أنظمة كشف الشذوذ الشبكي إلا أن الأنظمة القائمة على طرق التعلم العميق هي الأكثر فاعلية. عموماً تقنيات الذكاء الصناعي يمكن أن تجعل كشف الشذوذ الشبكي أسهل بكثير.

تحليل سلوك المستخدم هي تقنية للأمن السيبراني تستخدم لكشف الشذوذ الشبكي باستخدام الذكاء الصناعي وتحديد السلوك الذي قد يشير إلى هجوم إلكتروني.

تقدم هذه الرسالة توضيحاً لمفهوم كلاً من الأمن السيبراني والذكاء الصناعي. تمت مناقشة تقنية تحليل سلوك المستخدم بشكل نظري وعملي من خلال توضيح الدراسات السابقة. أخيراً اقترحنا نموذجاً هجيناً لكشف الشذوذ الشبكي باستخدام خوارزميات الذكاء الصناعي والخوارزمية الجينية.

الكلمات المفتاحية: البيانات الشاذة، كشف الشذوذ، الذكاء الصناعي، الأمن السيبراني، تحليل سلوك المستخدم، الشبكة العصبية، الخوارزمية الجينية.

قائمة الأشكال (List of Figures)

8	الشكل 1.2. بنية الشبكة العصبية الضحلة.
9	الشكل 2.2. بنية الشبكة العصبية العميقة.
15	الشكل 1.3. طريقة اتصال الأجهزة ضمن الشبكة.
17	الشكل 2.3. معالجة البيانات عبر طبقات الشبكة في النموذج المرجعي.
24	الشكل 3.3. توزيع البيانات الشاذة.
31	الشكل 1.4. توزيع نطاقات عناوين ال IP.
36	الشكل 1.5. تصنيف البيانات باستخدام خوارزمية ال SVM.
38	الشكل 2.5. بنية الخلية العصبية البيولوجية.
39	الشكل 3.5. بنية الخلية العصبية الصناعية.
42	الشكل 4.5. مثال عن شبكة عصبية صناعية.
49	الشكل 5.5. مثال يوضح بنية الشبكة العصبية المتكررة.
64	الشكل 1.6. قيم الأخطاء عبر الأجيال بعد إتمام عملية التدريب مع 40 جيل.
65	الشكل 2.6. رسم توزيع الأخطاء الطبيعية والشاذة.
66	الشكل 3.6. رسم توزيع الأخطاء لكل السجلات مع تمثيل لقيمة العتبة.
66	الشكل 4.6. مصفوفة الارتباك.
69	الشكل 5.6. منحنى ROC وقيمة ال AUC.

قائمة الجداول (List of Tables)

56	الجدول 1.6. الصبغيين الآباء في الـ GA.
56	الجدول 2.6. تقسيم الصبغيين الآباء بطريقة التقاطع الأولى.
57	الجدول 3.6. الصبغيين الأبناء الجديدين حسب طريقة التقاطع الأولى.
57	الجدول 4.6. تقسيم الصبغيين الآباء بطريقة التقاطع الثانية.
57	الجدول 5.6. الصبغيين الأبناء الجديدين حسب طريقة التقاطع الثانية.
59	الجدول 6.6. البيانات المستخدمة في النموذج المقترح من ملف logon.csv.
60	الجدول 7.6. ملف البيانات بعد استخراج الميزات وهو ملف processed_logon.csv.
61	الجدول 8.6. مثال لتحويل البيانات الفئوية إلى قيم عددية.
61	الجدول 9.6. ملف البيانات بعد التطبيع وهو ملف normalized_logon.csv.
68	الجدول 10.6. قيم التقييمات النهائية للنموذج المقترح.
72	الجدول 11.6. مقارنة بين النموذج المقترح ودراسيتين أخريتين.

الفصل الأول

مقدمة عامة

1.1. تمهيد (Introduction)

مع نشأة الثورة المعلوماتية وخاصةً في القرن الحادي والعشرين، أدت آثار التهديدات والجرائم الإلكترونية لظهور تحدٍ كبير للأمن الوطني والقومي. ظهرت حاجة ماسة لتوفير ضمانات أمنية وهو ما أسفر عن ظهور وتبلور مفهوم الأمن السيبراني (Cyber Security). بالطبع تطور الجريمة الإلكترونية يتطلب تطوراً في تقنيات الأمن السيبراني. الحاجة إلى العثور على وسائل حديثة تفتح الأبواب للبحث الدائم في هذا الصدد لضمان أمن البيانات. بحسب الدراسة [3] يتضح لدينا أن تطور تقنيات الأمن السيبراني مرتبط ارتباطاً وثيقاً باستخدام الذكاء الصناعي (Artificial Intelligence, AI). واحدة من الأساليب الجديدة التي تعتمد على الـ AI هي تقنية تحليل سلوك المستخدم (User Behavior Analysis, UBA) [34].

2.1. مشكلة البحث

تعتبر دراسة تقنية الـ UBA أمراً في غاية الصعوبة نتيجة للتطور الهائل في التكنولوجيا. التطور السريع يترتب عليه وجود مجموعة ضخمة من البيانات. البحث ضمن مجموعة كبيرة لتحديد السلوك المشبوه يستغرق الكثير من الوقت. لابد من مواكبة دائمة وتحديث مستمر لإيجاد نماذج جديدة أكثر كفاءة من سابقتها.

3.1. الهدف من البحث

لبيان الهدف من هذا البحث نقدم التساؤلات الآتية التي نعتزم الإجابة عنها:

- ✍ ما أهمية استخدام خوارزميات الـ AI في الأمن السيبراني وتقنية الـ UBA؟
- ✍ ما مدى فاعلية حلول تقنية الـ UBA في كشف الشذوذ الشبكي؟
- ✍ ما هي الخوارزميات المستخدمة في التقنية الأكثر فاعلية؟
- ✍ هل هناك فعلاً إمكانية لتحسين طرق الكشف عن الشذوذ الشبكي؟
- ✍ هل يمكن اقتراح نموذجاً هجيناً بين الخوارزمية الجينية والشبكة العصبية المتكررة لكشف الشذوذ الشبكي؟
- ✍ ما مدى كفاءة وموثوقية وملاءمة النموذج المقترح في تحديد الشذوذ الشبكي؟

4.1. أهمية البحث

تقدمت الجريمة الإلكترونية بمعدل تقدم التقنيات الناشئة نفسه. وفقاً لـ Statista، بلغ متوسط تكلفة خرق البيانات في الولايات المتحدة وحدها حوالي 2 مليون دولار في عام 2020. يجب على مسؤولي تكنولوجيا المعلومات مراقبة المستخدمين بشكل مستمر. المراقبة الدائمة لكشف السلوكيات الشاذة في الوقت الفعلي تقلل التكاليف. تعد الـ UBA الآن جزءاً لا يتجزأ من أمن تكنولوجيا المعلومات. تنفيذها أمر بالغ الأهمية لأي منظمة لمنع الانتهاكات الأمنية. تقلل هذه التقنية إلى حد كبير الوقت المستغرق لاكتشاف الهجمات الإلكترونية والاستجابة لها. تحدد المخاطر التي تفوقها الحلول التقليدية في الوقت الفعلي مما يجعلها تقنية ملائمة لمتطلبات المؤسسات.

5.1. بنية الرسالة

قمنا بتقسيم الرسالة إلى سبعة فصول على النحو الآتي:

الفصل الأول "مقدمة عامة": كما لاحظنا فقد عرضنا في هذا الفصل تمهيداً لمضمون الرسالة ووضحنا الحاجة إلى وجود الأمن السيبراني وضمان وجود تقنيات حديثة للتصدي للهجمات مثل تقنية الـ UBA. بالإضافة إلى ذلك طرحنا مشكلة البحث، أهدافه وأهميته. عرضنا محتويات الرسالة وتقسيماتها.

الفصل الثاني "تكاء صناعي": يوضح هذا الفصل مفهوم الـ AI بالإضافة إلى لمحة بسيطة عن فرعيه تعلم الآلة والتعلم العميق وبعضاً من خوارزمياتهما.

الفصل الثالث "الأمن السيبراني": يذكر لمحة عن الأمن السيبراني ويعرض أهم أنواعه. كما أنه يركز على أمن الشبكة وعرض نموذج الـ OSI. يعرض أيضاً بعضاً من تقنيات الأمن السيبراني وبالطبع يوضح مفهوم الشذوذ. **الفصل الرابع "تحليلات الأمان":** يشرح المفهوم النظري لتقنية الـ UBA من حيث المفهوم والمكونات ونقاط الضعف والقوة وغيرها من المفاهيم، كما يوضح الفرع الأب للتقنية.

الفصل الخامس "الخوارزميات المستخدمة في تقنية الـ UBA": يعرض بعضاً من الخوارزميات المستخدمة في التقنية لكشف الشذوذ الشبكي، بالإضافة إلى الدراسات السابقة لتلك الخوارزميات بشكل واسع ومفصل.

الفصل السادس "النموذج المقترح": يشرح الخوارزميات التي قمنا باستخدامها في نموذجنا المقترح، يوضح البيانات المختارة ويشرحها ويعرض النموذج المقترح بشكل مفصل مع النتائج التي حصلنا عليها.

الفصل السابع "الخاتمة والرؤى المستقبلية": يعرض أهم النتائج والتوصيات بالإضافة للخاتمة والرؤى المستقبلية.

الفصل الثاني

الذكاء الصناعي

1.2. مقدمة

اخترع الإنسان منذ العصور القديمة حتى العصور الحديثة العديد من الاختراعات التي اثبتت فائدتها للبشرية. واحدة من أهم الاختراعات هو الحاسوب والذي لعب دوراً مهماً في تخفيف الأعباء على الإنسان [19]. للحاسوب قدرة على معالجة البيانات بسرعة غير مسبوقة. مع مرور الوقت بدأ العلماء في التفكير في زيادة قدرة الحاسوب. الاتجاه كان لمحاكاة القدرات البشرية مثل التعلم والتفكير وليس فقط تنفيذ التعليمات الموجهة له. بدء توجه العلماء لمحاولة بناء آلات قادرة على تقليد البشر. هذه المحاولات كان لها دوراً حاسماً في نشأة الـ AI الذي كان نتاج دراسات دقيقة لسلوك الإنسان وطريقة تفكيره ومن ثم محاولة تنفيذها على شكل خوارزميات.

يتضمن هذا الفصل عرضاً لمفهوم وأنواع وبعض فروع الـ AI في كلاً من 2.2 و 3.2 و 4.2. حيث يتم توضيح ما هو الـ AI وتاريخ نشأته وشرحاً بسيطاً عن أنواعه وذكر بعضاً من خوارزمياته.

2.2. مفهوم الذكاء الصناعي (Artificial Intelligence Concept) [19]

الـ AI هو فرع من فروع علم الحاسوب الذي يهدف إلى تطوير الأنظمة التي تحاكي القدرات البشرية. الهدف هو تقديم أنظمة حاسوبية ذكية لها القدرة على الفهم، الإدراك، التحليل والتعلم. كلمة ذكاء تعني محاكاة قدرة التفكير بينما كلمة صناعي تعني من صنع البشر. تم توظيف الـ AI في مجالات عديدة مثل إدارة الأعمال، الفضاء، الدفاع والصحة. بينما أسهمت فيه العديد من المجالات مثل الرياضيات لتطوير الخوارزميات، علم الأحياء، علم الأعصاب لدراسة عقل الإنسان وسلوكه وأخيراً علم الحاسوب وهو العلم المسؤول عن تشغيل الخوارزمية.

بداية الخوارزميات كانت بهدف تتبع مخزون الحبوب والماشية. بدأ العلماء اليونانيون في عصر إقليدس وأرخميدس في صنع خوارزميات معقدة تتمثل على شكل خطوات. لم يكن لهذه الخطوات اسم محدد إلى أن جاء الخوارزمي في القرن التاسع وابتكر اسم الخوارزمية (Algorithm) [27]. أخذ تطور الخوارزمية في تسارع عندما بدأ تطور علم الرياضيات، ومع ذلك فإن قدرات الحاسوب والخوارزميات لم تتجاوز حداً معيناً. في يوم من أيام عام 1950 طرح آلان تورينغ (Alan Turing) استفساراً ألا وهو متى ستبدأ الآلات تتنافس البشر في المجالات الفكرية؟ وهل للآلات قدرة على التفكير؟ يمكن اعتبار هذا السؤال بداية مجال الـ AI [27]. إن أول آلة تم تصميمها

لتمثل شبكة عصبية بسيطة كانت في عام 1951 وذلك من قبل كل من مارفن منسكي (Marvin Minsky) ودين إدموند (Dean Edmond). أما ابتكار اسم (Artificial Intelligence) فكان في عام 1955 على يد جون مكارثي (John McCarthy). في عام 1969 عرضت شركة SRT العالمية¹ ولأول مرة روبوت يستخدم الـ AI يدعى Shakey.

3.2. أنواع الذكاء الصناعي (Types of Artificial Intelligence)

يمكن تصنيف الـ AI وفق خصائص معينة إلى نوعين: نوع قائم على القدرات ونوع قائم على الوظيفة. سنعرض هذين النوعين في الفقرات الآتية [19].

1.3.2. القائم على القدرات (Capabilities Based)

في الواقع، يتم تصنيف الذكاء الصناعي القائم على القدرات بدوره إلى ما يلي:

- ✍ **الضيق (Narrow):** النوع الذي يستطيع تنفيذ مجموعة من التعليمات المحددة دون القيام بأي نوع من أنواع التفكير، وهو النوع المستخدم في الأجهزة الحالية جميعها ويسمى أيضاً بالذكاء الضعيف.
- ✍ **العام (General):** النوع الذي يستطيع العمل مثل البشر فهو قادر على التفكير والتحليل بالقدرة البشرية نفسها. لكنه للأسف غير موجود حالياً وقد يصبح متاحاً في المستقبل القريب ويسمى كذلك بالقوي.
- ✍ **الفائق (Strong):** النوع الذي يستطيع أن يتفوق على القدرة البشرية من حيث التفكير، وهو نوع افتراضي لا وجود له حالياً ولكنه يشكل خطراً كبيراً في حال أصبح واقعاً ملموساً.

2.3.2. القائم على الوظيفة (Functionality Based)

يتم تصنيف الذكاء الصناعي القائمة على الوظيفة بدوره إلى ما يلي:

- ✍ **الآلات التفاعلية (Reactive Machines):** تعمل اعتماداً على بيانات محدودة وموجودة بمجموعة محددة مسبقاً أو تكون بيانات حالية. بمعنى آخر هذه الآلات لا تستطيع تخزين بيانات سابقة ومن الأمثلة على هذه الآلات ألفا غو² Alpha Go.
- ✍ **الذاكرة المحدودة (Limited Memory):** يمكن لهذه الأجهزة تخزين التجارب السابقة أو التخزين في الذاكرة لكن لمدة محدودة من الزمن. مثال عليها السيارات ذاتية القيادة (self-driving cars).

1 منظمة ومعهد أميركي غير ربحي للبحث العلمي مقرها الرئيسي في كاليفورنيا، تأسست عام 1946.

2 برنامج طُوّر من قبل الشركة البريطانية للذكاء الصناعي غوغل ديب مايند (Google DeepMind) عام 2015 ليصبح أول برنامج يهزم لاعب بشري محترف بلعبة غو وهي لعبة تشبه الشطرنج على لوحة مقسمة لـ 19 سطرًا وعمودًا.

☞ **نظرية العقل (Theory of Mind):** هي آلات أكثر تطوراً من سابقتها فهي قادرة على فهم القدرات العقلية والعاطفية للبشر. حالياً هي آلات غير موجودة لكن يعمل العلماء على تطوير مثلها في المستقبل.

☞ **الوعي الذاتي (Self-Awareness):** وهي آلات ذات مفهوم افتراضي لا وجود لها وتتفوق على الآلات التي في نظرية العقل، وهي تمثل آلات خارقة الذكاء.

بعد التعرف على أنواع الـ AI لابد من التطرق إلى فروع هذا المجال. فيما يلي سوف نحدد بعض هذه الفروع.

4.2. فروع الذكاء الصناعي (Branches of Artificial Intelligence)

للـ AI فروع عديدة نذكر منها [19]:

☞ **النظم الخبيرة (Expert Systems).**

☞ **الروبوتات (Robotics).**

☞ **تعلم الآلة (Machine Learning).**

☞ **التعلم العميق (Deep Learning).**

النظم الخبيرة هي أنظمة تستطيع اتخاذ القرار. الروبوتات هو تطوير آلات ذكية على شكل روبوت تطيع أوامر البشر. لكن في دراستنا سوف نركز على تعلم الآلة والتعلم العميق. يمكن تشبيه الـ AI بالعقل وتعلم الآلة هو الذي يستطيع الـ AI من خلاله اكتساب قدرات معرفية جديدة. من جهة أخرى تأتي أهمية التعلم العميق كونه أحد أساليب تعلم الآلة الأكثر تقدماً وفاعلية للتدريب الذاتي [38].

1.4.2. تعلم الآلة (Machine Learning, ML) [38]

يتم تعريف تعلم الآلة على أنه تطوير الخوارزميات التي تعطي الحاسوب القدرة على التعلم من التجربة والخبرات السابقة وذلك بتحليل البيانات. فالتعلم هنا يُستخدم لجعل الحاسوب يقوم بأعمال الإنسان ولكن بفاعلية أكثر. تُعطى الخوارزمية (الآلة) بعضاً من البيانات والتي تسمى عادةً ببيانات التدريب (Training Data). تقوم الآلة بتحليل البيانات مما يؤدي إلى التنبؤ بالمخرجات اعتماداً على المدخلات. تزيد كفاءة الآلة مع تقديم بيانات أكثر لها وهذا ما يسمح لها بالتطور والتعامل مع المشاكل المعقدة التي يصعب على الإنسان التعامل معها [19].

يتم تصنيف تعلم الآلة بحسب كيفية تعلم الخوارزمية على الشكل الآتي:

☞ **التعلم بإشراف (Supervised Learning):** في هذا النوع يتم تدريب الخوارزمية بإعطاء بيانات مصنفة ويكون الناتج محدداً مسبقاً. تقوم الخوارزمية بتوقع الناتج اعتماداً على المدخلات المصنفة، ثم مقارنة الناتج مع الناتج الفعلي ومحاولة تحسين عملية تحليل البيانات للحصول على مخرج أو ناتج جيد.

كلمة جيد تعني الأقرب للنتائج الفعلية. من مجالات استخدام الآلات التي تعتمد على هذا النوع من التعلم نذكر: التجارة، توقع الأسعار وتصفية البريد العشوائي.

✍ **التعلم بغير إشراف (Unsupervised Learning):** هنا البيانات المعطاة غير مصنفة والنتائج غير محددة. على الآلة تدريب نفسها من خلال البحث عن درجة التشابه بين تلك البيانات. تُحدد هذه الآلات الأنماط لإيجاد المخرج المناسب. من الاستخدامات لهذا النوع من التعلم الإعلان والتسويق الرقمي.

✍ **التعلم شبه الخاضع لإشراف (Semi Supervised Learning) [38]:** يتم إعطاء الكثير من البيانات غير المصنفة والقليل من البيانات المصنفة. وفقاً لهذا الخليط يعتبر نوع التعلم هذا ما بين التعلم بإشراف والتعلم بغير إشراف. من الملاحظ أن في نوع التعلم بإشراف هناك تدخل كبير للبشر بحيث تعتمد الخوارزمية على ما قدمه البشر لها. بينما في نوع التعلم بغير إشراف لا يوجد تدخل كبير من قبل البشر. هذا ما ينطبق أيضاً على التعلم شبه الخاضع لإشراف. بالإضافة لذلك، فإن قدرة هذا النوع على التعامل مع المشاكل أكبر بكثير. من أهم مجالات استخدام هذا النوع هو الصناعات الطبية وتحليل الكلام.

✍ **التعلم المعزز (Reinforcement Learning):** يعتمد على نظام التعلم بالتغذية الراجعة أي من خلال التجربة والخطأ، بحيث تتعلم الآلة كيفية تدريب نفسها وتستفيد من أخطاءها السابقة. يتم إعطاء الآلة مكافئة عند القيام بفعل مناسب، وإعطاءها عقوبة عن قيامها بفعل غير مناسب. هذا الأسلوب يساعد الآلة على التطور وإعطاء نتائج أفضل. يُنصح باستخدام هذا النوع عند عدم وجود بيانات كافية أو غير متناسقة. من الأمثلة على استخدام هذا النوع من الآلات نذكر السيارات ذاتية القيادة والكلب الآلي.

1.1.4.2. بعض خوارزميات تعلم الآلة

التعلم بإشراف والتعلم بغير إشراف هي أكثر الأنواع التي تهتمنا لذلك سوف نستعرض خوارزميات كلا النوعين.

✍ **التعلم بإشراف (Supervised Learning)** ويقسم لفئتين [17]:

• **التصنيف (Classification):** يستخدم عندما تكون المخرجات منفصلة ومن خوارزمياته:

- آلة شعاع الدعم (Support Vector Machine, SVM) وهذه الخوارزمية سوف نهتم بشرحها في الفصل الخامس.
- بايز الساذج (Naïve Bayes) أو تسمى بايز نايف.
- أقرب جار (K-Nearest Neighbor, KNN).
- شجرة القرار (Decision Tree).

- الغابات العشوائية (Random Forests, RF).
 - الانحدار اللوجستي (Logistic Regression).
 - الانحدار (Regression) يستخدم عندما تكون المخرجات منفصلة ومن خوارزمياته:
 - الانحدار الخطي (Liner Regression).
 - الانحدار الخطي المتعدد (Multiple Liner Regression).
 - ✍ التعلم بغير إشراف (Unsupervised Learning) ويقسم لفئتين [17]:
 - العنقدة (تجميع) (Clustering) ومن خوارزمياته:
 - التجميع بالمتوسط (K-means Clustering).
 - نموذج الخليط الغاوسي (Gaussian Mixture Model).
 - الارتباط (Association) ومن خوارزمياته:
 - خوارزمية الاستنتاج المباشر (Apriori Algorithm) أو ما تسمى بقواعد الارتباط.
 - نمو النمط المتكرر (Frequent-Pattern Growth, FP Growth).
- بعد أن تعرفنا على التعلم الآلي وبعض من خوارزمياته لننتقل لفرع التعلم العميق.

2.4.2. التعلم العميق (Deep Learning, DL) [19]

يعتبر التعلم العميق مجال فرعي من تعلم الآلة. يُستخدم في الـ DL شبكة عصبية صناعية لتنفيذ عمليات معقدة على كميات هائلة من البيانات. العمليات المطبقة تتم اعتماداً على ما يشابه قدرات وعمل الدماغ البشري. يتم تدريب الآلة باستخدام خوارزميات تتعلم بالأمثلة. مع تعدد طبقات الخوارزميات التي كانت في تعلم الآلة يصبح لدينا شبكة عصبية. بالتالي تتألف الشبكة العصبية من طبقات. تحوي كل طبقة عدداً من العقد العصبية يتراوح عددها من المئات إلى الآلاف [9]. تسمى الطبقة الأولى من الشبكة بطبقة المدخلات (Inputs Layer). أما الطبقة الأخيرة تسمى طبقة المخرجات (Outputs Layer)، والطبقات المتوسطة بين هاتين الطبقتين الأولى والأخيرة توصف بالطبقات الخفية (Hidden Layers).

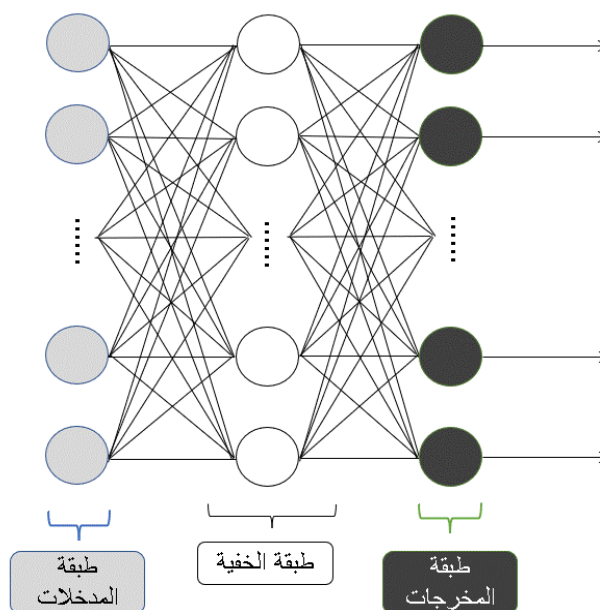
تكون الطبقات مترابطة بعضها مع بعض، وزيادة عددها يزيد من كفاءة الآلة. هذا العدد يعبر عن عمق الشبكة (Depth of the Network). بالطبع الشبكة العصبية قادرة على العمل على بيانات غير منتظمة ولا تحتاج لبيانات محددة مسبقاً ولذلك لابد من كمية كبيرة من البيانات تدعى عادةً (Big Data).

أول نموذج لشبكة عصبية كان في عام 1943 على يد وارن ماكولوتش (Warren McCulloch) مع والتر بيتس (Walter Pitts). ثم عمل فرانك روزينلات (Frank Rosenblatt) على نموذج البيرسبتون (Perceptron) عام 1958 ومن بعدها تتالت الأبحاث حتى عصرنا الحالي [9].

1.2.4.2. أنواع الشبكات العصبية (Types of Neural Networks)

يمكن تصنيف الشبكة العصبية إلى نوعين كما يلي [19]:

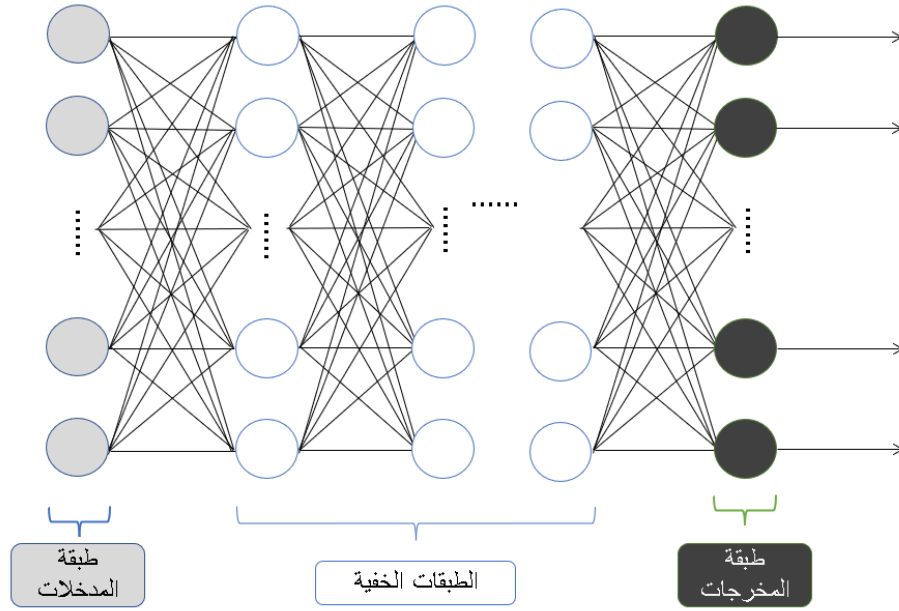
✍️ **الشبكة العصبية الضحلة (Shallow Neural Network):** تتألف الشبكة الضحلة من طبقة واحدة خفية فقط وتسمى أحياناً بالشبكة العصبية السطحية. يوضح الشكل 1.2 بنية الشبكة العصبية الضحلة.



الشكل 1.2 بنية الشبكة العصبية الضحلة.

✍️ **الشبكة العصبية العميقة (Deep Neural Network-DNN):** تتألف الشبكة العميقة من عدد كبير من الطبقات الخفية. يوضح الشكل 2.2 بنية الشبكة العصبية العميقة.

في عام 1990 كانت تعتبر الشبكة العصبية التي تحوي أكثر من طبقتين خفيتين شبكة عميقة، في حين أن الشبكة التي تملك طبقتين خفيتين فقط تُعتبر غير عميقة [18]. بينما يعتبر [19] أن الشبكة العصبية الضحلة تتكون من طبقة خفية واحدة فقط، والشبكة العميقة يجب أن تحوي على طبقتين خفيتين فأكثر. يمكن أن نبرر هذا الاختلاف من حقيقة كون التعامل مع عدد الطبقات الخفية الكبير، الذي قد يصل للعشرات أو المئات، أمر معتاد. بالتالي استخدام طبقتين أو حتى ثلاث طبقات خفية لم يعد يعبر عن العمق مقارنةً بالمئات. لكن سنعتبر أنه ابتداءً من طبقتين خفيتين يصبح لدينا شبكة عصبية عميقة.



الشكل 2.2 بنية الشبكة العصبية العميقة.

يوجد العديد من الأمثلة عن الشبكات العصبية بنوعها الضحلة والعميقة والتي نذكر أهمها [9]:

✍ **الشبكة العصبية ذات التغذية الأمامية (Feed-Forward Neural Network)** [19]: تنتقل

البيانات فيها باتجاه واحد من طبقة المدخلات إلى طبقة المخرجات دون تكرار أو عودة.

✍ **الشبكة العصبية المتكررة (Recurrent Neural Network, RNN)**: وهي التي تكرر فيها عملية

انتقال البيانات التي تمر من طبقة المدخلات إلى طبقة المخرجات عبر الزمن. التكرار هذا يولد ذاكرة يمكن

الاحتفاظ بها بالمدخل السابق وتذكره. تسمح الذاكرة بالتعلم من البيانات وتحقيق نتائج أفضل. سنقوم بشرح

هذه الشبكة بالتفصيل في الفصل الخامس من الرسالة.

✍ **الشبكة العصبية الملففة (Convolutional Neural Network, CNN)**: وهي الشبكة الأكثر

استخداماً في معالجة الصور. تم إنشاؤها لأول مرة على يد يان ليكون (Yann LeCun) عام 1988

وسماها حينها باسم LeNet.

✍ **الشبكة ذات الذاكرة طويلة (قصيرة) المدى (Long (Short) Term Memory, LSTM)**: وهي

نوع من أنواع الشبكة RNN ولكن لها القدرة على متابعة مسار البيانات لوقت طويل مما يجعلها أعقد.

هذه الشبكة من الشبكات التي سوف يتم التطرق لها في الفصل الخامس من الرسالة.

✍ إدراكات متعددة الطبقات (Multilayer Perceptron, MLP): وهي نموذج مطور من نموذج

Perceptron الذي تحدثنا عنه في الفقرة 2.4.2. المصمم على يد فرانك روزينلات.

الجدير بالذكر أن خوارزميات الـ ML قد تتطلب التدريب على مجموعة بيانات صغيرة، لكن تحتاج لمساعدة بشرية أكثر. أي يتم فيها إعطاء الآلات بيانات مصنفة وفق تصنيفات بشرية. بينما خوارزميات الـ DL لا تتطلب الكثير من المساعدة البشرية، لكنها في الوقت نفسه تحتاج بيانات كبيرة للتدريب [38].

6.2. خلاصة الفصل

قدمنا في هذا الفصل توضيح مفهوم الـ AI مع توضيح لأنوعه وأهم فروع. ركزنا بالحديث على فرعين أساسيين وهما تعلم الآلة والتعلم العميق. ذكرنا طرق التعلم في تعلم الآلة وبعضاً من خوارزمياته. بالطبع ستكون لدينا عودة لبعض خوارزميات تعلم الآلة كما أوضحنا وذلك في الفصل الخامس لشرحها بالتفصيل. شرحنا اعتمادية التعلم العميق على ما يسمى بالشبكة العصبية وذكرنا أبرز تلك الشبكات. لقد ذكرنا سابقاً عن أهمية تطبيق خوارزميات الـ AI في الأمن السيبراني ولأننا في هذا الفصل تحدثنا عن الـ AI فلا بد من أن نوضح مفهوم الأمن السيبراني، وهذا ما سوف نعرضه في الفصل القادم.

الفصل الثالث

الأمن السيبراني

1.3. مقدمة

يُعتبر الأمن السيبراني من العلوم المهمة جداً لأي مؤسسة أو شركة أو جهة حكومية أو حتى مستخدم فردي وذلك لحماية البيانات من الوصول غير المصرح به. العديد من المؤرخين والكتاب يرجعون أصل كلمة سايبير إلى نوربيرت وينر (Norbert Wiener) وذلك للتعبير عن التحكم الآلي. يعد وينر الأب الروحي المؤسس للسيبرنتيقية والتي تعني التحكم والتواصل بين الآلة والإنسان أو الحيوان وذلك بحسب وصفه للمصطلح من خلال مؤلفه في عام 1949 ("Cybernetics or Control and Communication in the Animal and Machine") فكان أول من استخدم هذا المصطلح في ذلك الوقت [4]. منذ ذلك الحين بدء مجموعة من العلماء في الفترة الممتدة بين خمسينيات وستينيات القرن العشرين باستخدام مصطلح سيبرنتيك. ثم تركز لاحقاً الاهتمام تدريجياً بمحاولة التصدي للهجمات. لا يمكن تحديد بدقة بداية الأمن السيبراني، إلا أن بداية سبعينيات القرن الماضي كانت مرحلة فارقة في تاريخ الأمن السيبراني. ففي عام 1971 قدم بوب توماس (Bob Thomas) أول برنامج حاسوب شبيه بالفايروس يدعى Creeper. بينما في عام 1972 ظهر أول مضاد فايروس يدعى Reaper بواسطة راي توملينسون (Ray Tomlinson). تم تطبيق هذا الفايروس ومن ثم مضاده على شبكة ARPANET¹ [16].

يتضمن هذا الفصل في الفقرة 2.3. تعريف الأمن السيبراني والفرق بينه وبين أمن المعلومات. ذكر بعضاً من أنواع الأمن السيبراني في الفقرة 3.3. التي تحوي شرحاً بسيطاً عن كل نوع. كوننا سنركز على أمن الشبكة لذلك سوف نتحدث عن الشبكة في الفقرة 4.3. التي توضح مفهومها وتصنيفها وبالإضافة للمحة عن النموذج المرجعي وشرح للطبقات السبع وأخيراً بعضاً من تقنيات حماية الشبكة. في نهاية الفصل سنتطرق لمفهوم الشذوذ وذلك ضمن الفقرة 5.3. والتي سوف تحوي على شرح لأنواع الشذوذ وبالإضافة لذكر بعض الطرق التي تُعتمد لكشفه.

2.3. مفهوم الأمن السيبراني (Cyber Security Concept)

الأمن السيبراني هو مجموعة التقنيات والعمليات المصممة بهدف حماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو السرقة أو الوصول غير المصرح به [4]. يشمل حماية الأجهزة كما يفعل مع البيانات مثل حماية

¹ شبكة وكالة مشاريع الأبحاث المتقدمة أو المتطورة (Advanced Research Projects Agency Network) اختصاراً ARPANET وهي أول شبكة حاسوب ومن أوائل الشبكات لنقل البيانات وتم إطلاقها عام 1969 في الولايات المتحدة الأمريكية.

الوسيط الذي يحمل البيانات أو تنتقل عبره. في حين عرفه إدوارد أمورسو (Edward Amoroso) على أنه وسائل للحد من خطر الهجوم على البرمجيات، أجهزة الحاسوب أو الشبكات. من هذه الوسائل نذكر الأدوات المختصة لمواجهة القرصنة وكشف الفايروسات [8]. كلمة (Cyber) هي كلمة يونانية تطلق على كل ما يتعلق بشبكة الحاسوب والإنترنت (Internet) والتطبيقات المختلفة والخدمات الإلكترونية [4]. تعددت التعريفات والمفهوم واحد فكان لنا في هذه الدراسة تعريف الأمن السيبراني على أنه مجموعة الإجراءات المتبعة للحفاظ على أمن الأجهزة والشبكات من أي نشاط يهدف إلى تهديد هذا الأمن.

تطورت تقنيات الأمن السيبراني بسرعة تطور أشكال وطرق الهجمات نفسها. أصبحت هذه التقنيات محط اهتمام الدول الكبرى وخاصة لما تساهم به في مجال الأمن القومي وارتباطها حتى في المجال السياسي.

1.2.3. الفرق بين الأمن السيبراني وأمن المعلومات

نشأ مجال أمن المعلومات (Information Security) عندما بدأت أجهزة الحاسوب بمختلف أنواعها باحتواء معلومات مهمة، وبالإضافة لوجود معلومات محفوظة بطرق مختلفة خارج نطاق الحاسوب، بدأ الاهتمام بحماية هذه المعلومات بشتى أنواعها. يُعرف أمن المعلومات على أنه مجموعة الإجراءات التي تُستخدم للمحافظة على المعلومات وسريتها ويبحث عن الأساليب لضمان حمايتها. يشمل أمن المعلومات العناصر الآتية [1]:

✍ **السرية (Confidentiality):** منع الوصول إلى المعلومات إلا من قبل الأشخاص المخول لهم وتحديد صلاحيات التعديل والحذف والإضافة.

✍ **التكامل وسلامة المحتوى (Integrity):** أن تكون المعلومة صحيحة عند إدخالها ولم يتم تغييرها.

✍ **التوافر والإتاحة (Availability):** إبقاء المعلومة متوفرة للمستخدم في أي وقت وعدم تعطل ذلك بسبب خلل في الأنظمة ووسائل الاتصال.

من الممكن اعتبار الأمن السيبراني فرعاً من فروع أمن المعلومات. إلا أنه مع التطور والتقدم أصبح أمن المعلومات يهتم بحماية البيانات والمعلومات بشقيها الإلكتروني والورقية وذلك من أي تهديد خارجي أو داخلي على خلاف الأمن السيبراني الذي يركز على حماية البيانات والمعلومات المخزنة إلكترونياً. بمعنى آخر ضمن الفضاء السيبراني أو الإلكتروني (Cyber Space) فقط [4]. الفضاء السيبراني هو شبكة مترابطة تتألف من الإنترنت وكل الأجهزة المتصلة بها بما في ذلك المعالجات، وهو مصطلح لعالم افتراضي مجرد وغير ملموس [26]. بالتالي عند الحديث عن البيانات المخزنة على الأجهزة والشبكات المتصلة بالإنترنت يكون التوجه للأمن السيبراني. طور الأمن السيبراني تقنيات عديدة وأصبح في هذا النطاق أوسع من أمن المعلومات ويعد خط الدفاع الأول. إلا أن

الأمن السيبراني لا يملك وسيلة لحماية البيانات والمعلومات غير المحفوظة إلكترونياً الأمر الذي يتميز به أمن المعلومات. يمكن القول إن القاسم المشترك بين أمن المعلومات والأمن السيبراني هو حماية المعلومات. أمن المعلومات يهتم بحمايتها أينما كانت، لكن الأمن السيبراني يركز على حمايتها ضمن نطاق شبكة الإنترنت [5].

3.3 أنواع الأمن السيبراني (Types of Cyber Security)

نظراً لتشعب الوسائط التي تنتقل عبرها البيانات كان لابد من وجود أنواع عديدة للأمن السيبراني وذلك تبعاً للوسيط الذي يحفظ أو ينقل البيانات ونذكر أهمها وأكثرها شمولية:

✍ **أمن الشبكة (Network Security) [4]:** وهو النوع الذي يُعنى بإبقاء شبكة الحاسوب محمية من البرامج الضارة أو القرصنة والمتسللين. يتم ذلك من خلال تطبيق مجموعة من التقنيات مما يجعل الشبكات فضاءً آمناً لمشاركة البيانات وتبادلها.

✍ **أمن التطبيقات (Application Security) [4]:** وهي التطبيقات المتصلة بالإنترنت مما يجعلها عرضة للاختراقات. يتم اتخاذ مجموعة من الإجراءات، ثم جعل المستخدم يشارك التطبيق من خلال حزمة التطبيقات ويثبت التطبيق من مصدر جدير بالثقة.

✍ **أمن الهواتف المحمولة (Mobile Security) [26]:** مثل الأجهزة اللوحية والمحمولة مهددة بالوصول للبيانات الشخصية أو هجمات تهدد أنظمة التشغيل. القدرة على الوصول لمثل هذه الأجهزة بشكل غير مصرح به قد يسبب فقدان للبيانات أو تلف الجهاز. لقد كان الأمن السيبراني بالمرصاد لها وتم العمل على مجموعة من التقنيات. أصبحت هواتف موظفي المؤسسات والشركات تملك صلاحية الوصول لنظام المؤسسة وبياناتها لضمان حماية هذه البيانات.

✍ **أمن السحابة (Cloud Security) [26]:** أصبح تخزين البيانات السحابية أمراً شائعاً، حيث بدأت كافة المؤسسات تعمل على تقنيات سحابية. تتضمن عملية حماية السحابة مجموعة من الاستراتيجيات وشروط من كيفية الوصول والتحكم بها وتوزيع بياناتها وغيرها.

✍ **الأمن التشغيلي (Operational Security) [4]:** يشمل العمليات والقرارات المتخذة للتحكم في البيانات وحمايتها مثل أذونات المستخدم¹ (User Permissions). عند الوصول إلى الشبكة أو مجموعة العمليات يُحدد متى وأين يتم تخزين البيانات.

1 تعني الأذونات قدرة التطبيق على الوصول للمعلومات والبيانات

☞ أمن إنترنت الأشياء (IoT Security) [26]: يقصد بإنترنت الأشياء مجموعة الأجهزة التي تتواصل بعضها مع بعض وتعمل متصلة بالإنترنت مثل السيارة ذاتية القيادة.

بالتأكيد يوجد المزيد من الأنواع التي تعتبر ذات فاعلية ولكن تبقى الأنواع المذكورة أعلاه هي الأكثر شيوعاً. الجدير بالذكر أن محور دراستنا يتركز على تقنية من تقنيات أمن الشبكة فحري بنا التطرق إليها وتوضيح مفهوم الشبكة والأجهزة المتعلقة بها. لكن لابد من الإشارة إلى أن التقنية المعتمدة في دراستنا ألا وهي الـ UBA لا يقتصر عملها وتطبيقها ضمن نطاق الشبكة فحسب بل يمكن تطبيقها أيضاً ضمن أمن التطبيقات.

4.3. الشبكة (Network)

عُرفت الشبكة حسب [8] بأنها ترابط بين جهازين أو أكثر وقد يكون هذا الترابط بوصلات مثل الأسلاك أو باستخدام أجهزة ما وتتألف الشبكة من عقد. العقدة هي مكون للشبكة لتنفيذ مهمة محددة ويمكن للعقدة أن تكون جهاز حاسوب أو أجهزة توجيه أو طابعات وغيرها. بتعريف أبسط كما ذكر في [7] الشبكة هي مجموعة الأجهزة (العقد) المترابطة بعضها مع بعض باستخدام وسائل اتصال مادية أو برمجية. يمكن للعقدة أن تكون حاسوباً أو أي جهاز قادر على إرسال واستقبال المعطيات.

الهدف من الشبكة هو التمكن من تبادل البيانات (Data) والاستفادة من الخدمات التي توفرها الأجهزة وهذه الخدمات تسمى الموارد (Resources) [7]. الموارد هي الخدمات المتاحة التي يمكن لمستخدم الشبكة الحصول عليها مثل الحصول على معلومات أو تبادل ملفات أو تخزين بيانات أو استخدام الطابعة.

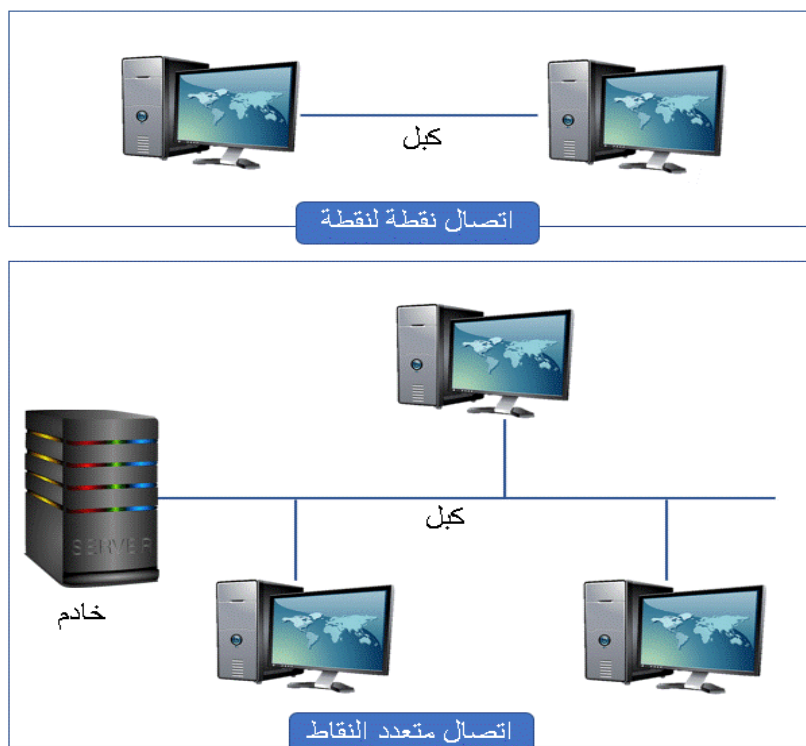
تُعرف البيانات على أنها كيان مادي ملموس يتمثل في شكل نبضات إلكترونية تُخزن بوسائط محددة لتتأقلمها ويمكن تقديرها وقياسها [8]. يقصد بذلك أن البيانات هي المدخلات إلى الحاسوب (Inputs) أما المعلومات هي المخرجات (Outputs) الناتجة عن معالجة تلك البيانات وهي ما يمكن للمستخدم الحصول عليها.

حقيقة الأمر أن تبادل البيانات يتم بين الأجهزة المختلفة وذلك عن طريق التطبيقات الموجودة في تلك الأجهزة. فمثلاً ليكن لدينا مستخدم ما يريد إرسال عبارة محددة لمستخدم آخر بالتالي من الأجهزة المستخدمة هنا هو جهاز الحاسوب والتطبيق المستخدم هنا هو تطبيق البريد الإلكتروني مثلاً. الجملة المرسله سوف تُرسل على شكل سلسلة من البتات (Bits) من المجموعة {0,1}. تمثل هذه البتات البيانات المتبادلة بين طرفي الاتصال وتكون مخزنة في ذاكرة الحاسوب. يتم إرسال البيانات كإشارة كهربائية رقمية على شكل قيم متتالية عبر الزمن من البتات. هذه الإشارة تتعرض للكثير من التغييرات قبل وصولها إلى المستقبل [7]. تجدر الإشارة هنا إلى كون الاتصال السابق بين جهازين كبل (Cable) يرتبط طرفه الأول بالمرسل والآخر بالمستقبل. بطبيعة الحال نقل البيانات يتم بين عدة

أجهزة وهذه هي الحالة الشائعة. يعتبر نقل البيانات بين عدة أجهزة غير قابل للتطبيق غالباً نظراً للمسافات البعيدة بين الأجهزة المعنية بنقل البيانات المطلوبة وهذا ما يأخذنا لتحديد نوع الاتصال [7]. يمكن تصنيف أنواع الاتصال بحسب عدد الأجهزة المؤلفة للشبكة إلى نوعين [2]: الأول هو الاتصال نقطة لنقطة (Point to Point) أما الثاني هو الاتصال متعدد النقاط (Multi Point) على الشكل الآتي:

✍ **الاتصال نقطة لنقطة (Point to Point):** يتم هذا الاتصال عبر كبل بين جهازين كما في مثالنا السابق وهو طريقة اتصال نادرة الاستخدام.

✍ **الاتصال متعدد النقاط (Multi Point):** هذا النوع هو الأكثر شيوعاً والذي يتم عن طريق مشاركة أكثر من جهاز على كبل واحد فقط.



الشكل 1.3. طريقة اتصال الأجهزة ضمن الشبكة.

يوضح الشكل 1.3. طريقة الاتصال ضمن الشبكة بشكله الأبسط. هنا من البديهي طرح السؤال الآتي هل هناك طريقة محددة لتوصيل الشبكة؟ وما إذا كان هنالك نطاق جغرافي يمكن أن تقتصر عليه الشبكة بناءً على طريقة الاتصال والتوصيل؟ ومن هذا المنطلق تم تقسيم الشبكة وفق تصنيفات عديدة.

لفهم تصميم الشبكات وأجهزتها لابد من دراسة طبقات الشبكة التي توضح هيكلية الشبكات وكيف تم هذا التقسيم لهذا وُجد النموذج المرجعي OSI.

1.4.3. طبقات الشبكة (النموذج المرجعي OSI) [22]

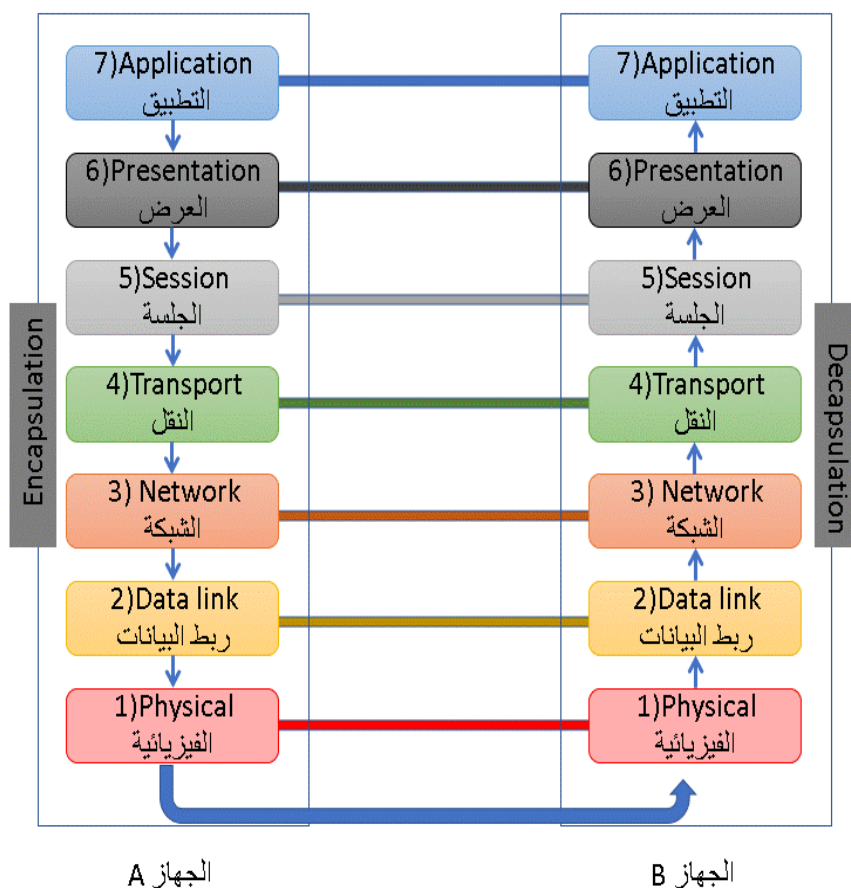
يُعرف النموذج المرجعي على أنه أسلوب تبسيط لهيكلية وتصميم الشبكات بحيث تم تقسيم الشبكة لسبع طبقات (Layers). يسمى هذا النموذج بالنموذج المرجعي الأساسي أو نموذج الطبقات السبع وذلك نسبةً للطبقات السبع، بالإضافة لمجموعة من البروتوكولات. بالطبع لقد أصبح يُعرف هذا التقسيم بنموذج OSI¹ وهو اختصاراً لعبارة (Open Systems Interconnection).

يهدف النموذج OSI لتسهيل عملية الاتصال ونقل البيانات بين نظامين (جهازين). كل طبقة تقدم وظائف محددة، بحيث تتعامل مع الطبقات الأدنى منها مباشرةً وتتيح وظائفها للطبقة الأعلى منها. كما تتكفل الطبقة بالتعامل مع الطبقة المشابهة لها (النند) في النظام الآخر أي مع الطبقة في المستوى نفسه. بالنسبة للبروتوكولات فبحسب [2] هي مجموعة قواعد للتحكم بالاتصال بين جهازين. أما في [7] فقد تم وصفها بأنها لغة تخاطب بين مكون لإحدى طبقات الشبكة على جهاز ما مع ما يقابلها من مكون الطبقة نفسها على جهاز آخر. أول بروتوكول تم استخدامه كان في نهاية عام 1970 [8].

تتم معالجة البيانات عبر الطبقات على الشكل الآتي: لنفترض أن التبادل هو بين الجهاز A المرسل والجهاز B المستقبل. عندها الاتصالات تحدث نزولاً وبدءاً من الطبقة الأعلى السابعة N في الجهاز A وهنا يتم تحويل البيانات إلى وحدة بيانات (البيانات التي يرغب البروتوكول بإرسالها). تُمرّر هذه الوحدة إلى الطبقة الأدنى منها أي N-1 والتي تقوم بإجراء التعديلات على البيانات وترسلها بدورها إلى الطبقة الأدنى N-2 وهكذا حتى تصل إلى الطبقة الأولى للجهاز A وتسمى هذه العملية بالتغليف (Encapsulation). في الطبقة الأولى للجهاز A يتم علاوةً على ذلك الإضافة والتعديل على البيانات وتنقلها للطبقة الأولى للجهاز B وهنا عملية الاتصالات في الجهاز المستقبل B بفك التغليف (Decapsulation) التي قامت به الطبقة المقابلة لها من الجهاز A. الطبقات في الجهاز B تقوم بسلسلة من فك التغليف حتى الوصول للطبقة السابعة في الجهاز B وهنا تعود البيانات العابرة التي

1 النموذج الربط البيئي للأنظمة المتقدمة الذي يصف ويحدد معايير اتصال الأنظمة الحاسوبية. تم تطويره من قبل المنظمة الدولية للمعايير SOI

تم إرسالها إلى شكلها الأصلي. يمكن القول إن التعديلات التي تطبق على البيانات هي عملية معالجة وأن الشكل التي تصل به إلى الطبقة السابعة للجهاز B تسمى معلومات والشكل 2.3. يوضح عملية المعالجة.



الجهاز A

الجهاز B

الشكل 2.3 معالجة البيانات عبر طبقات الشبكة في النموذج OSI.

ولتوضيح ذلك لابد من الدراسة المفصلة لكل طبقة [22]:

✍ **الطبقة الفيزيائية (Physical Layer):** الطبقة التي تستقبل وحدة البيانات من طبقة ربط البيانات وتحولها بالتقطيع إلى سلسلة من البتات $\{0,1\}$. يتم تحويل سلسلة البتات بالترميز (Encoding) لإشارات كهربائية أو ضوئية وإرسالها عبر كابل ناقل متصل بالوجهة الثانية (الجهاز الآخر). بالعكس تُعاد الإشارة المُستقبلية عبر الكابل لصيغة رقمية بفك الترميز (Decoding) وذلك بالجهاز المستقبل وثم تُرسل لطبقة ربط البيانات. بالطبع يوجد أنواع وثخانات مختلفة للكبل المستخدم. أما المكونات المهمة الموجودة في هذه الطبقة، بالإضافة للكابلات هي:

• **المكررات (Repeaters):** كل مكرر يقوم باستقبال الإشارات وإعادة توليدها لكونها تتعرض للخمود عند انتقالها عبر مسافة طويلة. لهذا السبب يُستخدم المكرر لمعالجة هذه المشكلة وبالتالي إمكانية ربط أجهزة بعيدة دون المعاناة من ضعف الإشارة.

• **المجمع (Hub):** هو مكرر له عدة منافذ (Ports) (فتحة للكابلات) بحيث يستقبل الإشارة من أحد المنافذ ويعيد توليدها ويرسلها على المنافذ الأخرى جميعها، وهو المستخدم في الشبكة النجمية.

✍ **طبقة ربط البيانات (Data Link Layer):** هي الطبقة المسؤولة عن تحويل البتات القادمة من الطبقة الفيزيائية إلى وحدات تدعى أطر أو إطار (Frames) في جهاز المستقبل، ثم إرسالها لطبقة الشبكة. بالعكس استقبال الوحدات من طبقة الشبكة وتحويلها بالتقطيع لأطر، ثم إرسالها للطبقة الفيزيائية في جهاز المرسل. كما يتم فيها إضافة تعريفية على البيانات تعرف عن مصدر ووجهة الجهاز الذي يتم إرسال واستقبال الأطر منه وهذا ما يسمى بالعنوان الفيزيائية (Physical Addressing). كما يتم فيها التحكم بالتدفق (كمية البيانات المرسل) والتحكم بالأخطاء في الأطر وغيرها من المهام. مكونات هذه الطبقة هي:

• **الجسر (Bridge):** تم اقتراح الجسر في بداية الثمانينيات قبل ظهور المجمعات. كانت مهمته قراءة الأطر الواردة إلى إحدى منافذه ومعرفة عنوان الوجهة المرسل لها وإرسال الأطر عبر المنفذ الذي يمكن عبره الوصول لتلك الوجهة، كون الجسر هو جهاز متعدد المنافذ. هذه العملية تدعى الابتدال (Switching)، وهذا المصطلح ظهر في نهاية التسعينيات.

• **المبدل (Switch):** المبدلات عالجت مشكلة التصادم عند إرسال البيانات عبر الأجهزة كون قدرة الجسر ضعيفة حينها في مثل هكذا مشاكل. زيادة عدد الجسور يؤدي لزيادة التصادمات. لكن مع وجود المبدل وهو جسر متعدد المنافذ، لم يعد زيادة عدد المبدلات يؤدي إلى زيادة عدد التصادمات. السبب بأن الجسر يحوي عدد محدد من المنافذ، مثلاً الحد الأقصى هو 16 بينما المبدل يمكن أن يتكون من مئات المنافذ. نلاحظ أن عملية الابتدال هذه يمكن اعتبارها ربط بين شبكتين بواسطة جسر (أو مبدل) وهذا أصبح دور الجسر (أو المبدل) مع الوقت.

✍ **طبقة الشبكة (Network Layer):** هي الطبقة التي تعمل على الاتصال مع طبقة النقل الأعلى منها وتستقبل منها وحدات البيانات. البيانات التي تستقبلها تقوم بتحويلها بالتقطيع لما يُعرف بالرمز (Packets) أو الطرود (Parcel) وذلك في الجهاز المرسل. تُرسل بطورها الرزم للطبقة الأدنى وهي طبقة ربط البيانات.

أما في الجهاز المستقبل فتتم العملية بشكل معاكس، حيث تستقبل هذه الطبقة الأطر من طبقة ربط البيانات وتحولها لرزم ومن ثم تنقلها للطبقة الأعلى وهي طبقة النقل. بالطبع يتم التواصل بين طبقة الشبكة في الجهاز المرسل وطبقة الشبكة في الجهاز المستقبل كما يحدث في الطبقات كلها. يضمن هذا التواصل التأكد من وصول الرزم بالشكل الصحيح والمكان الصحيح.

كما ذكرنا سابقاً فإن العنوان التي كانت تحدث في طبقة ربط البيانات هي عنوان فيزيائية وخاصة بالشبكة، بالتالي فهي محلية ولا معنى لها خارجها. أما في طبقة الشبكة فيوجد ما يسمى بالعنوان المنطقية (Logical Addressing) التي تُحدد وجهة الرزم وهي عامة لكل الشبكات. أحد العناوين المنطقية هي IP addresses. من الأجهزة المستخدمة في هذه الطبقة:

- **الموجه (Router):** هو الجهاز المسؤول عن قراءة العنوان والتحكم بعملية إرسال الرزم لوجهتها الصحيحة وربط الشبكات، كون إرسال الرزم يتم بين جهازين تابعين للشبكة نفسها أو شبكات مختلفة. الفرق الجوهرى بين الموجه والأجهزة الموجودة في الطبقات السابقة يكمن في حقيقة كون شرط الابتداء هو أن تكون الأجهزة مرتبطة بالشبكة ذاتها. أما الموجه لا يشترط أن تكون الأجهزة مرتبطة بالشبكة نفسها. يشارك الموجه بالعنوان وليس فقط قراءة العنوان. العناوين المستخدمة في شبكة الإنترنت هي IP addresses وهذا العنوان يُعطى للأجهزة وله عدد من الإصدارات. يُعد الإصدار الرابع IPv4 الأكثر استخداماً في حين أن الإصدار السادس IPv6 غير مستخدم بالرغم أنه مصمم لمعالجة المشاكل التي وُجدت في IPv4 والذي يتكون من 32 خانة (Bit) وكل خانة تأخذ قيمة من المجموعة {0,1}. لا يمكن لجهازين امتلاك عنوان الـ IP نفسه في الوقت نفسه ولكن العنوان يمكن أن يتم إعطائه لجهاز آخر بعد فترة. بمعنى أنه يتم تحريره من الجهاز الأول وإعطائه للآخر. بينما التمثيل المقروء هو التمثيل العشري المقسم لأربعة أقسام يحوي كل قسم أعداد قيمتها بين 0 و255 ويفصل بين كل قسم وآخر نقطة. فمثلاً التقسيم العشري 100.200.210.220 يقابل العنوان 01100100110010001101001011011100 ولكن لصعوبة قراءة العنوان بالأصفار والواحدات كان لابد من كتابتها بالتمثيل العشري. يقسم التمثيل العشري لقسمين¹ الأول من اليسار لمعرف الشبكة Network ID أو اختصاراً NID، والقسم الثاني من جهة اليمين لمعرف المضيف Host ID أو اختصاراً HID. تجدر الإشارة هنا أن الجهاز المضيف هو أي

1 معرف الشبكة هو الذي يحدد الشبكة التي تنتقل عبرها البيانات، معرف المضيف يحدد الجهاز التابع للشبكة الذي يرسل أو يستقبل هذه البيانات.

حاسوب أو جهاز متصل بالشبكة قد يكون مثلاً طابعة أو موجه وله عنوان من فضاء العناوين في طبقة الشبكة وإعطاء العنوان وهذا ما يسمى بالاستضافة. يمكن للجهاز القيام بمهام مختلفة منها تقديم موارد¹ (Resources) وعندها يسمى هذا الجهاز بالخادم² (Server). يمكن للمضيف أن يكون عقدة ضمن الشبكة إلا الأجهزة التي لا تملك عناوين مثل المبدلات أو المجمعات. نقول إن كل إصدار أو عنوان يحكمها بروتوكول يحدد عدد البتات أي N bit. لمعرفة المجموع الكلي للعناوين حسب البروتوكول نحسب 2^N وهذا العدد يسمى فضاء العنوان، وبالتالي في IPv4 لدينا 32 bit أي 2^{32} عنوان وهو ما يساوي 4,294,967,296 عنواناً.

✍ **طبقة النقل (Transport Layer):** تستقبل هذه الطبقة وحدات البيانات من الطبقة الأعلى (طبقة الجلسة). تحول البيانات التي تستقبلها بالنقطيع إلى مقاطع (Segments)، ثم تقوم بدورها بإرسالها للطبقة الأدنى (طبقة الشبكة). هذه العملية تحدث في الجهاز المرسل بينما تحدث في الجهاز المستقبل بشكل معاكس. لهذه الطبقة وظائف عديدة منها التحكم بالتدفق والأخطاء. في الطبقات السابقة تبادل البيانات من جهاز لجهاز لا تكون موثوقة فهي قد تحمل بعض الأخطاء أو لا تصل إلى وجهتها الصحيحة ولا في الترتيب الصحيح. طبقة النقل تحرص على التأكد من وصول البيانات إلى الوجهة المستلمة الصحيحة كما هي دون تلف أو نقصان وبالترتيب الصحيح. بالرغم من أنه يتم في الطبقة الثانية (طبقة ربط البيانات) معالجة الأخطاء، لكنها تعالج ما تلف في الطبقة الأولى (الطبقة الفيزيائية). بخلاف الطبقة الرابعة (طبقة النقل)، تتحكم الطبقة الثانية بالتدفق المتبادل بين الجهاز المرسل والمستقبل وتهتم فقط بكيفية نقل البيانات ولا تتأكد من وصول البيانات إلى الوجهة المستلمة كما لا تهتم بترتيبها.

✍ **طبقة الجلسة (Session Layer):** تهتم بإنهاء عمليات تبادل ونقل البيانات فمثلاً إرسال ثلاث رسائل مختلفة من قبل المستخدم في وقت متتالي تمثل ثلاث عمليات. تراعي هذه الطبقة وصول الرسائل الثلاث دون أن يحدث خلط. طبقة الجلسة لا تقوم بعملية نقل البيانات كما في الطبقات السابقة ولا تحوي بروتوكولات خاصة لها، وإنما تقوم بفصل العمليات وتنظيمها وتتأكد من وصولها بالشكل الذي يجب أن تصل به. تتيح هذه الطبقة إمكانية إرسال البيانات من الأجهزة بأي وقت حتى ولو في الوقت نفسه فتحفظ بصورة واضحة عما سيتم عرضه في واجهة المستخدم.

1 الموارد هي خدمات تقدمها الأجهزة كبيانات يطلبها متصفح الويب، خدمات تقدمها بعض الأجهزة كالتابعة أو أجهزة العرض وغيرها.

2 الخادم هو جهاز حاسوب ذو مواصفات عالية يقدم موارد وبالتالي كل خادم هو مضيف لكن العكس ليس صحيحاً.

✍ **طبقة العرض (Presentation Layer):** تصلها البيانات بشكلها النهائي في الجهاز المرسل. تقوم بتحويل النصوص المكتوبة في طبقة التطبيقات لبيانات يمكن تبادلها أي ل {0,1} وضغطها بسهولة تنقلها. تحول البيانات المستقبلية من الطبقات الأدنى إلى نصوص قابلة للعرض والقراءة في الجهاز المستقبل. أعني بذلك كمعلومات مفهومة يمكن عرضها بطبقة التطبيقات، بحيث الطرف المستقبل يفهم الرسالة بشكل صحيح. هذه الطبقة تقوم بدور المترجم. يمكن أن تكون تلك المعلومات صوراً أو فيديوهات وليس فقط نصوصاً. في النهاية يتم فك ضغط البيانات.

✍ **طبقة التطبيقات (Application Layer):** طبقة تواصل المستخدم مع التطبيقات مثل البريد الإلكتروني وتصفح الويب ونقل الملفات وغيرها.

كما هو معروف، فإن شبكة الإنترنت من أشهر الشبكات وأكثرها انتشاراً. كانت بدايتها في نهاية الستينيات القرن الماضي، وتحديداً مع شبكة (ARPANET). لكونها شبكة منتشرة تم تطوير نموذج خاص بها سمي نموذج الإنترنت (TCP/IP) ليكون أكثر بساطة وواقعية وأقل تعقيد من نموذج OSI. حقق نموذج الإنترنت التوافق بين التطبيقات المختلفة للأجهزة التي تتشارك بشبكة واحدة أو أكثر. كما أنه أتاح القدرة على التواصل والحصول على المعلومات بسرعة أكثر من نموذج OSI [7]. يقتصر نموذج الإنترنت على أربع طبقات فقط [7]:

✍ طبقة التطبيق: تنوب عن الطبقة السابعة والسادسة والخامسة في نموذج OSI.

✍ طبقة النقل: تنوب عن الطبقة الرابعة في نموذج OSI.

✍ طبقة الإنترنت: تنوب عن الطبقة الثالثة في نموذج OSI.

✍ طبقة الربط: تنوب عن الطبقة الثانية والأولى في نموذج OSI.

من الأجزاء التي تتواجد في الشبكات هي البوابات (Gateways) والتي تعمل في كل الطبقات لوصل شبكات مختلفة بالبروتوكولات. تسمح البوابات بمرور البيانات التي تتدفق عبر الشبكات. تعتبر البوابة نقطة دخول وخروج للشبكة ويطلق عليها أحياناً اسم محول البروتوكولات (Protocol Converter) [2].

على الرغم من أن الشبكات تمكّننا من الاتصال والوصول للبيانات وتبادلها بسهولة، إلا أنها أتاحت الفرص أمام بعض المستخدمين للقيام بسرقة وتسليم وتهديد أمن المؤسسات بسهولة. بعد أن فهمنا طبيعة الشبكات وآلية عملها لابد أن ننقل لموضوع يجب الاهتمام به وهو أمن الشبكات.

2.4.3. أمن الشبكة (Network Security) [5]

كما ذكرنا سابقاً فإن أمن الشبكات هو نوع من أنواع الأمن السيبراني وقد تم تعريفه على أنه أي عملية تم تصميمها لضمان استخدام الشبكة وحماية البيانات من العبث أو تهديد كي تبقى الشبكة والبيانات حصينة ضد أي هجوم له أهداف متنوعة. تسمى عملية الحماية هذه بمنع الهجمات السيبرانية (Cyber Attacks). قد عُرفت الهجمات السيبرانية على أنها هجوم متعمد ومقصود من قبل جهاز أو مجموعة من الأجهزة الحاسوبية ضد جهاز آخر أو مجموعة من الأجهزة التي تتصل بشبكة ما أو قد يكون هجوم ضد الشبكة بحد ذاتها. لهذه الهجمات السيبرانية أنواع نذكر أهمها وأشهرها:

✍ البرامج الخبيثة أو الضارة (Malware) [32]: هي برامج مصممة لإلحاق الضرر بالشبكة أو جهاز الحاسوب أو أنظمة التشغيل بطريقة خفية بالغالب مثل الديدان (Worm) والفايروسات (Viruses) وحصان طروادة (Trojans Horse).

✍ التصيد (Phishing) [42]: هي التظاهر والتكر بجهة أو كيان أو شركة موثوقة بهدف الحصول على معلومات سرية للمستخدم. يتم ذلك غالباً عبر البريد الإلكتروني.

✍ هجمات غير معروفة مسبقاً (Zero-Day Malware) [42]: هي برنامج استغلالي غير معروف مسبقاً ويصعب كشفه عادةً بالوسائل التي تعتمد على المعرفة المسبقة للهجمات. يتم فيها استغلال الثغرات (Vulnerabilities). الثغرة تعرف بأنها نقاط ضعف في نظام الحاسوب أو برامجه [26]. على سبيل المثال هجوم (Zero-Day) هو هجوم مفاجئ يستغل مجموعة من الثغرات ويسبب ضرراً كبيراً.

✍ التهديدات المتقدمة المستمرة (Advanced Persistent Threat, APT) [8]: هي هجوم مستمر ومعقد ومتطور. هدف الهجوم زيادة فترة البقاء ضمن الأنظمة والشبكات عن طريق أساليب تستطيع التهرب من أنظمة الكشف وبالتالي ضمان استمرارية الوصول للمعلومات السرية.

بالطبع الحماية وحفظ الأمن يتمان عن طريق كشف الهجمات آنفة الذكر والتحكم بالوصول والسماح للمستخدمين المخول لهم الوصول إلى موارد الشبكة ومنع الأشخاص المهاجمين من تنفيذ عملياتهم. توجد عدة تقنيات وطرق للقيام باكتشاف هذه الهجمات ولكن سنذكر بعضاً منها [5]:

✍ برامج مكافحة الفيروسات والبرامج الخبيثة: تهتم بكشف البرامج الخبيثة كالفايروسات (Viruses) والديدان (Worm) وغيرها من البرامج.

✍ **جدران الحماية (Firewalls) [8]:** هي جهاز أو برنامج يعمل كحاجز حماية يعمل وفق قواعد محددة لتحديد الزيارات المسموحة وغير المسموحة مثل منع الوصول إلى الروابط الخبيثة، بحيث يوضع هذا الحاجز بين شبكة المستخدم والشبكات الأخرى.

✍ **المعلومات الأمنية وإدارة الأحداث (Security Information and Event Management, SIEM):** تعمل على جمع البيانات وتحليلها مثل بيانات السجلات والأحداث. يتم كشف هجوم الـ APT وبعض أنواع هجوم Zero-Day من خلالها.

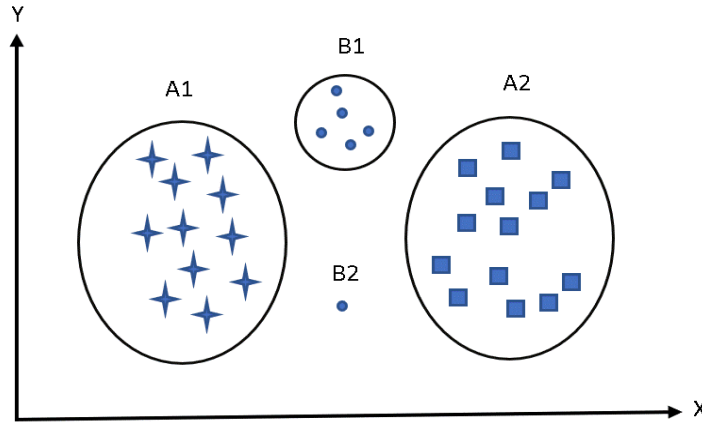
✍ **أنظمة منع التسلل (Intrusion Prevention Systems, IPS) وأنظمة كشف التسلل (Intrusion Detection Systems, IDS) [42]:** هي أنظمة تعمل على فحص حركة المرور وتحليل كمية كبيرة من البيانات. تعمل هذه الأنظمة على كشف تهديد معروف مسبقاً وأحياناً تهديد جديد ومنع هذا النشاط الخبيث من التقدم، من خلال تتبع حركة الملفات المشبوهة والبرامج الخبيثة لمنع انتشارها في الشبكة. نلاحظ أن معظم الطرق والتقنيات المذكورة آنفاً تعتمد بشكل أساسي على قواعد معروفة وأنماط محددة للكشف عن الهجمات فهي تعمل على تحديد هجمات معروفة كما ذكرنا. هذه التهديدات تشكل خطراً كبيراً وهي محور جدير بالاهتمام في مجال أمن الشبكة بشكل خاص والأمن السيبراني بشكل عام. إلا أن التهديدات الجديدة والمعقدة مثل هجمات الـ APT وأنواع كثيرة من هجوم الـ Zero-Day وهجمات أخرى قد تصدر عن مستخدم لا يظهر عليه صورة المخترق. تجدر الإشارة هنا إلا أن الطرق السابقة تفشل في كشف مثل هذه الهجمات. هنا يأتي دور التحليل السلوكي مثل تقنية الـ UBA فهي طرق ذات فاعلية كبيرة في كشف التهديدات غير المعروفة. يتم ذلك عن طريق الكشف عن سلوك الشبكة أو المستخدم الطبيعي وغير الطبيعي والبحث عن أنماط غير معروفة مسبقاً. سنتحدث عن هذه التقنية بشكل مفصل لاحقاً.

تعتبر الهجمات التي عرضناها أعلاه أنشطة خبيثة، فهي تعمل على إحداث تغييرات في عمل الشبكة مثل حركة متزايدة للبيانات أو وصول غير اعتيادي للملفات. يتم تحليل البيانات عادةً وتحديد السلوك الطبيعي والاعتيادي، عندئذٍ تلاحظ تلك الأنشطة الخبيثة لكونها مغايرة لسلوك الشبكة أو المستخدم. بمعنى آخر يُعد أي انحراف عن السلوك المعتاد للمستخدم نوعاً من أنواع الشذوذ الذي يستدعي الانتباه. لفهم ما هو الشذوذ وطرق كشفه عبر التقنيات المختلفة، لابد من عرض شرح مفصل عن هذا الموضوع.

5.3. الشذوذ (Anomaly)

مقدار البيانات التي يتم إنتاجها كل يوم في ازدياد. في عام 2021، أنتج المستخدمون 2.5 كوينتيليون¹ بايت من البيانات يومياً ومن المتوقع أن يصل إنتاج البيانات إلى 200 زيتابايت² بحلول عام 2025 [36]. يوجد حاجة لتحليل مثل هكذا بيانات على الرغم من ضخامتها بهدف إيجاد أنماط فيها وتصنيفها. تحليل هذه البيانات يساهم بتوظيفها في مجالات مختلفة بغرض إجراء دراسات عديدة. إلا أن هذه التحليلات تتأثر بوجود بيانات شاذة قد تشير إلى وجود سلوك غير طبيعي وهذا بدوره قد يدل على وجود اختراق للشبكة.

لا يوجد تعريف محدد وموحد للشذوذ. لذلك قمنا في هذه الرسالة بتعريف الشذوذ على أنه العنصر غير الطبيعي والمغاير عن نمط بقية العناصر. بالتالي البيانات الشاذة هي مجموعة البيانات التي تسلك سلوكاً مختلفاً وغير طبيعي ضمن مجموعة البيانات التي تملك نمطاً محدد وطبيعي. الشكل 3.3. يوضح كيفية توزيع البيانات الشاذة.



الشكل 3.3. توزيع البيانات الشاذة.

تعتبر المجموعتان A_1, A_2 مناطق ذات بيانات طبيعية، بينما المجموعة B_1 والنقطة B_2 تعتبران بيانات شاذة كونها تسلك سلوكاً مغايراً للبيانات الطبيعية. مقياس تحديد السلوك الطبيعي في المثال السابق يعتمد على الشكل. كشف الشذوذ الشبكي يعني العثور على أنماط في البيانات المارة ضمن الشبكة لا تتوافق مع السلوك المتوقع. يُشار إلى هذه البيانات غير المتوافقة على أنها شذوذ أو قيم متطرفة. هذان المصطلحان الأكثر شيوعاً للتعبير عن البيانات هذه في سياق كشف الشذوذ الشبكي [14].

1 الكوينتيليون هو رقم 1 متبوع بـ 18 صفراً

2 الزيتا هو رقم 1 متبوع بـ 21 صفراً

تتضمن عملية تحليل البيانات عادةً تحديد منطقة تمثل السلوك الطبيعي، ومن ثم تُحدّد البيانات الشاذة وفق الانحرافات عن هذه المنطقة. يمكن أن تعتبر مرحلة كشف الشذوذ المرحلة الأساسية التي يجب القيام بها قبل تحليل أي بيانات ومن ثم عزل هذا الشذوذ كونه قد يؤثر على نتائج التحليل ويجعلها غير دقيقة. لكن هذا الأمر بغاية الصعوبة وذلك لكون هذه الأنماط غير الطبيعية هي نتيجة لنشاط خبيث يهدف لجعل هذه الأنماط تبدو طبيعية. بدأت دراسة كشف الشذوذ في وقت مبكر من القرن التاسع عشر، وواصلت تطورها مع الزمن، لتصبح محوراً رئيسياً في البحوث الحديثة في مجال الأمن السيبراني [14].

1.5.3. أنواع الشذوذ (Types of Anomaly)

يوجد أنواع عديدة للشذوذ ولكن يمكن تصنيفه إلى ثلاثة أنواع رئيسية [14]:

✍ **شذوذ النقطة (Point Anomalies):** يحدث عند وجود عنصر واحد يختلف بصفاته عن بقية العناصر مثل الشكل 3.3. النقطة B_2 وكذلك مجموعة النقاط B_1 مثال على شذوذ النقطة. كما يمكن أن نسميها أيضاً بالنقطة الشاذة.

✍ **شذوذ السياق (Contextual Anomalies):** يحدث عندما يكون عنصر ما يقوم بسلوك غير متوافق مع سياق محدد. يُفهم السياق بأنه قاعدة عامة أو معتقد عام ويتم تحديد سمات محددة لهذا السياق. مثلاً على ذلك عند قراءة درجات الحرارة لكل شهر في سوريا فإن درجة الحرارة 35° هي مطابقة بالصفات لمفهوم درجة الحرارة، لكن إذا تم قراءة مثل هكذا درجة في فصل الشتاء عندها يعتبر شذوذ سياق لأن من المعروف أن الشتاء لا يمكن أن تكون درجة حرارة فيه 35° في سوريا. أما لو تم قراءة درجة الحرارة ووجد أنها مثلاً $1ak$ فهذه تعتبر شذوذ نقطة لأنه لا يوجد درجة حرارة $1ak$.

✍ **شذوذ جماعي (Collective Anomalies):** يحدث عندما تشكل مجموعة بيانات نمطاً متشابهاً مع بعضها البعض، ولكنها تختلف عن بقية العناصر. من الملاحظ أنه يمكن ربط الحالات السابقة جميعها. بعبارة أخرى قد يعتبر في بعض حالات شذوذ النقطة كشذوذ جماعي مثلاً.

تحديد مثل هذه الأنواع من الشذوذ يحتاج لطرق محددة قادرة على تمييز السلوك المغاير أو مقارنة هذا السلوك مع سلوك شاذ محدد مسبقاً.

2.5.3. طرائق كشف الشذوذ (Anomaly Detection Methods)

توجد عدة طرائق لتحديد تلك العناصر التي تسلك سلوك مغاير نذكر منها [14]:

✍ **طرائق الكشف الإحصائية (Statistical Detection Methods):** تعتمد هذه الطرائق على تحديد درجة انحراف كل نقطة عن تدفق البيانات الطبيعي. يتم تحديد درجة (Score) لكل نقطة تعتبر درجة شذوذ لها. لكن في دراستنا لن نعتمد على هذه الطرق.

✍ **طرائق تعلم الآلة (Machine Learning Methods):** هذه الطرق ظهرت لمعالجة المشاكل الموجودة في الطرائق الإحصائية. لكون إيجاد السلوك الشاذ أمر أكثر صعوبة عند عدم وجود بيانات مصنفة مسبقاً يمكن المقارنة بها. كان لابد من وجود نوع يكشف الشذوذ دون الاعتماد على تصنيفات مسبقة. ففي مجال تعلم الآلة لدينا كشف الشذوذ بإشراف، وهو يعتمد على كشف شذوذ معروف مسبقاً، وكشف شذوذ بغير إشراف وهو الذي يستطيع كشف الأنواع الجديدة.

✍ **طرائق التعلم العميق (Deep Learning Methods):** ظهرت هذه الطرائق نتيجة لوجود بعض المشاكل التي ظهرت عند استخدام الطرائق السابقة مثلاً فقدان البيانات. هي تعتبر أداة قوية للتعامل مع هذه المشاكل وقد تتفوق على سابقتها من الطرق في الكثير من الأحيان.

6.3. خلاصة الفصل

في هذا الفصل، سلطنا الضوء على مفاهيم الأمن السيبراني وبعضاً من أنواعه. شرحنا مفهوم الشبكة والنموذج المرجعي OSI وكيف يتم حفظ أمن الشبكة. وضحنا مفهوم الشذوذ ركزنا على طرائق اكتشافه سواء عبر الأساليب الإحصائية أو تقنيات تعلم الآلة والتعلم العميق. طرائق كشف الشذوذ تعمل جميعها لكشف الشذوذ الذي بدوره قد يشير لهجوم محتمل على المؤسسات ويهدد أمنها وسلامة بياناتها. هذا الشذوذ يتم من خلال بعض الطرق الخبيثة التي تجري عبر الشبكة. قد كان هذا الأمر محط اهتمام خبراء الأمن لذلك مع تقدم وتوسع الجريمة الإلكترونية. كان لابد من تطوير أساليب حماية تعتمد على أفضل الطرق للكشف عن الشذوذ. تُعتبر تحليلات الأمان والتي من أحد تقنياتها تقنية الـ UBA من الأساليب الحديثة في مجال كشف الشذوذ وهذا ما سوف نستعرضه في الفصل القادم.

الفصل الرابع

تحليلات الأمان

1.4. مقدمة

كما رأينا في الفصول السابقة، الجريمة الإلكترونية في تقدم وتطور دائم. لم تعد الأساليب التقليدية قادرة على تأمين الأنظمة بشكل كافٍ، مما أدى إلى الاعتماد على الذكاء الصناعي وتحليل البيانات كوسيلة للكشف عن التهديدات مبكراً. لجأت المؤسسات حول العالم مع بداية القرن الحادي والعشرين إلى عدد من حلول الأمن السيبراني المعتمدة على أساليب الذكاء الصناعي للحفاظ على أمن بياناتها. الأمر الذي اقتضى السعي للعثور على طرق للكشف المبكر للهجمات عبر الكشف المسبق عن أي شذوذ قد يدل على هجوم مستقبلي وذلك بهدف زيادة كفاءة وسائل الحماية ومواكبتها للتطور وتلبية حاجة المؤسسات لضمان أمنها الدائم.

سنتناول في هذا الفصل مفهوم تحليلات الأمان ضمن الفقرة 2.4. وهي أحد فروع الأمن السيبراني. إلى جانب هذا توضيح لتقنية تحليل سلوك المستخدم في الفقرة 3.4. وهي التقنية الأساسية لدراستنا حيث سنوضح مفهومها، مكوناتها، ركائزها، التهديدات التي تكشفها سلباتها وإيجابياتها.

2.4. مفهوم تحليلات الأمان (Security Analytics Concept) [35]

تحليلات الأمان هي نهج استباقي للأمن السيبراني والذي يعمل على جمع البيانات وتحليلها وذلك من خلال استخدام أدوات التحليل الأمني. تهدف إلى تحسين تحديد الهجمات الاستباقية وتحديد السلوكيات التي تشير إلى نشاط شاذ وتحديد التهديدات المحتملة مثل البرامج الضارة الخارجية وذلك في مراحل مبكرة. إن تحديد للتهديدات في مرحلة متقدمة يعني الاستجابة لإيقاف هذه التهديدات قبل التسلل للبنية التحتية للشبكة وتعريض البيانات للخطر. تعتبر تحليلات الأمان الحل الأمثل لمواجهة الحوادث الأمنية التي تهدد أمن الشبكات والمؤسسات. كون المتسللين أصبحوا في الأونة الأخيرة يجدون طرقاً جديدة لتجاوز الحلول الأمنية السابقة. الحلول الأمنية القديمة مثل أنظمة كشف التسلل وجدران الحماية وغيرها من الحلول التي تكشف التهديد حين حدوثه ومحاولة التصدي بعد فوات الأوان. أما تحليلات الأمان فهي تعمل على إنشاء عمليات بحث سريعة لتحديد مؤشرات مبكرة للهجوم وطرق لا يستطيع المتسللون تحديدها. تجمع تحليلات الأمان بين خوارزميات الـ AI وبين ما يعرف بتحليلات البيانات

الضخمة¹ (Big Data Analytics). تحليلات الأمان من أهم الأساليب التي توظف الـ AI في الأمن السيبراني. يتم ذلك من خلال طرق عديدة لمراقبة الشبكة وحركة المرور وبيانات سلوك المستخدم وهنا يمكن تسميتها بتحليلات الأمان السلوكية. من الأمثلة على تحليلات الأمان هي تقنية الـ UBA ومثال آخر هو تقنية الـ SIEM [37].

3.4. تحليل سلوك المستخدم (User Behavior Analysis)

تعتبر هذه التقنية واحدة من أهم التقنيات وطريقة أكثر شمولاً للتأكد من أن المؤسسة تتمتع بأمن تكنولوجيا المعلومات وخاصةً بعد أن أصبحت الأدوات والأنظمة القديمة بالية [6]. بداية التقنية كانت في عام 2014 في حين تم إضافة كلمة كيان² (Entity) وذلك في عام 2015 من قبل شركة Gartner³ [30].

عُرفت التقنية بأنها أحد تقنيات الأمن السيبراني التي تُستخدم لتحليل الأنشطة المشبوهة للمستخدمين في الشبكة باستخدام خوارزميات الـ AI مثل التعلم الآلي والخوارزميات الأخرى التي تحدد السلوك الذي قد يشير إلى هجوم إلكتروني (Cyber Attack) [33]. في نفس الصدد عُرِفَت على أنها نوع من عمليات الأمن السيبراني التعلم الآلي والتحليلات الإحصائية (Statistical Analytics) وغيرها من الخوارزميات لاكتشاف الهجمات التي تحدث ضمن الشبكة في الوقت الفعلي لحدوثها تقريباً [42].

يرمز اختصاراً للتقنية بالرمز (UBA) أما عندما تم إضافة كلمة الكيان أصبحت التقنية تُعرف اختصاراً بالرمز (UEBA). لكن في دراستنا هذه سوف نركز على دراسة تحليل سلوك المستخدم مع دراسة سلوك الكيان عموماً. لفهم المبدأ الذي تعمل به التقنية سوف نقوم بعرض مجموعة من الأمثلة:

☞ إذا اعتاد موظف ما على تسجيل دخول إلى النظام بانتظام في الساعة 9 صباحاً عندها يكون هذا الوقت هو الوقت الاعتيادي لتسجيل دخوله. فإذا قام هذا الموظف بشكل مفاجئ بتسجيل دخول في الساعة 2 صباحاً فسوف يعتبر هذا الأمر شاذاً كونه سلوكاً يختلف عن روتينه [33].

☞ في حال قيام مستخدم ما بتتزيل 10 ميغابايت من الملفات بانتظام. بشكل مفاجئ قام بتتزيل 15 غيغابايت سيعتبر كذلك هذا النشاط شاذاً [6].

1 تحليل البيانات الضخمة هو جمع العديد من مجموعات البيانات الكبيرة ودمجها وتحليلها والتي لا تستطيع إدارتها برامج المعالجة العادية والتقليدية.

2 الكيان يعني أجهزة التوجيه والخوادم ونقاط النهاية.

3 شركة Gartner وهي شركة ومؤسسة من المؤسسات العالمية الرائدة في مجال الاستثمارات والأبحاث التكنولوجية الأميركية تم تأسيسها عام 1979.

قيام الموظف أو مستخدم ما بتسجيل دخول بشكل دائم من موقع جغرافي محدد ثم فجأة سجل دخول من موقع بعيد جداً عن الموقع المعتاد بفارق زمني قصير سيكون أيضاً هذا دلالة على شذوذ. يمكن سرقة اسم مستخدم وكلمة مرور لشخص ما لكن لا يمكن التصرف تماماً كما يفعل هو عند دخوله للنظام. يمكن الكشف عن السلوك المعادي لكونه يختلف عن السلوك الاعتيادي والطبيعي للمستخدم [34]. يقصد هنا بالسلوك الزمان والمكان المتعلقان بالمستخدم، إلى جانب ذلك المواقع الإلكترونية التي يزورها، حركات النقر ونوع الملفات المحملة وحجمها ... إلخ. بالطبع إن اكتشاف مثل هذه التحركات المفاجئة ليس بالأمر السهل وهذا ما يترتب عليه أن تكون التقنية منظمة وحلولها هادفة، لهذا فإن لتقنية الـ UBA مفاتيح أساسية تعمل وفقها وذلك قبل البدء وهي الركائز ومن ثم يأتي دور مكونات التقنية التي توضح آلية عملها.

1.3.4. الركائز الثلاث لتحليل سلوك المستخدم [33]

توضح هذه الركائز متى يتم استخدام التقنية أي أنها المبادئ الأساسية التي يتم الانطلاق منها في تطبيق حلول الـ UBA وما الأمور التي يتم جمعها والمعلومات اللازمة لهذه التقنية. يمكن القول إننا سنطرح أدوات الـ UBA وذلك قبل البدء بعملية إيجاد الشذوذ وهي:

• حالات الاستخدام (Use Cases): والتي تعتبر الهدف الذي تبحث عنه التقنية فحلول الـ UBA تقوم بمراقبة النشاط العدائي مثل:

- مراقبة الموظفين: في حال كانت الشركة ترغب بإنشاء نظام أمني يراقب الموظفين لديها للكشف عن المستخدم المتسلل فعلى حلول الـ UBA أن توفر نظام لحالة الاستخدام هذه.
- مراقبة المضيفين الموثوقين: قد ترغب شركة ما بنظام يُعنى بالكشف عن موثوقية المضيف وهذه حالة استخدام لا بد لحلول الـ UBA توفيرها.

بالتالي حلول الـ UBA ينبغي أن تكون قابلة للتكيف مع مجموعة متنوعة من حالات الاستخدام على عكس بعض التقنيات التي تقوم بإجراء تحليل مخصص لحالة محددة واحدة [6].

• مصادر البيانات (Data Sources): يجب أن يتم تجميع البيانات من مستودعات البيانات أو من SIEM وهذه البيانات تعتبر من أهم الركائز.

• التحليلات (Analytics): يجب أن تتضمن حلول التقنية الكشف عن الشذوذ باستخدام طرق تحليلية متنوعة ومن هذه الطرق:

- تعلم الآلة (Machine Learning)

• النماذج الإحصائية (Statistical Models)

• التعلم العميق (Deep Learning) وغيرها من الطرق التي وضعناها سابقاً.

إلا أننا في دراستنا سوف نركز على خوارزميات الـ AI المختلفة.

لضمان سير العملية وتحقيق نجاحها، يجب أن تشمل حلول الـ UBA على مجموعة من المكونات والتي يجب مراعاتها وذلك بعد إيجاد حالة الاستخدام وتحديد هدف البحث وتأمين البيانات واختبار طريقة تحليل مناسبة.

2.3.4. مكونات تحليل سلوك المستخدم

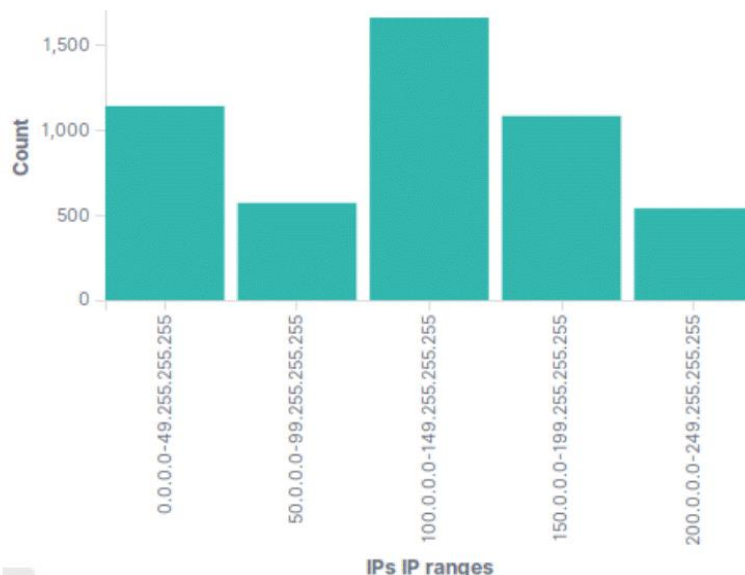
فيما يلي نعرض المكونات الرئيسية لحلول الـ UBA والتي تعتبر الترتيب المنسق لآلية عملها وكيفية سير حلول التقنية وما الشروط الواجب توفرها عند القيام بعملية كشف الشذوذ [33]:

✍ **تحليل البيانات (Data Analytics):** في تحليل البيانات يعين الحد الفاصل والذي يسمى الخط الأساسي (Baseline). يُعين الخط الأساسي من خلال جمع المعلومات عن سلوك المستخدمين الطبيعي وكذلك الكيانات (في حال الحديث عنها) باستخدام الطرق التحليلية المذكورة سابقاً. يتم بعد ذلك إصدار تنبيهات أمنية تلقائياً عند اكتشاف انحراف عن السلوك الطبيعي.

✍ **تكامل البيانات (Data Integration):** هنا نعني بأن تكون حلول وأنظمة الـ UBA قادرة على مقارنة بين البيانات والتي تم جمعها من مصادر مختلفة مع البيانات في النظام الأمني الحالي وفي حال عدم مطابقتها تُعتبر شذوذاً. نقصد بذلك أن اكتشاف الشذوذ لا يتم فقط من خلال مقارنة السلوك مع الخط الأساسي كما ذكرنا في تحليل البيانات. لا نكتفي ببيانات المستخدم ذاته بل أيضاً بمقارنة سلوكه مع أي نشاط معادي معروف مسبقاً لدى الأنظمة الأخرى مثل زيارة موقع ويب مشبوه فلا حاجة لمقارنة مثل هذه الزيارات مع المعلومات الاعتيادية للمستخدم.

✍ **عرض البيانات (Data Presentation):** هي الطريقة التي يتم تقديم البيانات فيها للمعنيين والمختصين وذلك لتسهيل قراءة المحتوى. يتم استخدام طرق مختلفة كجداول أو مخططات وذلك يساعد بتحديد الشذوذ وتمثيل العلاقة بين مجموعتين أو أكثر من مجموعات البيانات بشكل مرئي. أحد أشكال عرض البيانات يوضحها الشكل 1.4. والذي يتضمن عرض لتوزيع نطاقات عناوين الـ IP. حيث تم دمج البيانات المتعلقة بعناوين الـ IP وتخليها في رسم بياني وتوزيعها في نطاقات مختلفة وتم تسجيل عدد تلك العناوين في كل نطاق في الرسم البياني. يمثل الخط الأفقي النطاقات بينما الخط العمودي عدد العناوين فمثلاً نطاق الـ

IP الأكثر استخداماً هو 100.0.0.0 و149.255.255.255، حيث يصل إلى أكثر من 1500، أما أدنى نطاق فهو 200.0.0.0 و255.255.255.255.



الشكل 1.4. توزيع نطاقات عناوين الـ IP.

استناداً إلى ما سبق إن الآلية التي تعمل بها التقنية هي التعامل مع سجلات المستخدم وتحليل السلوك من خلال تلك السجلات لكل مستخدم على حدة. الهدف من التحليلات هو إيجاد أنماط معينة تعين كحد فاصل وتلك الأنماط هي السلوك الاعتيادي. بعد تحديد الحد الفاصل يتم مقارنة السلوك الجديد بهذا الحد الذي يعتبر النقطة المرجعية، بالتالي انحرافه عن هذه النقطة يجعله مصنف كسلوك شاذ. هذا ما يجعل التقنية تتمتع بقدرة كبيرة على تحديد الهجمات غير المحددة مسبقاً بخلاف الكثير من الأساليب الأخرى. من جهة أخرى تركز التقنية عند تحليل سلوك المستخدم أو حتى الكيان على جزء محدد من النظام أو حتى الشبكة. بينما نظام الـ IDS يقوم برصد الشبكة بأكملها بالتالي قدرته على كشف بعض الأنماط منخفضة حتى وإن كان يستطيع كشف الهجمات غير المحددة مسبقاً. عموماً الـ IDS يعتمد على قواعد محددة سابقاً بالتالي الكشف عن الهجمات اعتماداً على أنماط للهجمات المحددة والمعروفة ومن ثم مقارنة أي نمط أو نشاط بها لتحديد كونه شذوذاً أم لا. مما يعني أن هناك أنشطة قد تمر دون كشف عبر الـ IDS، بينما تكشفها تقنية الـ UBA. يمكن القول إن كلاً من الأسلوبين يمكن أن يكمل بعضهما البعض وبالتالي يمكن استخدامهما معاً لتحسين الأمن السيبراني.

بالطبع تطبيق الكشف عن الشذوذ بالأساليب الحديثة مثل التعلم الآلي ليس بالأمر حديث العهد، حيث يوجد دراسة في مجال كشف الشذوذ تعود لعام 1987 تحت عنوان (“An Intrusion Detection Model”)

وكذلك دراسة أخرى في عام 2009 بعنوان ("Anomaly Detection: A Survey") وهو عمل قد يعتبر حديث نوعاً ما [34]. هنالك الكثير من الدراسات في هذا الشأن إلا أن الاستجابة للحوادث وكشف الخروقات والتسلّلات واجهت العديد من التحديات مما جعل هذه الأساليب وتلك الدراسات عاجزة. أحد أكبر التحديات التي واجهتها الاستجابة للحوادث هو كمية البيانات الضخمة وكيفية استيعابها وتحليلها. تعتبر تفسير الحالات الشاذة أو الأنشطة الشاذة الناتجة عن السلوكيات الشاذة في الاستخدام أمراً بالغ الأهمية، فكانت في هذا الصدد تحليلات الأمان التي تعد مجالاً جديداً في مجال الأمن وتقنية الـ UBA تحديداً واحدة من أحدث الطرق التي تركز على تصرفات المستخدمين. أصبحت هذه التقنية الأكثر استخداماً مؤخراً لأنها تعمل على الكشف عن التسلّلات في الوقت الحالي في حين الأساليب الأخرى مثل جدران الحماية ليست مضمونة في هذه الحالة بنسبة 100% [34].

ولكن يبقى التساؤل المطروح ما الذي قد يميز هذه التقنية عن غيرها من التقنيات؟ أو ما هي حاجة الشركات والمؤسسات لمثل هذه الحلول في ظل وجود العديد من الأساليب الوقائية؟ نلاحظ من خلال القراءة الأولية أن تقنية الـ UBA تركز بشكل أساسي على أي سلوك مريب ينبئ عن وجود أمر يثير الشك لوجود تسلل مستقبلي قد بدأ فاعلوه بالبحث عن بيانات يمكن استخدامها لشن هجوم محتمل ضد عملاء شركة ما. عادةً يُقدم تحذير مسبق عن نوع من السلوكيات التي لا يتم اكتشافها بواسطة الحلول الأخرى بالتالي الإبلاغ عن هكذا نشاط في الوقت الفعلي أو شبه حقيقي ومنه التسريع من عملية الاستجابة للمخاطر. من جهة أخرى حلول الـ UBA قادرة على الكشف عن حالات غير معروفة مسبقاً فهي لا تقارن بنشاط خبيث معروف بالضرورة. بالطبع لا تغني تقنيتنا عن الأساليب الوقائية الأخرى ومن الضروري التأكيد على حاجة المؤسسات للدمج بين التقنيات المختلفة لتعزيز أمنها وأمن بياناتها وذلك لأن حلول الـ UBA تكشف السلوك المشبوه ولكن لا تستطيع إيقاف المتسللين.

وهنا لابد من بيان وظيفة التقنية وقدراتها وتحديد ما تستطيع كشفه وذلك من خلال التطرق إلى التهديدات التي تستطيع كشفها بحيث سنقوم بذكر بعضها.

3.3.4. التهديدات التي تحددها التقنية

تُمكن تقنية الـ UBA من اكتشاف هذه التهديدات التي تكون من الخارج مثل مهاجم خارج النظام أو المؤسسة أو تهديدات من الداخل مثل أحد موظفي الشركة وهذه التقنية قادرة على تحديد الكثير من التهديدات سواء كانت داخلية أو خارجية مثل [33]، [34]:

✍ **كشف التهديدات الداخلية (Detect Insider Threat):** الهجمات الداخلية هي تلك التي ينفذها مستخدم (موظف) يخطط للقيام بهجوم إلكتروني لضرب المؤسسة وأمنها. كونه من الصعب كشف مثل هكذا تهديد يدوياً أو عبر القيام بعمليات تفتيش فقد تم التوجه لحلول الـ UBA نظراً لأنها تعرف الأنشطة الاعتيادية للمستخدمين جميعهم فتكشف بسهولة النشاط غير المعتاد للمستخدم ويتم وضع علامة تلقائياً عند هذا النشاط واعتباره شذوذاً قد يدل على المستخدم الذي سوف ينفذ الهجوم المعادي.

✍ **كشف الحسابات المخترقة (Detect Compromised Accounts):** الحساب المخترق هو الذي يتم الوصول إليه من قبل مستخدمين غير مخول لهم الوصول مثل القرصنة (تهديد خارجي). يتم ذلك من خلال قيام المستخدم الفعلي للحساب بتثبيت برامج ضارة وذلك دون علمه أو قيام المهاجم بانتحال صفة وخداع المستخدم وطلب منه الحصول على بيانات الاعتماد الشخصية.

✍ **كشف خرق البيانات المحمية (Detect Breach of Protected Data):** وجود بيانات سرية يعني وجود الحاجة لحمايتها تقوم حلول الـ UBA بمراقبة محاولات الوصول إلى البيانات في الوقت الفعلي. تحديد فيما إذا كان هنالك مستخدم غير مخول له الوصول لهذه المعلومات يحاول الحصول عليها.

تعتبر التهديدات السابقة واحدة من أهم ما يمكن أن تحدده حلول الـ UBA فبالطبع يوجد المزيد من الهجمات التي يمكن كشفها عبر التقنية. بالرغم من أن هذه التقنية قد تحدد مجموعة متنوعة من التهديدات، فإن فهم الجوانب الإيجابية والسلبية المرتبطة بها يمكن أن تساعدنا على تقييم مدى فعاليتها بشكل أفضل.

4.3.4. سلبيات وإيجابيات التقنية [42]

ضمن الميزات التي تتمتع بها حلول الـ UBA المعتمدة على تحليلات السلوك بأنها تقوم بالحفاظ على قاعدة بيانات كائنات النظام، وتخزن سلوك النظام سواء كان طبيعياً أم غير طبيعي وهو ما يعرف بكشف الشذوذ. يقصد بكائنات النظام المستخدمين، الأجهزة والشبكات. الاحتفاظ بمثل هكذا قاعدة يجعل قدرة التقنية على تحليل ومراقبة السلوك الطبيعي وغير الطبيعي أفضل كونه يمكن ملاحظة أي تغيير في هذا السلوك.

يقدم ليوبولد (Leopold) حجة قوية بأن الـ UBA تتقدم لتصبح تقنية أمن المعلومات الأساسية وخاصةً لمديري تكنولوجيا المعلومات الذين يواجهون تحديات كبيرة. بحسب شركة Gartner في قائمتها لأبرز تقنيات الأمن أن الـ UBA قد اكتسبت سمعة كونها أحد أكثر التقنيات تأثيراً، فهي تقدم تحليلات شاملة ليست فقط حول سلوك

المستخدم بل حول الكيانات الأخرى مثل نقاط النهاية، الشبكات والتطبيقات وهذا ما يضمن الحصول على نتائج أكثر دقة وكشف أكثر فعالية للتهديدات.

من جوانب القوة كونها تعتبر أكثر فعالية بما يخص اكتشاف السلوك الخبيث للمستخدم من الـ SIEM. علاوة على ذلك تعتبر ذات كفاءة عالية في التعرف على التهديدات الداخلية وإصدار التنبيهات حولها. يجدر الإشارة إلى أن حلول الـ UBA لا تقوم بتجميع البيانات بل تعتمد على بيانات تم تجميعها مسبقاً عن طريق أدوات الأمان الأخرى [10]. هذا ما يجعل تطبيقها سريع الفعالية فلا يكون هنالك إضاعة للوقت لتجميع البيانات.

بينما تتمتع التقنية بجوانب مميزة مثل الكفاءة العالية فهي تمتلك بعض نقاط الضعف ومنها أن التقنية تعتمد على طرق مختلفة لتحليل السلوك الطبيعي للمستخدمين واكتشاف السلوك غير العادي ومن هذه الطرق التعلم الآلي وهذا ما يجعل التقنية عاجزة بعض الشيء. لأن التعلم الآلي عموماً لديه عجز في التعامل مع المستخدمين المميزين أو المسؤولين والخبراء الذين لديهم معرفة وفهم في مجال الأمن والـ AI وهؤلاء المستخدمين يصنفون كحالة فريدة لأن مهامهم تتطلب غالباً القيام بسلوكيات غير منتظمة مما يجعل من الصعب إنشاء الخط الأساسي. يمكن هذا أن يؤدي لنتائج غير دقيقة مما يقلل من فاعلية حلول الـ UBA.

عيب آخر للتقنية هو ان الهجمات التي تتم ببطء لا تستطيع الـ UBA كشفها مما يعني أنه يمكن التسلل إلى النظام دون اكتشاف باعتماد مثل هكذا استراتيجيات والتي تجعل التهديدات تصبح وكأنها غير موجودة.

4.4. خلاصة الفصل

استعرضنا في هذا الفصل مفهوم تحليلات الأمان. شرحنا مبدأ عمل تقنية الـ UBA وذكرنا ركائزها والتهديدات التي تحددها. ناقشنا الجوانب الإيجابية والسلبية لاستخدام تقنية الـ UBA وعرفنا أنها واحدة من هذه التقنيات التي تقدم نهجاً فعالاً للكشف عن الأنشطة الضارة والحفاظ على الأمان. لكن لا بد من الإشارة إلى كيفية تطبيق هذه التقنية في الواقع باستخدام الخوارزميات المختلفة وهذا ما سوف نستعرضه في الفصل الآتي. خلاصة القول إن مع زيادة التهديدات الأمنية أصبحت تقنيات تحليل الأمان أكثر أهمية من أي وقت سابق.

الفصل الخامس

الخوارزميات المستخدمة في تقنية الـ UBA

1.5. مقدمة

الخوارزميات هي المحرك الذي يجعل الـ AI قادراً على اكتشاف الأنماط غير الطبيعية. في هذا الفصل سنسلط الضوء على بعض الخوارزميات المستخدمة في الـ UBA لكشف الشذوذ الشبكي. سنتناول في الفقرة 2.5 شرحاً لخوارزمية الـ SVM ثم نستعرض بعضاً من الدراسات السابقة لهذه الخوارزمية في تقنية الـ UBA. في الفقرة 3.5 سوف نتحدث عن مفهوم الشبكات العصبية عموماً ثم عن الشبكة العصبية المتكررة خصوصاً وبعض الدراسات التي استخدمت هذه الشبكة في تقنية الـ UBA.

2.5. آلة شعاع الدعم SVM

1.2.5. مفهوم خوارزمية الـ SVM [25]

تُعد خوارزمية الـ SVM واحدة من أكثر تقنيات التعلم الآلي استخداماً في تصنيف البيانات وانحدارها. تتميز الخوارزمية بقدرتها على إيجاد الحد الفاصل الأمثل بين الفئات المختلفة من البيانات. تعتمد الـ SVM على مفهوم إيجاد حد فاصل بين الفئات لفصلها خطياً يسمى الفاصل بالمستوي الفائق (Hyperplane). يتم اختيار هذا الحد الفاصل بحيث تكون المسافة بينه وبين أقرب نقاط البيانات في كل فئة أكبر ما يمكن.

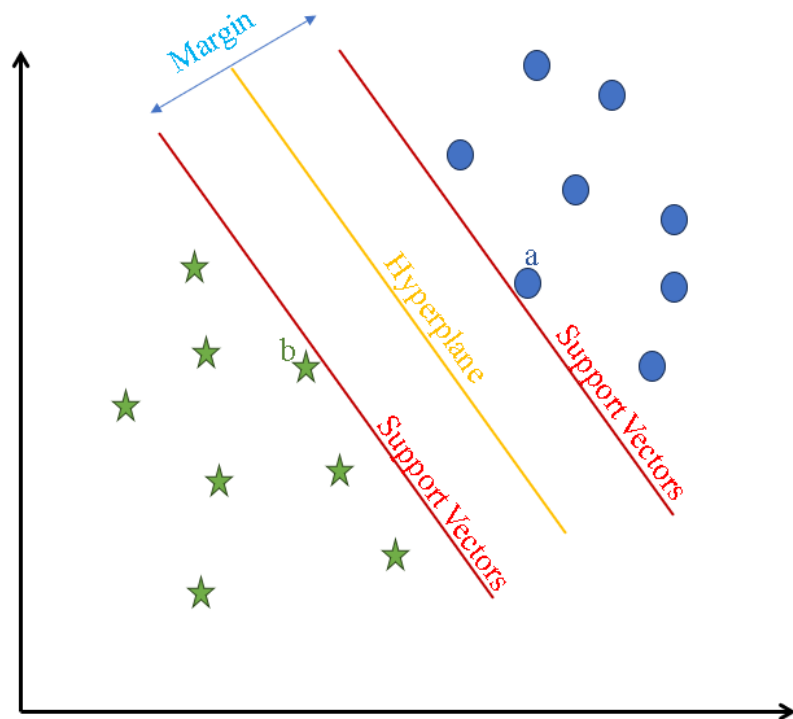
يُعرف الحد الفاصل بأنه المستوى الذي يفصل بين الفئات المختلفة ويتم تمثيله بالمعادلة الآتية:

$$y = W^T X + p = 0 \quad \dots (1.5)$$

حيث W^T هو متجه الأوزان و X هو متجه البيانات المدخلة المتمثلة على شكل نقاط و p هو معامل الإزاحة.

تسعى الـ SVM إلى إيجاد الحد الفاصل الذي يُعظم المسافة بين أقرب نقاط من الفئات المختلفة الذي نسميه الهامش الأقصى (Max Margin). يتم البحث عن أفضل قيمة لكلاً من W^T و p اعتماداً على نقاط مميزة تسمى نقاط الدعم التي نرسم عندها شعاع الدعم (Support Vector).

الشكل 1.5. يوضح طريقة فصل البيانات باستخدام خوارزمية الـ SVM.



الشكل 1.5. تصنيف البيانات باستخدام خوارزمية الـ svm.

في الشكل السابق كل من النقطتين a و b هما نقاط الدعم ومعادلة شعاع الدعم المرسوم عند النقطة a هو:

$$y = W^T X + p = 1 \quad \dots \quad (2.5)$$

أما ومعادلة شعاع الدعم المرسوم عند النقطة b هو:

$$y = W^T X + p = -1 \quad \dots \quad (3.5)$$

عندما لا تكون البيانات قابلة للفصل خطياً تستخدم خوارزمية الـ SVM تحويل النوى لتعيين البيانات إلى

فضاء بعدي أعلى. يتم التحويل باستخدام دالة النواة (Kernel Function)

أشهر أنواع دوال النوى المستخدمة في خوارزمية الـ SVM كما يلي [23]:

النواة الخطية (Linear Kernel) تعطى بالعلاقة:

$$k(x_i, x_j) = x_i \cdot x_j \quad \dots \quad (4.5)$$

النواة متعددة الحدود (Polynomial Kernel) تعطى بالعلاقة:

$$k(x_i, x_j) = (x_i \cdot x_j + c)^d \quad \dots \quad (5.5)$$

نواة الأساس الشعاعي (Radial Basis Function Kernel, RBF) تعطى بالعلاقة:

$$k(x_i, x_j) = e^{\frac{-\|x_i - x_j\|^2}{2\sigma^2}} \dots (6.5)$$

تُستخدم الـ SVM في مجموعة واسعة من تطبيقات التصنيف. يُدرب النموذج على بيانات مُصنفة لتحديد الحد الفاصل الأمثل. بعد التدريب يُستخدم النموذج لتصنيف بيانات جديدة بناءً على موقعها النسبي بالنسبة للحد الفاصل.

2.2.5. تحليل سلوك المستخدم بواسطة الـ SVM

تقدم الدراسة [24] طريقة لاكتشاف الأشخاص غير المصرح لهم باستخدام جهاز الحاسوب والهاتف المحمول. النموذج المطور قائم على نظام CyberSleep المكون من عدة وحدات رئيسية. مبدأ عمل النموذج هو تحليل ضغطات المفاتيح (Keystroke) في الحاسوب والنقرات (Taps) في الهاتف المحمول. تتضمن الوحدات الرئيسية للنظام: وحدة واجهة المستخدم الرسومية، وحدة جمع البيانات، وحدة التعلم الآلي ووحدة تنبيه النظام.

البيانات المستخدمة في نظام Windows تم جمع بيانات 5 مستخدمين. طُلب من المستخدم كتابة كلمة المرور "E3n.5Zx" 600 مرة وتسجيل 28 ميزة لكل محاولة. أما في نظام Android طُلب من 5 مستخدمين إدخال كلمة المرور "918720" 600 مرة.

الميزات الأساسية المستخرجة من ضغطات المفاتيح والنقرات هي: زمن الضغط (Hold Time)، الزمن بين ضغطتين متتاليتين (Down-Down Time) والزمن بين تحرير وضغط المفتاح التالي (Up-Down Time). في بيانات نظام Windows سُجل سرعة الضغط والفترات الزمنية بين كل ضغطة وأخرى. أما في نظام Android تم إضافة طريقة لمس الشاشة وحجم التلامس بين الإصبع والشاشة كميزات إضافية.

باستخدام خوارزمية الـ SVM احادي التصنيف One-Class SVM مع نواة RBF حُدد المستوى الفائق لتمييز السلوك الطبيعي. طريقة كشف السلوك الشاذ عند استقبال بيانات جديدة بتحديد في حال كانت تنتمي للسلوك الطبيعي أم لا. تم تدريب النموذج على بيانات المستخدمين الأصليين لتعلم نمط كتابتهم. نمط المستخدم عند إدخال كلمة المرور مثل سرعة الكتابة، الفترات بين الضغوط وطريقة لمس الشاشة في الهاتف. عندما يحاول شخص آخر استخدام الجهاز فإن طريقة كتابته ستكون مختلفة بمعنى غير مطابقة لنمط المستخدم الأصلي. المحاولة غير المطابقة للنمط الطبيعي تُعتبر محاولة دخول غير شرعية ويتم إرسال تنبيه للتحقق من الهوية.

تقييم الأداء والنتائج الخاصة بالنموذج بناءً تجربة عدة قيم بدالة النواة:

في نظام Windows: أفضل دقة عامة كانت 90% وأدنى دقة عامة كانت 71%. مقارنةً بأداء طرق أخرى مثل RF بأداء 89.2% يعتبر النموذج أفضل في التصنيف.

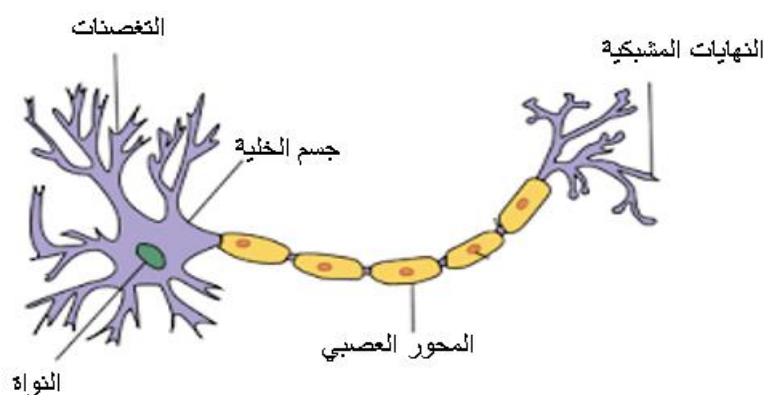
في نظام Android: أفضل دقة عامة كانت 99% وأدنى دقة عامة كانت 69%. مقارنةً بأداء طرق أخرى مثل أشجار القرار بأداء 96.8% يعتبر النموذج أفضل في التصنيف.

3.5. الشبكة العصبية المتكررة RNN

1.3.5. الشبكات العصبية

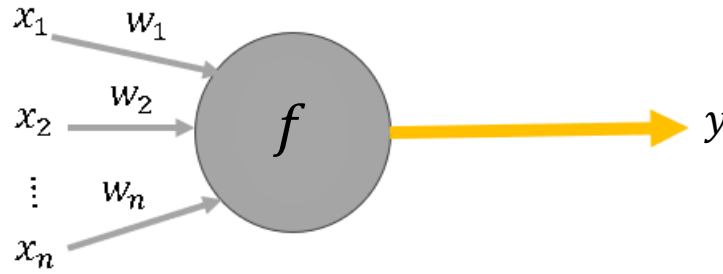
تعد الشبكات العصبية من أكثر خوارزميات الـ AI تقدماً. تُستلهم بنيتها من طريقة عمل الدماغ البشري وذلك في معالجة البيانات واتخاذ القرارات. بين مختلف أنواع الشبكات العصبية تبرز الـ RNN كخيار مثالي للتعامل مع البيانات الزمنية والمتسلسلة مثل سلوك المستخدم. في الفقرات القادمة سوف نشرح هيكل وآلية عمل الشبكات العصبية ثم سنستعرض كيفية عمل الـ RNN. بعد شرح الأساسيات النظرية سننتقل لبعض الدراسات والتطبيقات في مجال كشف الشذوذ الشبكي بحسب تقنية الـ UBA.

الشبكات العصبية الصناعية أو اختصاراً ANN هي جوهر التعلم العميق كما سبق أن شرحنا في الفصل الثاني. قد أوضحنا أن الشبكة العصبية تتألف من طبقات وكل طبقة تتكون من عقد عصبية. تسمى العقدة العصبية بالخلية العصبية الصناعية (Artificial Nerve Cell) وهي التي تشابه في الهيكل وآلية العمل بالخلية العصبية البيولوجية (Biological Nerve Cell). بالتالي مجموعة الخلايا العصبية المرتبطة تشكل الشبكة العصبية. تتألف الخلية العصبية البيولوجية من [18]: جسم الخلية (Cell Body) والذي يحتوي على النواة (Nucleus) والعديد من الامتدادات الفرعية والتي تسمى تغصينات (Dendrites). بعد الجسم يوجد امتداد طويل جداً يسمى المحور العصبي (Axon) في نهايته تفرعات تسمى النهايات المشبكية (Synaptic Terminal). يوضح الشكل 2.5. بنية الخلية العصبية البيولوجية والأقسام التي تم ذكرها قبل قليل.



الشكل 2.5. بنية الخلية العصبية البيولوجية.

تتلقى الخلية العصبية البيولوجية نبضات كهربائية عبر التغصنات ثم تقوم بإطلاق إشارتها الخاصة عبر النهايات المشبكية. بشكل مشابه الخلية العصبية تتلقى مجموعة من المدخلات $x_1, x_2, \dots, x_n$ ثم تقوم ومعالجتها من خلال تابع f والذي يسمى تابع التفعيل (Activation Function) وتعطي الناتج الخاصة بها y . يوضح الشكل 3.5. بنية الخلية العصبية الصناعية.



الشكل 3.5. بنية الخلية العصبية الصناعية.

أما عن توابع التفعيل فهي توابع قابلة للاشتقاق ومن هذه التوابع أربع توابع لا خطية وهي [18]:

$$\text{Sigmoid Function: } \sigma(x) = \frac{1}{1 + e^{-x}} \quad ; \sigma(x) \in [0,1] \quad \dots \quad (7.5)$$

$$\text{Tanh}(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \quad ; \text{Tanh}(x) \in [0,1] \quad \dots \quad (8.5)$$

$$\text{Relu}(x) = \max(0, x) = \begin{cases} 0 & ; x \leq 0 \\ x & ; x > 0 \end{cases} \quad \dots \quad (9.5)$$

$$\text{Softmax}(x) = \frac{e^x}{\sum_{j=1}^k e^{x_j}} \quad ; k \text{ هو عدد العينات } , \text{Softmax}(x) \in [0,1] \quad \dots \quad (10.5)$$

يحسب الناتج الخلية بالعلاقة $y = f(z)$ حيث f هو أحد توابع التفعيل السابقة، أما عن z فهو يحسب بالعلاقة الآتية $z = w_1x_1 + w_2x_2 + \dots + w_nx_n + b$ حيث $x_1, x_2, \dots, x_n$ قد تكون من طبقة المدخلات أو تكون مساوية لمخرجات خلية سابقة كما سوف نرى بالفقرات الآتية عند حساب ناتج خلية في طبقة خفية تلي طبقة خفية أخرى. أما $w_1, w_2, \dots, w_n$ هي الأوزان (Weights) التي تربط بين الخلايا العصبية وتفرض بقيم عشوائية بدايةً ثم يتم تحديثها وتعديلها لتصبح بأفضل قيم ممكنة. أما b فهو ما يسمى بالانحياز (Bias). بما أن الشبكة هي مجموعة من الخلايا العصبية فبعد سلسلة من العمليات التي تقوم بها كل خلية نصل لطبقة المخرجات الأخيرة وعندها يتم إعطاء الناتج النهائي O ويحسب من العلاقة $O = f(z)$.

سوف نقوم بكتابة الرموز السابقة بشكل يناسب الشبكة العصبية كما يلي [41]:

سنرمز للمدخلات بـ x_i^t حيث $i = 1, \dots, n$ أما n هو عدد الميزات (Features) أو الأعمدة التي سوف نتعامل بها في حال كانت البيانات على شكل جداول وسجلات. لدينا $x_0 = 1$ وهي التي تكون عادةً مضروبة بالانحياز. أما t يمثل رقم السجل المُدخل حيث $t = 1, \dots, m$ حيث m هو عدد السجلات. بالتالي يصبح لدينا مصفوفة المدخلات بالشكل:

$$X^t = \begin{bmatrix} x_1^t \\ \vdots \\ x_n^t \end{bmatrix}_{n \times 1}$$

سنرمز بـ w_{gj}^L للأوزان التي تربط بين الطبقات حيث L هو رقم الطبقة التي نقف عندها أو الحالية والتي تبدأ من رقم 1 وهو رقم طبقة المدخلات وتنتهي عند رقم الطبقة الأخيرة وهي طبقة المخرجات. أما رقم الخلية التي نقف عندها (الحالية) هو g ويأخذ القيم $g = 1, \dots, p$ حيث p هو عدد خلايا الطبقة الحالية L . أما رقم الخلية التي سوف نتحرك باتجاهها عندها (التالية) هو j ويأخذ القيم $j = 1, \dots, p'$ حيث p' هو عدد خلايا الطبقة التالية $L + 1$. بالتالي يصبح لدينا مصفوفة الأوزان بالشكل:

$$W^L = \begin{bmatrix} w_{11}^L & w_{21}^L & \dots & w_{p1}^L \\ w_{12}^L & w_{22}^L & \dots & w_{p2}^L \\ \vdots & \ddots & & \vdots \\ w_{1p'}^L & w_{2p'}^L & \dots & w_{pp'}^L \end{bmatrix}_{p' \times p}$$

نلاحظ أن الأدلة لدينا لا تتوافق مع مبدأ كتابة المصفوفات عادةً القائم على رقم السطر ثم العمود.

نسمي خرج الخلية التي في الطبقة الخفية بـ h_k^L حيث L هو رقم الطبقة ورقم أول طبقة خفية هو 2. أما رقم الخلية الخفية التي نقف عندها (الحالية) هو k ويأخذ القيم $k = 1, \dots, q$ حيث q هو عدد خلايا الطبقة الخفية الحالية وهنا لحساب الخرج في الخلايا الخفية سوف نناقش حالتين:

- عند حساب خرج الخلايا في الطبقة الخفية الأولى أي عندما $L = 2$ يكون القانون:

$$h_k^2 = f \left(\sum_{r=1}^s w_{rk}^1 x_r^t + b_k^1 x_0^t \right) \dots (11.5)$$

حيث $x_0^t = 1$ و x_r^t هي المدخلات من طبقة المدخلات. أما $k = 1, \dots, q$ حيث q هو عدد خلايا الطبقة الخفية التي نسحب عندها وهي الطبقة الخفية الأولى. s هو عدد خلايا الطبقة السابقة (طبقة المدخلات) التي نقف عندها عندما $L = 1$. أما w_{rk}^1 هي الأوزان الطبقة الأولى والتي تربط بين الطبقة التي نقف عندها وهي الطبقة المدخلات $L = 1$ والخلية ذات الرقم k في

الطبقة الخفية الأولى $L = 2$ التي سوف نقوم بالحساب عندها ونتجه باتجاهها. أما b_k^1 هي الانحيازات الطبقة الأولى $L = 1$. يمكن أن نكتب قانون مصفوفة الطبقة الخفية الأولى بالشكل:

$$H^2 = f(W^1 X^t + B^1) = f(Z^2) \dots (12.5)$$

حيث

$$H^2 = \begin{bmatrix} h_1^2 \\ \vdots \\ h_q^2 \end{bmatrix}_{q \times 1} \quad \text{و} \quad X^t = \begin{bmatrix} x_1^t \\ \vdots \\ x_n^t \end{bmatrix}_{n \times 1} \quad \text{و} \quad B^1 = \begin{bmatrix} b_1^1 \\ \vdots \\ b_q^1 \end{bmatrix}_{q \times 1}$$

حيث كلاً من $h_1^2, h_2^2, \dots, h_q^2$ يتم حسابها من القانون (1).

• أما عند الطبقات الخفية الباقية أي عندما $L = 3$ فما فوق يكون القانون:

$$h_k^L = f \left(\sum_{r=1}^S w_{rk}^{L-1} h_r^{L-1} + b_k^{L-1} h_0^{L-1} \right) \dots (13.5)$$

حيث $h_0^{L-1} = 1$ و h_r^{L-1} هي النواتج الخلايا في الطبقة الخفية السابقة. أما $k = 1, \dots, q$ حيث q هو عدد خلايا الطبقة الخفية التي نحسب عندها و S هو عدد خلايا الطبقة الخفية السابقة. أما w_{rk}^{L-1} هي الأوزان التي تربط بين الطبقة التي نقف عندها والتي تعتبر السابقة بالنسبة للطبقة الخفية التي نحسبها وبين الخلية ذات الرقم k في الطبقة الخفية التي سوف نقوم بالحساب عندها ونتجه باتجاهها. أما b_k^{L-1} هي الانحيازات الطبقة السابقة. يمكن أن نكتب قانون مصفوفة الطبقة الخفية بدءاً من الطبقة الخفية الثانية بالشكل:

$$H^L = f(W^{L-1} H^{L-1} + B^{L-1}) = f(Z^L) \dots (14.5)$$

حيث

$$H^L = \begin{bmatrix} h_1^L \\ \vdots \\ h_q^L \end{bmatrix}_{q \times 1} \quad \text{و} \quad B^{L-1} = \begin{bmatrix} b_1^{L-1} \\ \vdots \\ b_q^{L-1} \end{bmatrix}_{q \times 1}$$

نرمز بـ $o_{k'}^{L,t}$ للناتج النهائي الذي سوف تتوقعه الشبكة حيث $k' = 1, \dots, q'$ أما q' هو عدد المخرجات المتوقعة أي عدد خلايا طبقة المخرجات و L هو رقم طبقة المخرجات ويعطى قانون الناتج النهائي بالشكل:

$$o_{k'}^{L,t} = f \left(\sum_{r=1}^S w_{rk'}^{L-1} h_r^{L-1} + b_{k'}^{L-1} h_0^{L-1} \right) \dots (15.5)$$

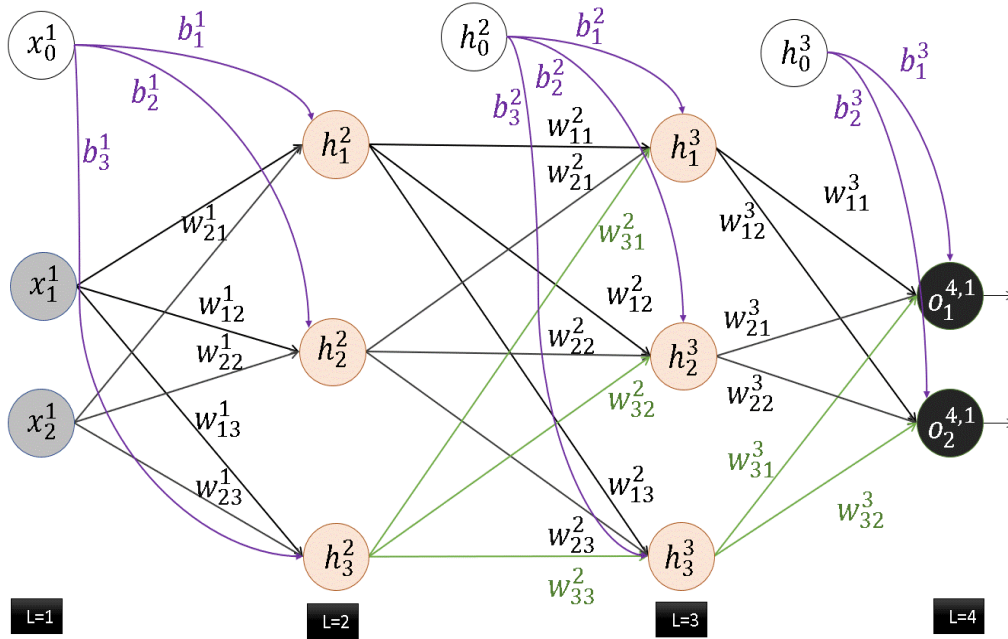
حيث $h_0^{L-1} = 1$ و h_r^{L-1} هي النواتج الخلايا في الطبقة الخفية الأخيرة. أما $k' = 1, \dots, q'$ حيث q' هو عدد خلايا الطبقة التي نحسبها وهي طبقة المخرجات و S هو عدد خلايا الطبقة الخفية السابقة وهي الطبقة الخفية الأخيرة. أما $w_{rk'}^{L-1}$ هي الأوزان التي تربط بين الطبقة التي نقف عندها وهي آخر طبقة خفية والخلية ذات الرقم k' في الطبقة المخرجات التي سوف نقوم بالحساب عندها ونتجه باتجاهها. أما $b_{k'}^{L-1}$ هي الانحيازات الطبقة السابقة (آخر طبقة خفية). يعطى قانون مصفوفة طبقة المخرجات بالشكل:

$$O^{L,t} = f(W^{L-1}H^{L-1} + B^{L-1}) = f(Z^{L,t}) \quad \dots (16.5)$$

حيث

$$O^{L,t} = \begin{bmatrix} o_1^{L,t} \\ \vdots \\ o_{q'}^{L,t} \end{bmatrix}_{q' \times 1} \quad \text{و} \quad B^{L-1} = \begin{bmatrix} b_1^{L-1} \\ \vdots \\ b_{q'}^{L-1} \end{bmatrix}_{q' \times 1}$$

بأخذ مثال بسيط وذلك بالتطبيق على الشكل 4.5. مثال عن شبكة عصبية صناعية.



4.5. مثال عن شبكة عصبية صناعية.

بأخذ بيانات على شكل جدول يحوي على عدد من السجلات وأربع أعمدة عمودين للمدخلات بالتالي $n = 2$ وعمودين للمخرجات بالتالي $q' = 2$. لنأخذ السجل الأول وبالتالي يكون $t = 1$ وعليه يكون $i = 1, 2$ و $k' = 1, 2$. لتكن الشبكة العصبية التي تتكون من أربع طبقات بحيث طبقة المدخلات $L = 1$ وتحوي خليتين.

طبقتين خفيتين الأولى $L = 2$ أما الثانية $L = 3$ وتمتلك كل واحدة ثلاث خلايا. أما طبقة المخرجات $L = 4$ وتحتوي على خليتين. لنكتب المصفوفات الموافقة لهذه الشبكة:

$$X^1 = \begin{bmatrix} x_1^1 \\ x_2^1 \end{bmatrix}_{2 \times 1} \quad \text{مصفوفة المدخلات } L = 1$$

حيث $t = 1$ و $i = 1, 2$ وكذلك $n = 2$.

مصفوفة الأوزان $L = 1$ (التي تربط بين الطبقة التي نقف عندها وهي طبقة المدخلات والطبقة التي نتجه إليها وهي للطبقة الثانية التي سوف نحسبها وهي الطبقة الخفية الأولى بالتالي بين $L = 1$ و $L = 2$).

$$W^1 = \begin{bmatrix} w_{11}^1 & w_{21}^1 \\ w_{12}^1 & w_{22}^1 \\ w_{13}^1 & w_{23}^1 \end{bmatrix}_{3 \times 2}$$

حيث أن $g = 1, 2$ و $p = 2$ و $j = 1, 2, 3$ و $p' = 3$.

$$B^1 = \begin{bmatrix} b_1^1 \\ b_2^1 \\ b_3^1 \end{bmatrix}_{3 \times 1} \quad \text{مصفوفة الانحيازات } L = 1 \text{ (طبقة المدخلات)}$$

حيث أن $k = 1, 2, 3$ وكذلك $q = 3$.

$$H^2 = \begin{bmatrix} h_1^2 \\ h_2^2 \\ h_3^2 \end{bmatrix}_{3 \times 1} \quad \text{مصفوفة الطبقة الخفية الأولى } L = 2$$

حيث أن $k = 1, 2, 3$ و $q = 3$.

مصفوفة الأوزان $L = 2$ (التي تربط بين الطبقة التي نقف عندها وهي الطبقة الخفية الأولى والطبقة التي نتجه إليها وهي الطبقة الخفية الثانية التي سوف نحسبها بالتالي بين $L = 2$ و $L = 3$).

$$W^2 = \begin{bmatrix} w_{11}^2 & w_{21}^2 & w_{31}^2 \\ w_{12}^2 & w_{22}^2 & w_{32}^2 \\ w_{13}^2 & w_{23}^2 & w_{33}^2 \end{bmatrix}_{3 \times 3}$$

حيث أن $g = 1, 2, 3$ و $p = 3$ و $j = 1, 2, 3$ و $p' = 3$.

$$B^2 = \begin{bmatrix} b_1^2 \\ b_2^2 \\ b_3^2 \end{bmatrix}_{3 \times 1} \quad \text{مصفوفة الانحيازات } L = 2 \text{ أي الطبقة الخفية الأولى}$$

حيث أن $k = 1, 2, 3$ و $q = 3$.

$$H^3 = \begin{bmatrix} h_1^3 \\ h_2^3 \\ h_3^3 \end{bmatrix}_{3 \times 1} \quad \text{مصفوفة الطبقة الخفية الثانية } L = 3$$

حيث أن $k = 1, 2, 3$ و $q = 3$.

مصفوفة الأوزان $L = 3$ (التي تربط بين الطبقة التي نقف عندها وهي الطبقة الخفية الثانية والطبقة التي نتجه إليها وهي الطبقة المخرجات التي سوف نحسبها أي بين $L = 3$ و $L = 4$).

$$W^3 = \begin{bmatrix} w_{11}^3 & w_{21}^3 & w_{31}^3 \\ w_{12}^3 & w_{22}^3 & w_{32}^3 \end{bmatrix}_{2 \times 3}$$

حيث أن $g = 1, 2, 3$ و $p = 3$ و $j = 1, 2$ و $p' = 2$.

$$B^3 = \begin{bmatrix} b_1^3 \\ b_2^3 \end{bmatrix}_{2 \times 1} \quad \text{مصفوفة الانحيازات } L = 3 \text{ أي الطبقة الخفية الثانية}$$

حيث أن $k' = 1, 2$ و $q' = 2$.

$$O^{4,1} = \begin{bmatrix} o_1^{4,1} \\ o_2^{4,1} \end{bmatrix}_{2 \times 1} \quad \text{مصفوفة الطبقة المخرجات } L = 4$$

حيث أن $t = 1$ وأن $k' = 1, 2, 3$ و $q' = 3$.

بالتالي بتطبيق القوانين (12.5) و (14.5) و (16.5) نجد:

$$H^2 = f(Z^2) = f(W^1 X^1 + B^1) = f \left(\begin{bmatrix} w_{11}^1 & w_{21}^1 \\ w_{12}^1 & w_{22}^1 \\ w_{13}^1 & w_{23}^1 \end{bmatrix} \begin{bmatrix} x_1^1 \\ x_2^1 \end{bmatrix} + \begin{bmatrix} b_1^1 \\ b_2^1 \\ b_3^1 \end{bmatrix} \right)$$

$$= f \left(\begin{bmatrix} w_{11}^1 x_1^1 + w_{21}^1 x_2^1 \\ w_{12}^1 x_1^1 + w_{22}^1 x_2^1 \\ w_{13}^1 x_1^1 + w_{23}^1 x_2^1 \end{bmatrix} + \begin{bmatrix} b_1^1 \\ b_2^1 \\ b_3^1 \end{bmatrix} \right)$$

$$= f \left(\begin{bmatrix} w_{11}^1 x_1^1 + w_{21}^1 x_2^1 + b_1^1 \\ w_{12}^1 x_1^1 + w_{22}^1 x_2^1 + b_2^1 \\ w_{13}^1 x_1^1 + w_{23}^1 x_2^1 + b_3^1 \end{bmatrix} \right) = \begin{bmatrix} f(w_{11}^1 x_1^1 + w_{21}^1 x_2^1 + b_1^1) \\ f(w_{12}^1 x_1^1 + w_{22}^1 x_2^1 + b_2^1) \\ f(w_{13}^1 x_1^1 + w_{23}^1 x_2^1 + b_3^1) \end{bmatrix} = \begin{bmatrix} h_1^2 \\ h_2^2 \\ h_3^2 \end{bmatrix}$$

وهذا ما يوافق القانون (11.5) حيث يمكن أن نكتب

$$h_1^2 = f(w_{11}^1 x_1^1 + w_{21}^1 x_2^1 + b_1^1) = f \left(\sum_{r=1}^2 w_{r1}^1 x_r^1 + b_1^1 x_o^1 \right) ; x_o^1 = 1$$

$$h_2^2 = f(w_{12}^1 x_1^1 + w_{22}^1 x_2^1 + b_2^1) = f \left(\sum_{r=1}^2 w_{r2}^1 x_r^1 + b_2^1 x_o^1 \right) ; x_o^1 = 1$$

$$h_3^2 = f(w_{13}^1 x_1^1 + w_{23}^1 x_2^1 + b_3^1) = f \left(\sum_{r=1}^2 w_{r3}^1 x_r^1 + b_3^1 x_o^1 \right) ; x_o^1 = 1$$

$$H^3 = f(Z^3) = f(W^2 H^2 + B^2) = f \left(\begin{bmatrix} w_{11}^2 & w_{21}^2 & w_{31}^2 \\ w_{12}^2 & w_{22}^2 & w_{32}^2 \\ w_{13}^2 & w_{23}^2 & w_{33}^2 \end{bmatrix} \begin{bmatrix} h_1^2 \\ h_2^2 \\ h_3^2 \end{bmatrix} + \begin{bmatrix} b_1^2 \\ b_2^2 \\ b_3^2 \end{bmatrix} \right)$$

$$= f \left(\begin{bmatrix} w_{11}^2 h_1^2 + w_{21}^2 h_2^2 + w_{31}^2 h_3^2 \\ w_{12}^2 h_1^2 + w_{22}^2 h_2^2 + w_{32}^2 h_3^2 \\ w_{13}^2 h_1^2 + w_{23}^2 h_2^2 + w_{33}^2 h_3^2 \end{bmatrix} + \begin{bmatrix} b_1^2 \\ b_2^2 \\ b_3^2 \end{bmatrix} \right) = f \left(\begin{bmatrix} w_{11}^2 h_1^2 + w_{21}^2 h_2^2 + w_{31}^2 h_3^2 + b_1^2 \\ w_{12}^2 h_1^2 + w_{22}^2 h_2^2 + w_{32}^2 h_3^2 + b_2^2 \\ w_{13}^2 h_1^2 + w_{23}^2 h_2^2 + w_{33}^2 h_3^2 + b_3^2 \end{bmatrix} \right)$$

$$= \begin{bmatrix} f(w_{11}^2 h_1^2 + w_{21}^2 h_2^2 + w_{31}^2 h_3^2 + b_1^2) \\ f(w_{12}^2 h_1^2 + w_{22}^2 h_2^2 + w_{32}^2 h_3^2 + b_2^2) \\ f(w_{13}^2 h_1^2 + w_{23}^2 h_2^2 + w_{33}^2 h_3^2 + b_3^2) \end{bmatrix} = \begin{bmatrix} h_1^3 \\ h_2^3 \\ h_3^3 \end{bmatrix}$$

وهذا ما يوافق القانون (13.5) حيث يمكن أن نكتب

$$h_1^3 = f(w_{11}^2 h_1^2 + w_{21}^2 h_2^2 + w_{31}^2 h_3^2 + b_1^2) = f\left(\sum_{r=1}^3 w_{r1}^2 h_r^2 + b_1^2 h_o^2\right); h_o^2 = 1$$

$$h_2^3 = f(w_{12}^2 h_1^2 + w_{22}^2 h_2^2 + w_{32}^2 h_3^2 + b_2^2) = f\left(\sum_{r=1}^3 w_{r2}^2 h_r^2 + b_2^2 h_o^2\right); h_o^2 = 1$$

$$h_3^3 = f(w_{13}^2 h_1^2 + w_{23}^2 h_2^2 + w_{32}^2 h_3^2 + b_3^2) = f\left(\sum_{r=1}^3 w_{r3}^2 h_r^2 + b_3^2 h_o^2\right); x_o^1 = 1$$

$$\begin{aligned} O^{4,1} &= f(Z^{4,1}) = f(W^3 H^3 + B^3) = f\left(\begin{bmatrix} w_{11}^3 & w_{21}^3 & w_{31}^3 \\ w_{12}^3 & w_{22}^3 & w_{32}^3 \end{bmatrix} \begin{bmatrix} h_1^3 \\ h_2^3 \\ h_3^3 \end{bmatrix} + \begin{bmatrix} b_1^3 \\ b_2^3 \end{bmatrix}\right) \\ &= f\left(\begin{bmatrix} w_{11}^3 h_1^3 + w_{21}^3 h_2^3 + w_{31}^3 h_3^3 \\ w_{12}^3 h_1^3 + w_{22}^3 h_2^3 + w_{32}^3 h_3^3 \end{bmatrix} + \begin{bmatrix} b_1^3 \\ b_2^3 \end{bmatrix}\right) = f\left(\begin{bmatrix} w_{11}^3 h_1^3 + w_{21}^3 h_2^3 + w_{31}^3 h_3^3 + b_1^3 \\ w_{12}^3 h_1^3 + w_{22}^3 h_2^3 + w_{32}^3 h_3^3 + b_2^3 \end{bmatrix}\right) \\ &= \begin{bmatrix} f(w_{11}^3 h_1^3 + w_{21}^3 h_2^3 + w_{31}^3 h_3^3 + b_1^3) \\ f(w_{12}^3 h_1^3 + w_{22}^3 h_2^3 + w_{32}^3 h_3^3 + b_2^3) \end{bmatrix} = \begin{bmatrix} o_1^{4,1} \\ o_2^{4,1} \end{bmatrix} \end{aligned}$$

وهذا ما يوافق القانون (15.5) حيث يمكن أن نكتب

$$o_1^{4,1} = f(w_{11}^3 h_1^3 + w_{21}^3 h_2^3 + w_{31}^3 h_3^3 + b_1^3) = f\left(\sum_{r=1}^3 w_{r1}^3 h_r^3 + b_1^3 h_o^3\right); h_o^3 = 1$$

$$o_2^{4,1} = f(w_{12}^3 h_1^3 + w_{22}^3 h_2^3 + w_{32}^3 h_3^3 + b_2^3) = f\left(\sum_{r=1}^3 w_{r2}^3 h_r^3 + b_2^3 h_o^3\right); h_o^3 = 1$$

الأسلوب السابق بالحسابات بدءاً من طبقة المدخلات حتى طبقة المخرجات يسمى بالمسار الأمامي (Forward Propagation) وكوننا لا نستخدم أي حلقات أو تكرارات فإننا نتعامل مع ما يسمى بالتغذية الأمامية (Feed-Forward). أما لو كان لدينا أي تكرارات فإنه يتم التعديل على هذا المسار الأمامي بحيث يحمل بقوانينه التغذية الراجعة (Feed-Back) وهذا ما سوف نراه لاحقاً مع الشبكة العصبية المتكررة. بالنسبة لتتابع التفعيل عادةً يتم استخدام $Tanh(x)$ في حساب نواتج الخلايا الخفية و $\sigma(x)$ في حساب الناتج النهائي.

بعد المسار الأمامي يتم حساب معادلة الخطأ (Loss Function) وذلك باعتبار y^t هو الخرج الفعلي وأن $\hat{y}^t$ هو الخرج المتوقع $O^{L,t}$. حيث كلاً من y^t و $O^{L,t}$ مصفوفات وعندها نكتب معادلة الخطأ بأخذ دالة متوسط الخطأ التربيعي (Mean Square Error, MSE) بالشكل:

$$E = MSE(y^t, \hat{y}^t) = (y^t - \hat{y}^t)^2 \dots (17.5)$$

ولأننا سوف نقوم بالاشتقاق على التعديل على المعادلة (17.5) واستخدام دالة متوسط الخطأ التربيعي المعدلة، فتكتب معادلة الخطأ بالشكل:

$$E(t) = \frac{1}{2} (y^t - O^{L,t})^2 \dots (18.5)$$

وكون المهمة هي تحديث الأوزان والانحيازات من أجل تقليل قيمة الخطأ سوف نقوم بما يسمى بالمسار الخلفي (Back Propagation) وباستخدام التدرج الاشتقاقي أو ما يسمى بالانحدار التدريجي (Gradient Descent) الذي يطبق قاعدة السلسلة (Chain Rule) [18].

بال تطبيق على المثال السابق واستخدام القانون (18.5). باعتبار أن لدينا مصفوفات الأوزان تحتوي 21 وزن أما مصفوفات الانحيازات فتحتوي على 8 انحيازات، و $t = 1$.

$$\frac{\partial E(t)}{\partial W^3} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial W^3} \dots (19.5)$$

$$\frac{\partial E(t)}{\partial W^2} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial H^3} \cdot \frac{\partial H^3}{\partial Z^3} \cdot \frac{\partial Z^3}{\partial W^2} \dots (20.5)$$

$$\frac{\partial E(t)}{\partial W^1} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial H^3} \cdot \frac{\partial H^3}{\partial Z^3} \cdot \frac{\partial Z^3}{\partial H^2} \cdot \frac{\partial H^2}{\partial W^1} \dots (21.5)$$

$$\frac{\partial E(t)}{\partial B^3} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial B^3} \dots (22.5)$$

$$\frac{\partial E(t)}{\partial B^2} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial H^3} \cdot \frac{\partial H^3}{\partial Z^3} \cdot \frac{\partial Z^3}{\partial B^2} \dots (23.5)$$

$$\frac{\partial E(t)}{\partial B^1} = \frac{\partial E(t)}{\partial O^{4,1}} \cdot \frac{\partial O^{4,1}}{\partial Z^{4,1}} \cdot \frac{\partial Z^{4,1}}{\partial H^3} \cdot \frac{\partial H^3}{\partial Z^3} \cdot \frac{\partial Z^3}{\partial H^2} \cdot \frac{\partial H^2}{\partial B^1} \dots (24.5)$$

وعندها باعتبار أن α هو معامل التعلم (Learning Rate) عندها تحديث الأوزان يعطى بالعلاقات.

$$W_{new}^3 = W^3 - \alpha \frac{\partial E(t)}{\partial W^3} \dots (25.5)$$

$$W_{new}^2 = W^2 - \alpha \frac{\partial E(t)}{\partial W^2} \dots (26.5)$$

$$W_{new}^1 = W^1 - \alpha \frac{\partial E(t)}{\partial W^1} \dots (27.5)$$

$$B_{new}^3 = B^3 - \alpha \frac{\partial E(t)}{\partial B^3} \dots (28.5)$$

$$B_{new}^2 = B^2 - \alpha \frac{\partial E(t)}{\partial B^2} \dots (29.5)$$

$$B_{new}^1 = B^1 - \alpha \frac{\partial E(t)}{\partial B^1} \dots (30.5)$$

$$W_{new}^L = W^L - \alpha \frac{\partial E(t)}{\partial W^L} \dots (32.5), B_{new}^L = B^L - \alpha \frac{\partial E(t)}{\partial B^L} \dots (31.5) \quad \text{بالتعميم نجد أن}$$

يعطى قانون الخطأ الكلي بالشكل الآتي:

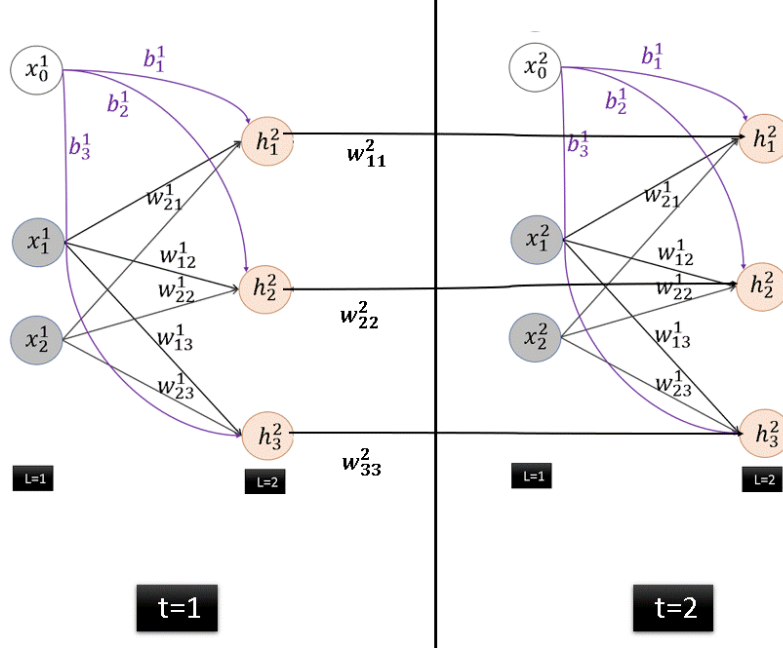
$$E = \sum_{t=1}^m E(t) = \sum_{t=1}^m \frac{1}{2} (y^t - o^{L,t})^2 \dots (33.5)$$

وبتكرار المسارين الأمامي والخلفي يتم تدريب الشبكة حتى تصل لأصغر قيمة للخطأ عندها تستقر الشبكة.

2.3.5. مفهوم شبكة RNN [41]

تعد الـ RNN واحدة من الشبكات العصبية التي تعتمد على ما يسمى التغذية الراجعة (Feed-Back). هذه الشبكة تحوي تكرارات مع تطبيق كلاً من المسار الأمامي والخلفي. لفهم ما هو معنى التكرارات والحلقات نلاحظ أن بالقوانين السابقة لدينا حساب بحسب قيم t والتي تمثل رقم السجل حيث $t = 1, \dots, m$ و m هو عدد كامل السجلات. في كل معادلة لم يتم الأخذ بعين الاعتبار إلا t أما الآن فلحساب ناتج خلية الخفية عند t يجب معرفة القيم والحسابات السابقة لنفس الخلية الخفية ولكن عند $t - 1$. كل سجل يعتمد على ما سبقه من سجلات وهذا هو مفهوم التكرار وهو ما يجعل النموذج قادر على تتبع الزمني للأحداث بأسلوب أكثر سهولة. بالتالي يمكن تصور لشكل الشبكة العصبية المتكررة بحسب المثال السابق كما في الشكل 5.5. الذي يوضح الحلقات والتكرارات في الشبكة العصبية المتكررة. حيث هو $t = 1$ السجل الأول أما $t = 2$ هو السجل الثاني. القسم اليسار هو حساب الخلايا العصبية للطبقة العصبية الأولى عند السجل الأول. أما القسم الأيمن هو حسابات الخلايا العصبية للطبقة

الخفية الأولى للسجل الثاني والتي تُحسب بالاستفادة من حسابات السجل السابق. هذا ما يحدث عند حساب أي ناتج لخلية عصبية بحسب كل سجل.



الشكل 5.5. مثال يوضح بنية الشبكة العصبية المتكررة.

وعندها تصبح القوانين كما يلي وذلك بتسمية الخرج السابق في الزمن $t - 1$ للخلية العصبية الخفية نفسها بـ $a_k^{L,t-1}$ عوضاً عن h_k^L وذلك لسهولة التعامل في الحسابات. عندها تصبح لدينا مصفوفة الطبقة الخفية بالرمز $A^{L,t-1}$ عوضاً عن الرمز H^L . أما باقي الرموز فتبقى كما هي.

يمكن أن نكتب قانون مصفوفة الطبقة الخفية الأولى عندما $L = 2$ بالشكل:

$$H^{2,t} = f(W_{ah}^1 A^{1,t-1} + W_{xh}^1 X^t + B_h^1) = f(Z^{2,t}) \quad \dots (34.5)$$

أما عند الطبقات الخفية الباقية أي عندما $L = 3$ فما فوق يكون القانون:

$$H^{L,t} = f(W_{ah}^{L-1} A^{L,t-1} + W_{hh}^{L-1} H^{L-1,t} + B_h^{L-1}) = f(Z^{L,t}) \quad \dots (35.5)$$

ويعطى قانون الناتج النهائي بالقانون:

$$O^{L,t} = f(W_{ho}^{L-1} H^{L-1,t} + B_o^{L-1}) = f(Z^{L,t}) \quad \dots (36.5)$$

بالمقارنة بين المعادلة (12.5) و (34.5) نجد أن $W_{xh}^1 X^t = W^1 X^t$ وأن $B_h^1 = B^1$.

بالمقارنة بين المعادلة (14.5) و (35.5) نجد أن $W_{hh}^{L-1} H^{L-1,t} = W^{L-1} H^{L-1}$ وأن $B_h^{L-1} = B^{L-1}$.

بالمقارنة بين المعادلة (16.5) و (36.5) نجد أن $W_{ho}^{L-1}H^{L-1,t} = W^{L-1}H^{L-1}$ وأن $B_o^{L-1} = B^{L-1}$.

أما بالنسبة لمعادلة الخطأ والمسار الخلفي يتم بنفس الأسلوب مع ملاحظة وجود أوزان جديدة التي تربط بين الزمنين t و $t - 1$. تعديل الأوزان يكون بنفس الأسلوب والقوانين ذاتها المعادلات رقم (18.5)، (31.5)، (32.5)، (33.5) هي القوانين المستخدمة في الـ RNN. أما توابع التنفيع فهي التوابع المستخدمة المذكورة ذاتها.

تطوراً لـ RNN ظهرت أنواع لتعالج المشاكل الموجودة مثل مشاكل بالاشتقاق أو تتبّع الأحداث لفترة أطول وهي:

☞ الوحدة متكررة البوابة (Gated Recurrent Unit, GRU).

☞ الذاكرة طويلة (قصيرة) المدى (Long (Short) Term Memory, LSTM).

لكتابة قوانين كل منهما يجب توضيح لرمز معين سوف نستخدمه في القوانين. لتكن لدينا المتجهات الآتية

$$X^t = [d, e] \text{ و } h^{t-1} = [a, b, c] \text{ عندها يكون } [X^t, h^{t-1}] = [d, e, a, b, c]$$

المعادلات في الـ GRU هي [29]:

$$u^t = \sigma(W_u \cdot [X^t, A^{t-1}] + B_u) \quad \dots (37.5) \quad \text{بوابة التجديد (Update Gate)}$$

$$r^t = \sigma(W_r \cdot [X^t, A^{t-1}] + B_r) \quad \dots (38.5) \quad \text{بوابة الإعادة (Reset Gate)}$$

$$\tilde{H}^t = \tanh(W_h \cdot [r^t * X^t, A^{t-1}] + B_h) \quad \dots (39.5) \quad (* \text{ الضرب العنصري })$$

$$H^t = (1 - u^t) * A^{t-1} + u^t * \tilde{H}^t \quad \dots (40.5) \quad \text{لحساب ناتج الطبقة الخفية}$$

u^t تحدد فيما إذا كان سيتم تحديث الذاكرة بمعلومات جديدة أم لا: فإذا أخذت القيمة 1 أي تحديث الذاكرة وإضافة معلومات جديدة (المدخلات الجديدة)، أما 0 عدم تحديثها.

r^t تحدد فيما إذا سيتم تذكر المعلومات القديمة أم لا: فإذا أخذت القيمة 1 بمعنى تذكر المعلومات القديمة وإضافتها للذاكرة، أما 0 عدم تذكرها.

$\tilde{H}^t$ هي الذاكرة الجديدة التي سيتم إضافة المعلومات الجديدة إليها.

H^t هي الخرج والذاكرة النهائية للخلية العصبية التي قد تحتفظ بمعلومات الذاكرة الجديدة أو المعلومات القديمة.

المعادلات في الـ LSTM هي [20]:

$$f^t = \sigma(W_f \cdot [X^t, A^{t-1}] + B_f) \quad \dots (41.5) \quad \text{بوابة النسيان (Forget Gate)}$$

$$i^t = \sigma(W_i \cdot [X^t, A^{t-1}] + B_i) \quad \dots (42.5) \quad \text{بوابة الإدخال (Input Gate)}$$

$$\tilde{c}^t = \tanh(W_c \cdot [X^t, A^{t-1}] + B_c) \quad \dots (43.5) \quad \text{محتوى الذاكرة الجديدة}$$

$$c^t = f^t * c^{t-1} + i^t * \tilde{c}^t \quad \dots (44.5) \quad (* \text{ الضرب العنصري })$$

$$o^t = \sigma(W_o \cdot [X^t, A^{t-1}] + B_o) \quad \dots (45.5) \quad \text{بوابة الخرج (Output Gate)}$$

$$h^t = o^t \cdot \tanh(c^t) \quad \dots (46.5) \quad \text{حالة (الذاكرة) نهائية}$$

f^t تحدد فيما إذا سيتم تذكر المعلومات القديمة أم لا: فإذا أخذت القيمة 1 ويعني ذلك تذكر المعلومات القديمة وإضافتها للذاكرة، أما 0 فهذا يعني عدم تذكرها.

r^t تحدد فيما إذا نضيف المعلومات الجديدة على الذاكرة الجديدة أم لا: فإذا أخذت القيمة 1 فيتم تحديث الذاكرة وإضافة معلومات جديدة (المدخلات الجديدة)، أما 0 فهذا يعني عدم تحديثها.

o^t تحدد فيما إذا سيتم أخذه محتويات الذاكرة النهائية كمخرجات أم لا: فإذا أخذت القيمة 1 أي أخذ محتويات الذاكرة وإضافتها كخرج، أما 0 فهذا يعني عدم أخذها.

c^t تمثل الذاكرة النهائية للخلية العصبية التي قد تحوي المعلومات القديمة أو الجديدة أو كلاهما معاً.

$\tilde{c}^t$ تمثل الذاكرة الجديدة المؤقتة التي سوف نضيف فيها المعلومات الجديدة.

3.3.5. تحليل سلوك المستخدم باستخدام الـ RNN

تم استخدام شبكة الـ RNN بأنواعها في الـ UBA. في هذه الدراسات التي سنتطرق لها تم استخدام مجموعة بيانات اصطناعية cert بإصدار r4.2. هذه البيانات مخصصة لدراسة كشف التهديد الداخلي وسوف نتحدث عنها في الفصل السادس. في الدراسة الأولى [31] تم تصميم نموذج باستخدام الـ GRU والتشفير التلقائي (Autoencoder). أما في الدراسة الثانية [11] فقد استخدمت شبكة الـ GRU والتعامل مع سلوك المستخدم كسلسلة زمنية مشابهة للتسلسل النصي الموجود في تسلسل اللغة الطبيعية. تعتبر الدراستين من الدراسات الهامة لتطبيقها طريقة حديثة ومبتكرة. في الفقرات الآتية شرح تفصيلي لكلتا الدراستين.

في الدراسة الأولى [31] تم توضيح أهمية تصميم نموذج لكشف التهديد الداخلي لكونه أكثر صعوبة من كشف التهديد الخارجي. بالطبع تم ذكر كون الطرق التقليدية مثل جدران الحماية أثبتت فشلها في هذا المجال. تقوم الدراسة على تجميع الأحداث اليومية واستخراج الميزات (Features) وتصميم النموذج يتعلم الأنماط العادية والنشاط الطبيعي للمستخدم من ثم التعرف على النشاط الشاذ من خلال مقارنة قيمة معالجة الخطأ لكل مدخل مع عتبة

محددة (Threshold). تم تجميع الأحداث اليومية في متجهات بحسب الميزات التي تم استخراجها. لتكون البيانات مناسبة للنموذج والدخول إلى الشبكة تم تطبيع البيانات لتصبح ضمن النطاق من 0 إلى 1. كان التطبيع باستخدام مقياس نموذج الأقصى الإحصائي (Statistical Max Model Scaling) المعطى بالقانون الآتي حيث $X_{(i,m)}$ هو نشاط المستخدم الواحد:

$$X_{(i,m)} = \frac{X_{(i,m)}}{(X_m)_{max}} \quad \dots \dots (47.5)$$

تم برمجة النموذج باستخدام معدل التعلم 0.001 والمحسن Adam وعدد الدورات (Epochs) بمقدار 100 وحجم الدفعة (Batch Size) بمقدار 256 ولغة البرمجة Python. تم اختبار عتبات مختلفة وكانت 0.03 العتبة المثلى. استخدم في معادلة الخطأ معادلة متوسط الخطأ المطلق (Mean Absolute Error, MAE) والتي تعطى بالعلاقة الآتية:

$$MAE = \frac{1}{N} \sum_i^N |x_i - x| \quad \dots \dots (48.5)$$

حيث x_i هو المدخل أما x فهو المخرج الذي يمثل فك تشفير المدخل. لتحديد الشذوذ استخدم المعيار المعطى بالقانون حيث E هي قيمة معادلة الخطأ:

$$f(x_i) = \begin{cases} Anomaly & \text{if } E_i \geq Thershold \\ Normal & \text{otherwise} \end{cases} \quad \dots \dots (49.5)$$

أثبت النموذج نجاحاً عند العتبة المنخفضة ولكنه فشل بتصنيف بعض القيم الإيجابية (السلوك الشاذ). حيث كان تقييم النموذج شاملاً نوعاً ما وبلغت الدقة القيمة 80.1% أما قيمة الـ AUC فكانت 0.8732 وهي قيمة جيدة. من القيم السابقة نجد أن النموذج جيد جداً في تمييز السلوك الطبيعي. من التوصيات أنه قد يكون استخدام شبكة الـ LSTM أفضل. من نقاط قوة هذه الدراسة التقييم الشامل للنموذج مما يبين قدرات النموذج بشكل جيد ولكن بالمقابل لم يتم إعطاء أسباب واضحة لمشكلة النموذج في تمييز السلوك الشاذ ولا تقديم حلول مناسبة.

أما في الدراسة الثانية [11] تم استخراج الميزات. البيانات المستخرجة تم التعامل معها بشكل مشابه لتسلسل اللغة الطبيعية (التعامل معها ككلمات) وتم تحويل البيانات لتمثيل رقمي باستخدام (One-Hot-Vector). تمت برمجة النموذج باعتماد 20 دورة الذي يسعى لكشف الأنماط الطبيعية لكل مستخدم وملاحظة أي انحراف عنها كنشاط غير متوقع وتصنيفه كتهديد محتمل. لم يتم تقديم تقييم شاملاً للنموذج إلا أن الدقة العامة كانت نسبة 92%. ذكرت الدراسة أن النموذج يواجه مشكلة مع البيانات غير المتوازنة حيث عدد السجلات التي تحوي سلوك شاذ قليل

جداً مقارنةً مع السجلات التي تحمل سلوكاً طبيعياً. من التوصيات استخدام خوارزمية الـ ADASYN لحل مشكلة النموذج. من نقاط قوة الدراسة أن النموذج يتمتع بدقة عامة عالية وتم تقديم أسباب واضحة مع حلول لمشكلة النموذج ولكن من الجدير بالذكر أنه لم يتم تقديم تقييم شامل للنموذج واقتصره على 20 دورة فقط.

فمن جانب آخر تم استخدام شبكة الـ LSTM في الدراسة الثالثة [12] التي وضحت صعوبة كشف التهديدات الداخلية وأهمية تقنية الـ UBA في هذا الصدد. قد قدمت الدراسة وصفاً أكثر تفصيلاً للنموذج من سابقتها حيث ذكر أن تم تقسيم العمل على نموذجين الأول لتعلم السلوك الطبيعي للمستخدم والثاني لكشف الشذوذ. تمت مناقشة طريقة استخراج الميزات بالتفصيل وبالطبع تطبيع البيانات في النموذج الأول والتطبيع كان باستخدام القانون:

$$p'_j = \frac{p_j - \min(p_j)}{\max(p_j) - \min(p_j)} \quad \dots \dots (50.5)$$

حيث p_j هي نشاط المستخدم ومن ثم حساب معادلة الخطأ كان باستخدام MSE التي تعطى بالعلاقة:

$$MSE = \frac{1}{N} \sum_i^N |x_i - y_i|^2 \quad \dots \dots (51.5)$$

حيث x_i هو المدخل أما y_i فهو المخرج و N عدد السجلات. تم تحديد العتبة المناسبة ϑ من خلال القانون:

$$\vartheta = \gamma \left(\frac{1}{N} \sum_i^N \varepsilon_i \right) \quad \dots \dots (52.5)$$

حيث γ ثابت لتعديل العتبة و ε_i قيمة الخطأ للسلسلة i الخاصة بأنشطة المستخدم الواحد.

أما في النموذج الثاني كشف السلوك الشاذ كان من خلال المعيار:

$$y_i = \begin{cases} Anomaly & \text{if } \varepsilon_i > \vartheta \\ Normal & \text{otherwise} \end{cases} \quad \dots \dots (53.5)$$

تمت برمجة النموذج باستخدام 5 طبقات خفية وحجم دفعة بمقدار 50 وعدد الدورات 10 وتقسيم البيانات 70% من البيانات للتدريب و30% للاختبار مع معدل تعلم 1. تجربة ثلاث نماذج تختلف بعدد الخلايا مختلفة في كل طبقة واثبت النموذج الأول الذي يحوي عدد خلايا أكثر دقة عليا حيث قيمة الـ AUC فكانت 0.97 وهي قيمة مرتفعة. من نقاط قوة الدراسة الدقة العالية التي حققها النموذج الأول ومناقشة تفصيلية لاستخراج الميزات إلا أنها لم تقدم تقييم شامل للنموذج على الرغم من تجربة عدة نماذج فهي لا تكفي لإثبات فاعلية النماذج.

تستخدم الدراستان الأولى والثانية الشبكة العصبية ذاتها التي سيُبنى النموذج المقترح وفقها. في الفصل السادس سنقوم بعرض مقارنة بين نموذجنا المقترح وهاتين الدراستين، موضحين كفاءته مقارنةً مع نماذج مشابهة من حيث نوع الشبكة. أما في الدراسة الثالثة [12] فهي تستخدم نوع شبكة متكررة مختلفة عن المستخدمة في النموذج وهو شبكة الـ LSTM. سنقدم مقارنة بسيطة ما بين الدراسة الثالثة ونموذجنا المقترح في الفصل السادس. نعيد المقارنة بدراسة مختلفة من حيث نوع الشبكة لتوضيح إمكانية بناء نموذج قوي باستخدام شبكة الـ GRU يفوق بقدراته نموذج مبني بشبكة أقوى مثل شبكة الـ LSTM.

4.5. خلاصة الفصل

قدّمنا في هذا الفصل شرحاً مفصلاً لأهم الخوارزميات المستخدمة في تقنية الـ UBA. ناقشنا دراسة استخدمت خوارزمية الـ SVM المطبقة على بيانات النقر وقد لاحظنا أن النموذج كان فعال أكثر من بعض النماذج الأخرى مثل أشجار القرار. شرحنا مبدأ عمل الشبكات العصبية بالتفصيل وركزنا على شبكة الـ RNN. تحدثنا عن 3 دراسات استخدمت الـ RNN بأنواعها والتي استخدمت مجموعة البيانات ذاتها. تبين من الدراسات السابقة التي عرضناها أن مازالت النماذج المطبقة تواجه صعوبات في كشف الشذوذ. لاحظنا أن المشكلة في تلك الدراسات كانت نتيجة لعدم توازن البيانات. في سبيل معالجة المشكلة اقترحنا نموذج هجين بين الـ GRU والـ GA. سوف نقدم هذا النموذج في الفصل القادم.

الفصل السادس

النموذج المقترح

1.6 مقدمة

ساعدت أنواع الخوارزميات المختلفة على مر العصور في حل الكثير من المسائل. من بين هذه الخوارزميات تلك التي تبحث عن الحل الأمثل والتي تسمى بالخوارزميات الأمثلية. في هذا الفصل سنتحدث عن النموذج المقترح ونشرح طريقة تصميمه بالتفصيل. لذلك لا بد من توضيح بعض الأدوات التي سوف نستخدمها. ففي الفقرة 2.6 نتحدث عن الخوارزمية الجينية وهي واحدة من تلك الخوارزميات الأمثلية. أما في الفقرة 3.6 سوف نقوم بتحديد مجموعة البيانات المستخدمة. أما في الفقرة 4.6 سوف نعرض المراحل الخمس التي مر بها النموذج الهجين الذي اقترحناه. قمنا بتصميم النموذج ليعمل بشكل مشابه لنهج التشفير التلقائي (Autoencoder) بهدف حل مشكلة عدم توازن البيانات. أخيراً في الفقرة 5.6 سوف نناقش النتائج التي حصلنا عليها.

2.6 الخوارزمية الجينية (Genetic Algorithm, GA)

يعود أصل الخوارزمية الجينية لما يسمى بالخوارزميات التطورية (Evolutionary Algorithms) التي تم تقديمها أول مرة في عام 1965 [13]. أما الخوارزمية الجينية تم تقديمها لاحقاً في عام 1975 على يد جون هولاند (John Holland). من المعروف أن هذه الخوارزمية مستوحاة من الواقع فهي تحاكي مبدأ الوراثة والتمثيل الجيني للكائنات الحية [40]. يمكن شرح هذه الخوارزمية على أنها مجموعة من الخطوات والتعليمات التي تهدف لحل مسألة ما والوصول لأقرب حل أو الحل الأمثل بين مجموعة من الحلول.

تتألف الكائنات الحية عموماً من مجموعة خلايا. كل خلية تحمل سلاسل من الـ DNA. كل سلسلة تسمى صبغي (Chromosome). يقسم كل صبغي لمجموعة من الجينات (Genes) التي تحمل صفات الكائن. بشكل مشابه لـ GA يكون لدينا مجموعة من الأفراد وكل فرد يتمثل على شكل صبغي الذي يُقسم بدوره لمجموعة من الجينات. لكن على خلاف الجين الموجود في الخلية الحية، كل جين هو عبارة عن بت (Bit) أي 0 أو 1.

أما آلية عمل الـ GA فسوف نعرضها وفق مجموعة من المراحل كما يلي [40]:

- **الخطوة الأولى:** التعداد السكاني الابتدائي (Initial Population) بإنشاء مجموعة من n صبغي.
- **الخطوة الثانية:** حساب كفاءة كل صبغي.
- **الخطوة الثالثة:** تكرار مجموعة من الخطوات للحصول على n صبغي جديد.
- **الخطوة الرابعة:** استبدال المجموعة القديمة من الصبغيات بالمجموعة الجديدة.

• **الخطوة الخامسة:** التكرار من الخطوة الثانية للوصول لشرط توقف ما.

لنشرح كلاً من الخطوات السابقة بالتفصيل [28]:

التعداد السكاني الابتدائي: يتم إنشاء مجموعة عشوائية من الصبغيات n صبغي عشوائي في المجموعة الأولية وهي مجموعة الأفراد الأولية. كل صبغي يمثل حل من حلول المشكلة على شكل سلسلة بطول L من القيم الممثلة بالنظام العد الثنائي ويمكن اعتماد نظام عد آخر.

حساب كفاءة كل صبغي: وذلك من خلال دالة اللياقة (Fitness Function) وهي تابع رياضي يمكن تحديده بما يتناسب مع المسألة. الصبغي الأفضل هو صاحب أكبر أو أصغر قيمة للدالة حسب نوع المسألة.

تكرار مجموعة من الخطوات للحصول على مجموعة جديدة:

أولاً الاختيار (Selection) وذلك باختيار أفضل زوج (أو أزواج) صبغيات من المجموعة الحالية. يتم ذلك بالاعتماد على قيم دالة اللياقة المحسوبة لكل صبغي. الصبغيات المختارة تعتبر الصبغيات الآباء ويفضل اختيار عدد من الآباء وليكن m .

ثانياً التقاطع (Crossover): وهي مرحلة التزاوج لإنتاج الصبغيات الأبناء. يتم ذلك بتبادل أجزاء بين الصبغيات الآباء وبالتالي دمج كل صبغيين للحصول على صبغيين جديدين. يوجد عدة طرق لهذا التقاطع. الجدول 1.6. يوضح الصبغيين الآباء المختارين.

الجدول 1.6. الصبغيين الآباء في الـ GA.

01010101	صبغي أب 1
11110000	صبغي أب 2

الطريقة الأولى للتقاطع هي تجزئة السلسلة الخاصة لكل صبغي لقسمين وتبديل الجزء الأيمن مع الأيمن أو الأيسر مع الأيسر. مثلاً تجزئة السلسلتين السابقتين من اليسار إلى اليمين بـ 3 خانات إلى 5 خانات كما في الجدول 2.6. الذي يوضح طريقة التجزئة المذكورة.

الجدول 2.6. تقسيم الصبغيين الآباء بطريقة التقاطع الأولى.

01010101	صبغي أب 1
11110000	صبغي أب 2

تبديل القسم الأيمن من الصبغي الأول مع القسم الأيمن من الصبغي الثاني كما في الجدول 3.6. الذي يوضح طريقة التبديل والصبغيات الجديدة التي حصلنا عليها.

الجدول 3.6. الصبغيين الأبناء الجديدين حسب طريقة التقاطع الأولى.

01010000	صبغي أب 1
11110101	صبغي أب 2

بالطبع يمكن اختيار التجزئة بالعدد الذي نرغب به وتبديل الأجزاء التي تتناسبنا. الطريقة الثانية للتقاطع وهي اختيار عدد عشوائي $k \in [1, L]$ ، ثم القيام بتبديل المواقع التي تقع ضمن المجال $[k, k + a]$ حيث a عدد طبيعي يحقق أن $k < a$ و $k + a, a \in [1, L]$. مثلاً باختيار الأعداد $a = 3$ و $k = 2$ عندها المجال الذي سوف نقوم بتبديله هو $[2, 5]$ (أي من المحرف الثاني إلى المحرف الخامس) كما يوضح الجدول 4.6. الذي يحوي الصبغيين المستخدمين في الطريقة السابقة.

الجدول 4.6. تقسيم الصبغيين الآباء بطريقة التقاطع الثانية.

01010101	صبغي أب 1
11110000	صبغي أب 2

بتبديل الأقسام في المجال المحدد في الجدول 4.6. نحصل على صبغيين جديدين كما في الجدول 5.6.

الجدول 5.6. الصبغيين الأبناء الجديدين حسب طريقة التقاطع الثانية.

01110101	صبغي أب 1
11010000	صبغي أب 2

ثالثاً الطفرة (Mutation): نضيف قيمة جديدة عشوائية نسميها طفرة. تتم هذه الخطوة باستبدال خانة ما من صبغيات الأبناء بهذه الطفرة. هدف إحداث طفرة هو تأمين التنوع في الصبغيات مما يتيح الفرصة للوصول لقيم أفضل. من الأمثلة على الطفرة مثلاً تبديل الخانة الرابعة بالقيمة المعاكسة (استبدال 1 بـ 0 والعكس صحيح). من الممكن توليد قيمة عشوائية بحسب نظام العد المستخدم واستبدال أحد الخانات به.

استبدال المجموعة القديمة بالمجموعة الجديدة: ليكن عدد الصبغيات n وعدد الآباء m يجب أن يتم توليد عدد من الأبناء بمقدار $t=n-m$. بجمع كلاً من الصبغيات الآباء والأبناء معاً ووضعهم عوضاً عن الصبغيات القديمة نحصل على مجموعة جديدة من الصبغيات تسمى جيل (Generation).

التكرار من الخطوة الثانية: بعد أن يصبح لدينا مجموعة جديدة من الصبغيات نحسب كفاءة كل صبغي جديد ثم نقوم باختيار الصبغيات الأفضل كأباء، ثم إجراء التزاوج والطفرة بينها لتوليد مجموعة جديدة. مع تكرار هذه العملية نحصل على عدد من الأجيال حتى الوصول لشرط التوقف. شرط التوقف يُحدد إما عدم الحصول على نتائج جديدة في الحل أو عند الوصول للعدد الأعظمي للأجيال الذي يحدد في بداية المسألة.

3.6. مجموعة البيانات (Dataset) [21]

مجموعة البيانات المختارة هي مجموعة التهديدات الداخلية الاصطناعية المعروفة بـ CERT وهي اختصاراً لـ (Computer Emergency Response Team). لها عدة إصدارات والإصدار المستخدم في دراستنا هو r4.2 وهو الإصدار الأكثر شيوعاً. تتكون المجموعة في هذا الإصدار من عدة ملفات. يحوي كل ملف عدد من السجلات. تتضمن المجموعة 1000 مستخدم أما عدد السجلات الإجمالي فهو 32,770,227، من بينهم 7,323 حدثاً خبيثاً تم حقنه. أما الأنشطة التي تخزن في كل ملف فقد كانت على مدار 502 يوماً ومن الملفات نذكر: logon.csv: يحوي على بيانات حول تسجيلات الدخول والخروج للمستخدمين. device.csv: يحوي على بيانات حول الأجهزة المستخدمة في الشبكة. http.csv: يحوي على بيانات حول النشاطات الخاصة بالبروتوكولات المرتبطة بالشبكة. file.csv: يحوي على بيانات حول الوصول للملفات والأنشطة المتعلقة بها. psychometric.csv: يحوي على بيانات نفسية للمستخدمين.

البيانات الحقيقية التي تشابه هذه البيانات تُحفظ في سجلات الخادم وتُجمع عند قيام المستخدم بالأنشطة المختلفة. بداية يتم جمع البيانات عند طبقة التطبيقات وترسل عبر طبقة النقل بالخادم وفق بروتوكولات محددة وتدار الجلسة أثناء تفاعل المستخدم مع الخدمة من خلال طبقة الخدمة (راجع النموذج OSI في الفصل الثالث).

4.6. النموذج المقترح (Proposed Model)

على الرغم من وجود العديد من الدراسات السابقة التي استخدمت خوارزميات الذكاء الصناعي (مثل الشبكات العصبية) في تقنية الـ UBA، إلا أن أغلبها واجهت تحدياً جوهرياً يتمثل في عدم توازن البيانات، مما أثر سلباً على دقة الكشف عن الشذوذ في هذه النماذج. انطلاقاً من هذه الفجوة، نقدم في هذه الدراسة نموذجاً هجيناً يسمى GGRU وهو اختصاراً لـ Genetic Gated Recurrent Unit أي الوحدة متكررة البوابة الجينية. يعتمد

نموذجنا على بنية الـ GRU (راجع الفصل الخامس) المُحسنة باستخدام الـ GA على عكس النماذج التقليدية. يهدف هذا النهج إلى تجاوز القيود التقليدية وتحقيق توازن بين الكشف الحقيقي والإنذارات الكاذبة، وهو ما لم تتجح فيه العديد من النماذج السابقة. النموذج الذي قمنا باقتراحه لا يعتمد على بيانات مصنفة مسبقاً وإنما يتعلم السلوك الطبيعي عن طريق إعادة بناء المدخلات (Inputs Reconstruction). بما أن البيانات غير مصنفة، فإنه يمكن تطبيق نموذجنا المقترح على بيانات فعلية كون البيانات في الواقع لا تكون مصنفة مسبقاً. بعد تعلم الأنماط الطبيعية يتم اكتشاف الانحرافات بناءً على خطأ الإعادة وهذا ما سوف يمثل الخط الأساسي (راجع الفصل الرابع). قمنا بتطبيق النموذج المقترح على ملف logon.csv وبرمجته باستخدام لغة البرمجة Python وعدة مكتبات Numpy, Pandas, Tensorflow, Keras, Pygad, Sklearn, Matplotlib, Datetime, Seabron ومحرر الأكواد Visual Studio Code (انظر إلى الملحق). قسمنا العمل إلى 5 مراحل وهي:

✍ **المرحلة الأولى:** معالجة البيانات لاستخراج الميزات.

✍ **المرحلة الثانية:** تحويل البيانات الفئوية وتطبيع كامل البيانات ضمن المجال [0,1]، ثم تقسيم البيانات لبيانات تدريب وبيانات اختبار.

✍ **المرحلة الثالثة:** بناء الشبكة وتدريب النموذج باستخدام بيانات التدريب لتعلم السلوك الطبيعي للمستخدم.

يتم في هذه المرحلة استخدام الـ GA لتحديث الأوزان عوضاً عن طريقة الاشتقاق (راجع الفصل الخامس).

✍ **المرحلة الرابعة:** اختبار النموذج على بيانات الاختبار واكتشاف الشذوذ بتصنيف البيانات بطريقتين.

✍ **المرحلة الخامسة:** التقييم النهائي للنموذج من أجل قياس فعاليته.

لنناقش المراحل الخمس بشكل مفصل في الفقرات الآتية:

المرحلة الأولى: الملف المستخدم يحوي 854,860 سجلاً و5 أعمدة. البيانات غير مصنفة بمعنى لا يوجد عمود يحوي معلومة عن السجل في حال كان يمثل سلوكاً طبيعياً أم لا. الميزات كما يلي:

معرف السجل (id) والتاريخ (date) ومعرف المستخدم (user) ومعرف الجهاز (pc) والنشاط (activity).

يوضح الجدول 6.6 جزء من الملف المستخدم والبيانات الموجودة.

الجدول 6.6. البيانات المستخدمة في النموذج المقترح من ملف logon.csv.

Index	Id	Date	User	Pc	Activity
1	{X1D9-S0ES98JV-5357PWMI}	02/01/2010 06:49:00	NGF0157	PC-6056	Logon
2	{G2B3-L6EJ61GT-2222RKSO}	02/01/2010 06:50:00	LRR0148	PC-4275	Logon
:					
854,860	{T0U1-P7DT83QQ-7295ICZR}	17/05/2011 06:43:35	BJM0111	PC-6866	Logoff

اخترنا "user" و "pc" كميزات أساسية وتجاهلنا "id" كونها تتعلق بالسجل وليس المستخدم. بالإضافة إلى ذلك، استخرجنا ميزات إضافية مثل مدة الجلسة (duration) ووقت تسجيل الخروج (logofftime) ووقت تسجيل الدخول (logontime) واليوم من الأسبوع (weekday) مما يعني أنه لدينا 6 ميزات. حسبنا مدة الجلسة وفقاً للسجلات التي تحوي تسجيل دخول من خلال البحث عن الكلمة Logon لكل مستخدم تبعاً لـ "user" و "pc" وحفظنا النتائج. ثم حددنا السجل الخاص بتسجيل الخروج من خلال البحث عن الكلمة Logoff، بحيث يكون تسجيل الخروج هذا مقابل لسجل تسجيل دخول سابق. بعد ذلك حسبنا الفرق بين موعد تسجيل الدخول والخروج وفقاً للأوقات والتواريخ الخاصة بهذا المستخدم. عيّنا اليوم الخاص بالنشاط المذكور سابقاً وحفظنا النتيجة في ملف processed_logon.csv. مع تكرار هذه العملية استخرجنا الميزات المطلوبة في ملف يحوي على 384,251 سجل وهي الميزات الآتية: معرف المستخدم "User"، معرف الجهاز "Pc"، مدة الجلسة "Duration"، اليوم من الأسبوع "Weekday"، وقت تسجيل الدخول "Logontime" وكذلك وقت تسجيل الخروج "Logofftime".

الجدول 7.6. يوضح بيانات الملف المذكور سابقاً.

الجدول 7.6. ملف البيانات بعد استخراج الميزات وهو ملف processed_logon.csv.

Index	User	Pc	Logontime	Logofftime	Duration	Weekday
1	LRR0148	PC-4124	02/01/2010 06:53:04	02/01/2010 07:24:53	0.53027777	Saturday
2	NOB0181	PC-4124	02/01/2010 07:40:42	02/01/2010 07:46:55	0.10361111	Saturday
:						
384,251	BJM0111	PC-6866	17/05/2011 03:09:35	17/05/2011 06:43:35	3.56666666	Tuesday

المرحلة الثانية: حولنا أوقات تسجيل الدخول والخروج الخاصة بـ "Logontime" و "Logofftime" إلى قيم بالثواني. حسبنا الوقت على شكل ثنائي وذلك بالبداية بالزمن 00:00:00 من بداية اليوم. فعلى سبيل المثال باعتبار اليوم يبدأ بتوقيت 00:00:00 بمنتصف الليل فعندها تكون الساعة 2:00:00 بعد منتصف الليل هي بمقدار ساعتين من بداية اليوم وتتمثل بالقيمة $2 \times 3600 = 7200$ ثانية. التحويل يعتمد على القانون:

$$(1.6) \dots \text{Total seconds} = \text{seconds} + (60 \times \text{minute}) + (3600 \times \text{hour})$$

بعد تحويل الأوقات لثنائي قسمنا البيانات بحسب الميزات لقسمين: القسم الأول يحوي البيانات ذات القيم العددية مثل "Logontime" و "Logofftime" و "Duration" والقسم الثاني يتضمن البيانات الفئوية والتي يمكن فصلها لفئات مثل "User" و "Pc" و "Weekday". بعد التقسيم طبعنا البيانات الخاصة بالقسم الأول لتكون مناسبة للدخول إلى الشبكة وذلك باستخدام طريقة Min-Max-Scaling والتي تعطى بالقانون (2.6):

$$p'_j = \frac{p_j - \min(p_j)}{\max(p_j) - \min(p_j)} \dots \dots (2.6)$$

تمثل p_j نشاط المستخدم مثل LRR0148 الموجودة في السطر الأول من الجدول 7.6، p'_j فهي القيمة الجديدة لهذا النشاط. أما $\min(p_j)$ فهي أصغر قيمة في العمود التي تتواجد به p_j والقيمة $\max(p_j)$ هي أكبر قيمة في ذلك العمود. القسم الثاني الخاص بالبيانات الفئوية حولناها بالتمثيل العددي باستخدام Label Encoder. الجدول 8.6. يوضح تطبيق التحويل السابق على أيام الأسبوع.

الجدول 8.6. مثال لتحويل البيانات الفئوية إلى قيم عددية.

Wednesday	Tuesday	Thursday	Sunday	Saturday	Monday	Friday	اليوم
6	5	4	3	2	1	0	التحويل

يظهر الجدول 8.6. أنه يتم ترتيب البيانات بحسب الترتيب الأبجدي للأحرف ومن ثم مقابلتها مع مجموعة الأعداد الطبيعية. بعد أن تصبح البيانات الفئوية بالشكل العددي، يتم تطبيق التطبيع عليها وفق المعادلة (2.6) وبهذا تصبح كل البيانات ضمن المجال $[0,1]$. بما أن البيانات مقسمة فلابد من دمج الأعمدة بعد عملية التطبيع وذلك وفق الترتيب الأصلي اعتماداً على الـ index. حفظنا النتائج في ملف normalized_logon.csv والجدول 9.6. يوضح شكل البيانات بعد التطبيع المحفوظة في الملف الأخير.

الجدول 9.6. ملف البيانات بعد التطبيع وهو ملف normalized_logon.csv.

index	User	Pc	Logontime	Logofftime	Duration	Weekday
1	0.620620	0.409181	0.286855	0.308913	0.385833	0.333333
2	0.725725	0.409181	0.319934	0.324218	0.007490	0.333333
⋮						
384,251	0.113113	0.684630	0.131656	0.280225	0.259874	0.833333

بعد التطبيع قسمنا البيانات بنسبة 70% للتدريب و30% للاختبار مع الاحتفاظ بالترتيب نفسه وحفظناها في ملفين. بهدف جعل البيانات مناسبة للاستخدام في شبكة الـ GRU عدلنا الملفين السابقين لتصبح البيانات على شكل الثلاثية [Samples, Timesteps, Features]، حيث أن Samples هو عدد السجلات الخاص بكل ملف و Timesteps تعني الخطوة الزمنية (سنعتبرها هنا سجل سجل) أما Features فهي الميزات وعددها 6. حفظنا النتائج في ملفين، ملف لبيانات التدريب train_data.npy أبعاده هي [6, 1, 268, 975] وملف لبيانات الاختبار test_data.npy أبعاده هي [6, 1, 155, 276] وهي أبعاد مناسبة للشبكات التي تهتم بالتسلسلات الزمنية.

المرحلة الثالثة: استخدمنا ملف `train_data.npy` لتدريب الشبكة العصبية الـ GRU التي بُنيت باستخدام مكتبة Keras. بنينا الشبكة باستخدام الطبقات الآتية:

طبقة GRU أولى: التي تحوي على طبقة المدخلات ضمناً مع 24 خلية وتم البدء بهذه الطبقة وذلك لتعلم الأنماط الزمنية الأكثر تعقيداً. تم إخراج النتائج منها وفق مبدأ إرجاع التسلسل بالشكل الثلاثي. دالة التنغيع المستخدمة في الحساب هي دالة $Tanh(x)$.

طبقة GRU ثانية: وتمثل أول طبقة خفية وتحوي 12 خلية. تتعلم الأنماط الزمنية مع تخفيف التمثيل للحصول على نتائج مركزة. لا تعيد إرجاع التسلسل فتعطي الناتج بشكل ثنائي الأبعاد بحيث لا تعد الخطوة الزمنية ضمن الأبعاد. كوننا لن نستخدم طبقات الـ GRU في الطبقات التالية فلا داعي لإرجاع التسلسل أما لو استخدمنا طبقات الـ GRU في الطبقات التالية فكان لا بد من الشكل الثلاثي للأبعاد، ودالة التنغيع هي $Tanh(x)$.

طبقة Dense أولى: وتمثل الطبقة الخفية الثانية وتحوي 8 خلايا. تحول مخرجات الطبقة السابقة بشكل مناسب أي تقلل الأبعاد لتصبح أقرب للخروج النهائي. بالطبع تتعلم الأنماط غير الخطية، ودالة التنغيع هي $Tanh(x)$.
طبقة Dense ثانية: وتمثل الطبقة الخفية الثالثة وتحوي 6 خلايا. تقلل الأبعاد لتسهيل الانتقال للخروج النهائي للشبكة. بالطبع تتعلم الأنماط غير الخطية كما تفعل سابقتها، ودالة التنغيع هي $Tanh(x)$.

طبقة Dense ثالثة: وتمثل الطبقة المخرجات وتحوي 6 خلايا تتوافق مع عدد المخرجات النهائية، بحيث أن هذه الطبقة تعطي نسخة مُعاد بناؤها من المدخلات التي عددها 6. بهذا تعمل الشبكة كمشفّر تلقائي. أما دالة التنغيع المستخدمة في هذه الطبقة الأخيرة فهي $\sigma(x)$.

بالطبع هدف الشبكة هو تعلم الأنماط التي تمثل السلوك الطبيعي للمستخدم. عوضاً عن المسار الخلفي لتحديث الأوزان استخدمنا الـ GA والتي تتبع القيم الآتية:

التعداد السكاني الابتدائي: يتم توليد مجموعة الأوزان الابتدائية¹ كفرد من أفراد التعداد وذلك بشكل عشوائي. حددنا 8 مجموعات من الأوزان الابتدائية وهذا ما يمثل عدد الحلول المقترحة.

عدد الأباء للتراوح: اخترنا 4 أفراد من أصل 8 الذي يمثل العدد الكلي لأفراد التعداد.

السماح بتكرار الأوزان: اعتمدنا على شرط عدم السماح بتكرار الأوزان وذلك لضمان التنوع.

تقييم اللياقة لكل فرد: قيمنا بتقييم كل فرد بناءً على دالة اللياقة لقياس جودته بإعادة البناء. حسبنا النتائج الخاصة بالشبكة بحسب الفرد ومن ثم حسبنا قيمة الخطأ لكل سجل. اعتمدنا معادلة متوسط الخطأ التربيعي MSE لكونها أفضل من MAE في حساب الخطأ وذلك لحساسيتها للقيم المتطرفة. تعطى معادلة MSE بالعلاقة (3.6):

1 مجموعة الأوزان: هي الأوزان والانحيازات لكامل الشبكة من طبقة المدخلات حتى طبقة المخرجات، وتعتبر فرد واحد من التعداد السكاني.

$$E_j = \frac{1}{N} \sum_{i=1}^N (x_{ij} - \hat{x}_{ij})^2 \quad \dots \dots (3.6)$$

حيث x_i هو المدخل أما $\hat{x}_i$ فهو إعادة البناء و N عدد الميزات. أما E_j فيمثل قيمة خطأ السجل الذي رقمه j . بعد ذلك قمنا بحساب المتوسط الحسابي لقيم أخطاء السجلات ككل. هذا المتوسط يعبر عن قيمة الخطأ للفرد الذي يمثل قيمة لياقة الفرد ويحسب بالقانون الآتي:

$$E = \frac{1}{M} \sum_{j=1}^M E_j \quad \dots \dots (4.6)$$

حيث M هو العدد الكلي للسجلات. مع تقليل هذه E يتعلم النموذج توقع السلوك الطبيعي. الاختيار: في هذه المرحلة يتم اختيار الأفراد الأفضل (أولئك الذين لديهم أقل قيمة لـ E) الذين يمثلون الآباء. التقاطع: تم دمج الأوزان من الآباء لإنتاج أفراد جديدة تمثل الأبناء وهذا ما يشبه مبدأ التزاوج. يتم ذلك وفق القانون:

$$W_{new} = \alpha W_{parint1} + (1 - \alpha) W_{parint2} \quad \dots \dots (5.6)$$

حيث α هو معامل التزاوج وقيمته تتراوح بين 0 و 1 ولكنها تُحدد ضمناً أثناء البرمجة. الطفرة: تم تطبيق تعديلات عشوائية على الأبناء لإدخال تنوع في الأجيال التالية. عدد الأفراد التي سوف يتم تطبيق الطفرة عليهم حدد بالنسبة 5% من الأفراد. أما الطفرة فتحدث بحسب القانون (6.6):

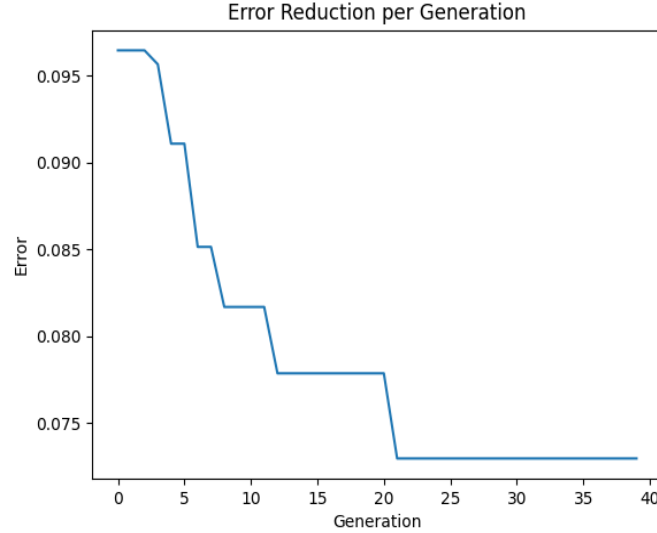
$$W_{mutation} = W + \Delta W \quad \dots \dots (6.6)$$

حيث ΔW هو معامل الطفرة وقيمته تتراوح بين 0 و 1 ولكنها تُحدد ضمناً أثناء البرمجة كما هو الحال مع معامل التزاوج. أما W فيمثل الفرد الذي سوف تُطبق الطفرة عليه.

بعد ذلك تم تحديث المجموعة الأولية كلها ليصبح لدينا مجموعة جديدة من الأفراد عددها 8. المجموعة الجديدة تمثل الجيل الجديد ومكونة من الآباء المختارين والأبناء بعد إجراء الطفرات. يتم حساب قيمة اللياقة للأبناء واسترجاع قيم اللياقة للآباء التي تحفظ مع كل عملية حساب. يتم اختيار أفضل قيمة لـ E من بين قيم E لكل أفراد هذا الجيل الجديد والتي تمثل قيمة الخطأ النهائية للجيل ككل. يتم الاحتفاظ بقيمة الخطأ النهائية بهدف تقليلها بكل جيل.

الإنهاء: تستمر الخوارزمية في التكرار حتى يتم الوصول إلى الحد الأقصى لعدد الأجيال الذي تم تحديده بـ 40 جيل. بالطبع يتم طباعة القيم النهائية لأفضل خطأ في كل جيل. الشكل 1.6. يوضح قيم الأخطاء الخاصة بالأجيال بعد إتمام كامل الخوارزمية.

نلاحظ من الشكل 1.6. التحسن الكبير في قيمة E واستقرار الشبكة المتمثل بالخط المستقيم. القيمة الأخيرة كانت 0.072 تقريباً والتي تدل على أن النموذج تدرب بشكل جيد. بالطبع استخرجنا الحل الأفضل (الفرد صاحب القيمة $E = 0.072$) وحفظناه مع النموذج في ملف `gru_model_genetic.keras` وذلك لاستخدامه في المرحلة التالية وهي اختبار النموذج والتتصيف.



الشكل 1.6. قيم الأخطاء عبر الأجيال بعد إتمام عملية التدريب مع 40 جيل.

المرحلة الرابعة: بعد تدريب النموذج حملنا النموذج المحفوظ في الملف `gru_model_genetic.keras` وبيانات الاختبار من الملف `test_data.npy`. حسبنا أخطاء إعادة البناء للسجلات الجديدة ومن ثم صنفنا السجلات بطريقتين وذلك لعدم وجود تصنيفات فعلية. التصنيف باعتماد قيمة الخطأ فقط: تم التصنيف الأولي للسجلات استناداً إلى قيمة الخطأ المحسوب. إذا كان خطأ الإعادة أكبر من β يتم تصنيف السجل على أنه شاذ (1). إذا كان الخطأ أصغر يتم اعتبار السجل طبيعياً (0). حيث يتم التصنيف الأولي وفق التابع (7.6):

$$f(x_j) = \begin{cases} Anomaly(1) & \text{if } E_j \geq \beta \\ Normal(0) & \text{otherwise} \end{cases} \dots (7.6)$$

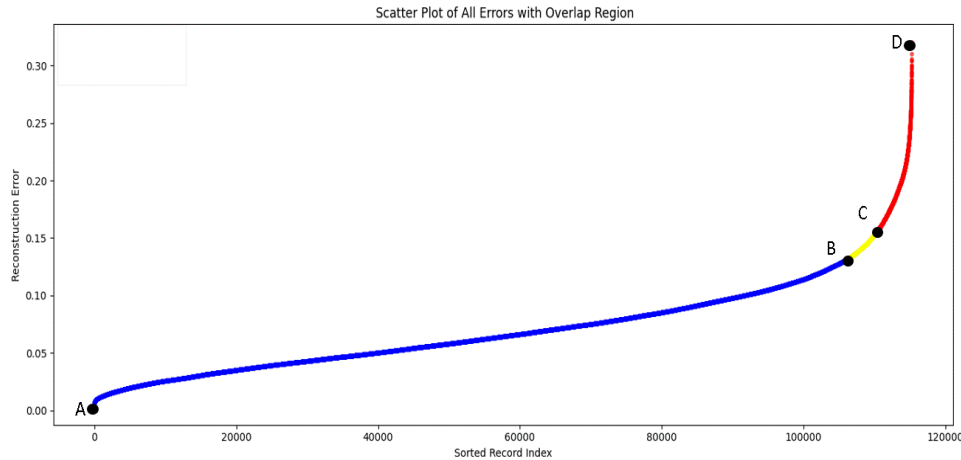
حيث β هي مجموع المتوسط الحسابي وضعفي الانحراف المعياري لقيم الأخطاء للسجلات جميعها و x_i هو السجل المراد تصنيفه. أما E_i فهو قيمة الخطأ لإعادة بناء هذا السجل. استناداً إلى هذه التصنيفات الأولية، حفظنا النتائج في ملف `initial_test_result.csv`. الملف هو عبارة عن جدول يحوي عمودين أحدهما قيمة الخطأ الخاصة بالسجل والثاني التصنيف الابتدائي 0 أو 1.

التصنيف باعتماد قيمة الخطأ والعتبة: حددنا عتبة (Threshold) بحسب النسبة المئوية (95%) التي بلغت قيمتها 0.15 تقريباً. قارنّا الأخطاء المحسوبة مع هذه العتبة لتصنيف السجلات النهائية. إذا تجاوز الخطأ العتبة (0.15) يتم تصنيف السجل على أنه شاذ، بينما يتم تصنيف السجلات الأخرى على أنها طبيعية. التصنيف النهائي وفقاً للتابع (8.6):

$$f(x_j) = \begin{cases} Anomaly(1) & \text{if } E_j \geq Threshold \\ Normal(0) & \text{otherwise} \end{cases} \dots (8.6)$$

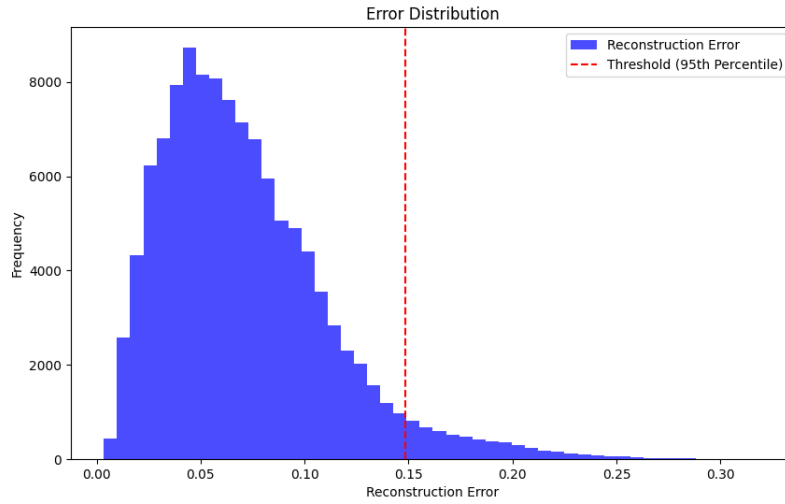
أخيراً، حفظنا النتائج بعد مقارنة الأخطاء بالعتبة المحددة في ملف final_test_result.csv. هذا الملف يحوي عمودين أيضاً قيمة الخطأ والتصنيف النهائي لكل سجل.

الشكل 2.6. يوضح الرسم البياني لتوزيع الأخطاء الطبيعية والشاذة. نلاحظ من الشكل 2.6. أن جزء المنحني من النقطة A إلى النقطة B يمثل توزيع الأخطاء الطبيعية، من النقطة C إلى النقطة D يمثل توزيع الأخطاء الشاذة. أما النقط بين النقطة B والنقطة C فتمثل منطقة التداخل. النقاط الخاصة بالسلوك الطبيعي ذات العدد الأكبر وهو أمر جيد كون السجلات الطبيعية أكثر وأنه صنف معظم السجلات الطبيعية بشكل جيد. وجود تداخل بسيط بين الفئتين يعني أن النموذج قادر على الفصل بين الطبيعي وغير الطبيعي بشكل جيد، كما أن النموذج فعال ولكن بتحديد أفضل للعتبة يصبح التداخل أقل.



الشكل 2.6. رسم توزيع الأخطاء الطبيعية والشاذة.

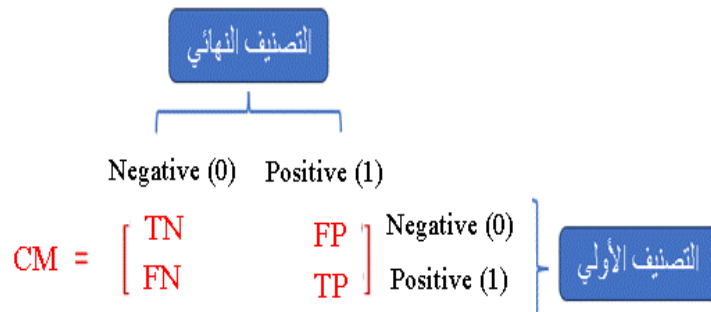
الشكل 3.6. يبين توزيع كامل الأخطاء بالاعتماد على مبدأ الأعمدة مع بيان عدد السجلات التي تحمل قيمة الخطأ نفسها. الخط المنقط يوضح العتبة التي تفصل بين السجلات الطبيعية على اليسار والشاذة على اليمين.



الشكل 3.6. رسم توزيع الأخطاء لكل السجلات معاً مع تمثيل لقيمة العتبة.

نلاحظ من الشكل 3.6. تزايد ارتفاعات الأعمدة اليسارية والتي تقع خلف العتبة وهو أمر جيد كونها تمثل السجلات الطبيعية التي عددها أكبر ما يمكن. أما ارتفاعات الأعمدة اليمينية والتي تقع بعد العتبة فهي منخفضة وهذا أمر طبيعي. بالرغم من وجود ذيل طويل نسبياً من اليمين، إلا أنه غير كثيف فهو أمر مقبول. مما سبق نجد أن النموذج قادر على تمييز الشذوذ وكشفه ولكنه يعاني من كشف بعض الحالات الشاذة التي يصعب تمييزها.

المرحلة الخامسة: قيمنا النموذج بشكل شامل بناءً على النتائج التي حصلنا عليها في التصنيفين الأولي والنهائي. حسبنا مصفوفة الارتباك (Confusion Matrix) الموضحة بالشكل 4.6. والتي تُحسب عادةً بين التصنيف الحقيقي والتصنيف بناءً على العتبة [15]. القيمة 0 (أي السجل طبيعي) تعتبر قيمة سلبية أما 1 (أي السجل شاذ) تعتبر قيمة إيجابية.



الشكل 4.6. مصفوفة الارتباك.

TN (True Negative): تمثل السلبي الصحيح. أي أن السجل تم تصنيفه بالتصنيف الأولي والتصنيف النهائي على أنه نشاط طبيعي. بالتالي تم تصنيف السجل على أنه طبيعي وهو فعلاً طبيعي.

(False Positive) FP: تمثل الإيجابي الخاطئ. بمعنى أن السجل تم تصنيفه بالتصنيف الأولي على أنه طبيعي أما بالتصنيف النهائي على أنه شاذ. بالتالي تم تصنيف السجل على أنه شاذ وهو في الحقيقة طبيعي.

(False Negative) FN: تمثل السلبي الخاطئ. أي أن السجل تم تصنيفه بالتصنيف الأولي على أنه شاذ أما بالتصنيف النهائي على أنه طبيعي. بالتالي تم تصنيف السجل على أنه طبيعي وهو في الحقيقة شاذ.

(True Positive) TP: تمثل الإيجابي الصحيح. بمعنى أن السجل تم تصنيفه بالتصنيف الأولي والتصنيف النهائي على أنه نشاط شاذ. بالتالي تم تصنيف السجل على أنه شاذ وهو فعلاً شاذ.

بعد حساب المصفوفة قمنا بتعيين كلاً من المقاييس الآتية، وذلك باعتبار التصنيف الأولي هو التصنيف الفعلي أما التصنيف النهائي هو تصنيف الشبكة [15]:

(1) الدقة (Precision): وهي نسبة الحالات التي صُنفت بشكل صحيح على أنها شاذة (طبيعية) من أصل كل الحالات التي تم تصنيفها على أنها شاذة (طبيعية).

تعطى علاقة التصنيف الصحيح للحالات الشاذة من أصل كل الحالات المصنفة على أنها شاذة:

$$Precision = \frac{TP}{TP+FP} \quad (9.6)$$

تعطى علاقة التصنيف الصحيح للحالات الطبيعية من أصل كل الحالات المصنفة على أنها طبيعية:

$$Precision = \frac{TN}{TN+FN} \quad (10.6)$$

(2) الاسترجاع (Recall): وهي نسبة الحالات التي صُنفت بشكل صحيح على أنها شاذة (طبيعية) من أصل كل الحالات التي هي فعلاً شاذة (طبيعية).

(3) تعطى علاقة دقة تصنيف الحالات الشاذة من أصل كل الحالات التي هي فعلاً شاذة:

$$Recall = \frac{TP}{TP+FN} \quad (11.6)$$

تعطى علاقة دقة تصنيف الحالات الطبيعية من أصل كل الحالات التي هي فعلاً طبيعية:

$$Recall = \frac{TN}{TN+FP} \quad (12.6)$$

(4) متوسط التوافق بين الدقة والاسترجاع (F1-Score): وهو مقياس التوازن بين الدقة والاسترجاع. تعطى علاقة دقة تصنيف الحالات الشاذة:

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (13.6)$$

(5) الدقة العامة (Accuracy): وهي نسبة الحالات التي صنفنا بشكل صحيح على أنها شاذة وطبيعية من أصل كل الحالات التي تم تصنيفها. تعطى علاقة الدقة العامة بالشكل:

$$Accuracy = \frac{TN+TP}{TN+TP+FP+FN} \quad (14.6)$$

(6) معدل الإيجابي الخاطئ (False Positive Rate): أو اختصاراً FPR وتعطى بالعلاقة:

$$Precision = \frac{FP}{TN+FP} \quad (15.6)$$

(7) معدل الإيجابي الصحيح (True Positive Rate): أو اختصاراً TPR وتعطى بالعلاقة:

$$Precision = \frac{TP}{FN+FP} \quad (16.6)$$

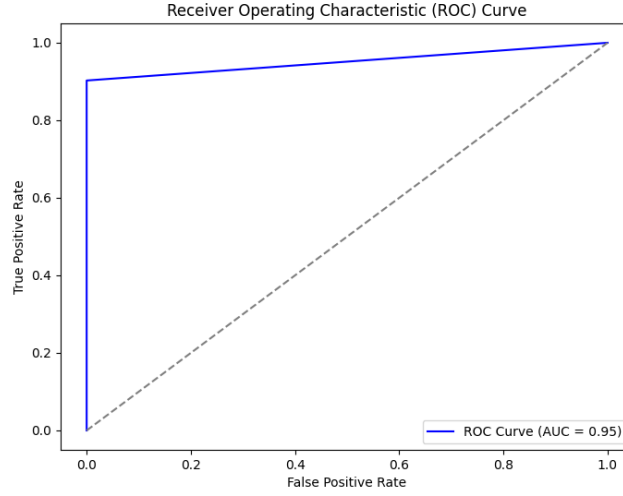
لرسم كل من المنحني (Receiver Operating Characteristic, ROC) ومساحة تحت المنحني (Area Under the Curve, AUC) نعتمد على المعدلين FPR و TPR السابقين بحيث TPR المحور العمودي و FPR المحور الأفقي. كلما كانت قيمة الـ AUC أقرب إلى 1 يكون النموذج أفضل. في الفقرة التالية سوف نستعرض القيم المحسوبة من التقييمات السابقة مع تحليلها تحليلاً دقيقاً للتحقق من قدرة وكفاءة النموذج الذي قمنا باقتراحه.

5.5. النتائج

كما ذكرنا سابقاً فقد صممنا نموذجاً هجيناً يهدف لحل مشكلة عدم التوازن وضعف كشف الشذوذ. فيما يلي سنقوم بتحليل النتائج التي حصلنا عليها بعد اختبار نموذجنا المقترح وتقييمه النهائي والشامل بناءً على المقاييس المبينة في الجدول 10.6. والمنحني ROC وقيمة الـ AUC في الشكل 5.6.

الجدول 10.6. قيم التقييمات النهائية للنموذج المقترح.

	precision	recall	f1-score
0	1.00	0.99	1.00
1	0.90	1.00	0.95
accuracy			1.00
macro avg	0.95	1.00	0.97
weighted avg	1.00	1.00	1.00



الشكل 5.6. منحنى ROC وقيمة الـ AUC.

تحليل قيم كلاً من الدقة والاسترجاع وF1 عند الفئات

بما أن النموذج تعلم السلوك الطبيعي (الفئة 0) ثم حاول كشف السلوك الشاذ (الفئة 1)، فإن هذه المقاييس تعطي لنا فكرة عن دقة الكشف عن الشذوذ ومدى فعالية النموذج في تقليل الأخطاء.

• فئة 0 (السلوك الطبيعي):

- الدقة (1.00): هذا يعني أن السجلات جميعها التي تم تصنيفها كسلوك طبيعي كانت فعلاً سلوكاً طبيعياً. النموذج دقيق جداً في تصنيف السلوك الطبيعي ولا يخطئ في هذا الصدد.
- الاسترجاع (0.99): هذا يعني أن النموذج اكتشف 99% من السجلات الطبيعية جميعها بشكل صحيح. هناك 1% من السجلات الطبيعية تم تصنيفها كشاذة (إنذارات خاطئة). لذلك يبقى هناك مجال لتحسين اكتشاف السلوك الطبيعي.

- درجة F1 (1.00): تمثل درجة F1 توازناً ممتازاً بين الدقة والاسترجاع في فئة السلوك الطبيعي.

• فئة 1 (السلوك الشاذ):

- الدقة (0.90): تعني هذه القيمة أن 90% من السجلات التي صنفها النموذج كشاذة كانت فعلاً شاذة. هناك 10% من السجلات التي صنفها النموذج كشاذة لكنها كانت سلوكاً طبيعياً (إنذارات خاطئة). إذاً النموذج بحاجة لتحسين قدرته على تحديد السلوك الشاذ بدقة أكبر.

○ الاسترجاع (1.00): هذه القيمة تشير إلى أن النموذج اكتشف السجلات الشاذة جميعها بشكل صحيح. لا يوجد أي سجل شاذ تم تصنيفه بشكل خاطئ كطبيعي. هذا يعني أن النموذج نجح في اكتشاف الحالات الشاذة جميعها دون أن يفوت أي منها.

○ درجة F1 (0.95): درجة F1 لفئة السلوك الشاذ هي 95% وهي تمثل توازناً جيداً بين الدقة والاسترجاع. القيمة جيدة، ولكن هناك مجال لتحسين الدقة لتقليل الإنذارات الخاطئة التي يتم تصنيفها كشاذة.

الخلاصة (1) التحليل الأولي للنموذج المقترح بناءً على التقييمات عند فئة السلوك الشاذ والطبيعي:

- النموذج يحقق أداءً جيداً في كشف السلوك الشاذ، حيث أن الاسترجاع مرتفع جداً (1.00) مما يعني أنه يكتشف السلوكيات الشاذة جميعها. لكن الدقة (0.90) تشير إلى وجود بعض الإنذارات الخاطئة.
 - بالنسبة لـ السلوك الطبيعي، الدقة ممتازة (1.00) مما يعني أن النموذج لا يخطئ في تصنيف السلوك الطبيعي. لكن الاسترجاع (0.99) يشير إلى أن النموذج قد يفوت عدد قليل جداً من السجلات الطبيعية التي تم تصنيفها بشكل خاطئ كسجلات شاذة. عدد من الإنذارات الكاذبة تُشكل حاجة لتحسين أداء النموذج.
 - قيمة الـ FP مرتفعة قليلاً مما يجعل دقة كشف الشذوذ واسترجاع السلوك الطبيعي منخفضة. يعود ذلك إلى طريقة اختيار عتبة التصنيف أو تحسين ميزات البيانات وعدد الميزات الذي من الممكن زيادته قليلاً.
- 🔍 تحليل قيم كل من الدقة والاسترجاع والتوازن عموماً يجب أن نتعرف على ما يلي:

Macro Average (1)

- يتم حساب متوسط كل من التقييمات للفئات جميعها بالتساوي بغض النظر عن عدد العينات في كل فئة.
- مفيد عندما تكون الفئات متوازنة أو عندما تريد تقييم أداء النموذج لكل فئة بشكل منفصل.

Weighted Average (2)

- يأخذ بعين الاعتبار عدد العينات في كل فئة عند حساب المتوسط.
- إذا كانت هناك فئة ذات عدد عينات كبير فإن تأثيرها سيكون أكبر على القيم المحسوبة.

والآن أصبح بالإمكان تحليل القيم المتبقية كما يلي:

• Macro Avg Precision = 0.95 (الدقة المتوسطة):

- يوضح أن النموذج بشكل عام دقيق بنسبة 95% عند تحديد سجل ما بناءً بأنه ينتمي إلى فئة معينة.
- يوجد أخطاء بالتصنيف بسبب قيمة الـ FP المرتفعة.

• Weighted Avg Precision = 1.00 (الدقة الموزونة):

- الدقة هنا مرتفعة لأن الفئة 0 (السلوك الطبيعي) لديها عدد عينات أكبر مما يؤثر على المتوسط.

○ يشير إلى أن معظم التوقعات التي قام بها النموذج صحيحة عند التعامل مع كل فئة مع مراعاة عدم التوازن.

• Macro Avg Recall = 1.00 (الاسترجاع المتوسط)

○ يوضح أن النموذج يستعيد 100% من الحالات الشاذة الفعلية. بمعنى أن النموذج جيد جداً في التقاط السلوكيات الشاذة على الرغم من عددها القليل.

• Weighted Avg Recall = 1.00 (الاسترجاع الموزون)

○ يأخذ بعين الاعتبار التوزيع غير المتوازن للفئات. تم تعديله حسب توزيع الفئات.
○ قيمته المرتفعة تشير إلى أداء قوي للنموذج.

• Macro Avg F1-score = 0.90

○ هذا يعني أن النموذج يحقق توازناً جيداً بين الدقة والاسترجاع عند النظر إلى كل الفئات بالتساوي.
○ يشير إلى أن النموذج ليس منحازاً بشدة لإحدى الفئات.

• Weighted Avg F1-score = 0.97

○ نظراً لأن الفئة 0 تمثل معظم البيانات، فإن هذه القيمة تعكس الأداء العام للنموذج بناءً على توزيع البيانات.
○ ارتفاع هذه القيمة يشير إلى أن النموذج لديه توازن ممتاز لكنه قد يحتاج إلى تحسين الدقة للفئة الشاذة.

الخلاصة (2) التحليل النهائي وفقاً لقيم التقييمات عموماً:

- أداء مرتفع جداً في الاسترجاع (100%) مما يعني أن النموذج يكتشف معظم الحالات الشاذة.
- دقة ممتازة (95%) لكنها بحاجة للتحسين. الـ 5% المتبقية بسبب وجود بعض الإنذارات الكاذبة كونه يصنف بعض السجلات العادية على أنها شاذة.
- التوازن بين الدقة والاسترجاع (F1-score = 97%) ممتاز، مما يعني أن النموذج يعمل بكفاءة في تصنيف الفئتين. لا يوجد مشكلة مع عدم توازن البيانات ويظهر تصنيفاً فعالاً وأداء قوي جداً.
- أما بالنسبة للدقة العامة فكانت 100% وهي نسبة السجلات التي صنفها النموذج بشكل صحيح. قيمة الـ AUC بلغت 95% وهذا يعني أن النموذج قادر على تمييز الحالات الطبيعية والشاذة. على الرغم من أن النموذج يكتشف الشذوذ بشكل ممتاز، إلا أن تحسين الدقة قد يقلل من الإنذارات الخاطئة ويعزز موثوقية النموذج. مع ذلك قد استطعنا حل مشكلة عدم التوازن ولكن النموذج يحتاج لتحسين قيمة الـ FP.

كما ذكرنا سابقاً فقد قمنا بإجراء مقارنة بين نموذجنا المقترح وبعض النماذج المقترحة في هذا المجال. فقد قمنا بدايةً بمقارنة النموذج المقترح مع دراستين سابقتين تستخدم نوع الشبكة ذاتها في كشف الشذوذ (راجع الفصل الخامس). نوضح في الجدول 11.6 مقارنة بين النموذج ودراسيتين المختارتين:

الجدول 11.6. مقارنة بين النموذج المقترح ودراسيتين آخريتين.

المعيار	النموذج المقترح	الدراسة [11]	الدراسة [31]
الشبكة المستخدمة	GRU	GRU	GRU
تمثيل البيانات	التطبيع لتصبح البيانات ضمن نطاق 0 إلى 1 وذلك باستخدام طريقة Min-Max-Scaling	تحويل البيانات للتمثيل الرقمي بواسطة طريقة One-Hot-Vector	التطبيع لتصبح البيانات ضمن نطاق 0 إلى 1 وذلك باستخدام طريقة Statistical Max Model Scaling
دالة الخطأ	MSE	لم تحدد	MAE
طريقة التحسين والتدريب	GA مع 40 جيل	عدد دورات 20 فقط	Adam مع 100 دورة ومعدل التعلم 0.001
عتبة الشذوذ	محسوبة بالنسبة المئوية اعتماداً على توزيع الخطأ	غير محددة بشكل دقيق	تم اختبار عتبات مختلفة و 0.03 هي العتبة المثلى
الدقة	Accuracy = 1.00 Precision = 0.95	Accuracy = 0.92	Precision = 0.80
الاسترجاع	1.00	غير متوفرة	غير متوفرة
AUC	0.95	لم يتم ذكره	0.87
مشكلة مع عدم توازن البيانات	لا يوجد مشكلة حيث يتعامل مع الشذوذ بشكل جيد إلا أنه قيمة ال FP عالية قليلاً	يعاني من عدم توازن البيانات مما قلل قدرة النموذج على كشف الشذوذ بشكل دقيق	يعاني من عدم توازن البيانات مما قلل قدرة النموذج على كشف الشذوذ بشكل دقيق

بناءً على جدول المقارنة 11.6،، تمكنا من تحليل أفضلية النموذج المقترح اعتماداً على معايير محددة مثل الجودة والأداء مقارنة بالدراسات الأخرى. فيما يلي نبين التحليل الدقيق والشامل:

الدراسة [11]

- تمثيل البيانات: يعتمد على تنظيم السجلات إلى تسلسل استناداً إلى الأنشطة اليومية. لكن لا يوجد توضيح في حال تم تطبيع البيانات أم لا.

- خوارزمية التدريب والتحسين: لم يتم تحديد تفاصيل دقيقة حول الخوارزمية المستخدمة، لكن الاستفادة من الـ GRU يُظهر أن الطريقة فعّالة.
- الدقة العامة 0.92: أدنى من دقة النموذج المقترح، إلا أنه يعتبر أداءً متميزاً في تصنيف السلوك الشاذ.
- مشكلة عدم توازن البيانات: يوجد مشكلة مع عدم التوازن.

الدراسة [31]

- تمثيل البيانات: تعتمد على تجميع الأحداث اليومية لكل مستخدم وتطبيع البيانات بأقصى القيم الإحصائية. هذا يؤدي إلى بعض التحديات في تمثيل البيانات بدقة عند التعامل مع بيانات ذات توزيعات غير متوازنة.
- خوارزمية التدريب والتحسين: استخدام Adam مع معدل تعلم ثابت 0.001 قد يكون فعالاً، لكنه يفتقر إلى الابتكار في استخدام خوارزميات غير تقليدية.
- دالة الخطأ MAE: هي دالة خطأ متوازنة، لكنها قد تكون أقل ملاءمة من MSE في بعض الحالات التي تتطلب تمييزاً دقيقاً بين الأنشطة الشاذة.
- الدقة 0.80: تعتبر دقة جيدة، ولكنها أقل من الدقة في النموذج المقترح.
- AUC: 0.87 أقل من 0.90 في النموذج المقترح، مما يعني أن النموذج المقترح يعرض أداءً أفضل في التفريق بين الحالات الطبيعية والشاذة.
- مشكلة عدم توازن البيانات: يوجد مشكلة مع عدم التوازن.

النموذج الذي قمنا باقتراحه

- تمثيل البيانات: يستخدم حساب مدة الجلسة، اليوم والوقت بناءً على النشاط اليومي. يقوم بتطبيع البيانات لتكون موحدة باستخدام طريقة تقلل من التباين في البيانات وعدم التوازن.
- خوارزمية التدريب والتحسين: استخدام الـ GA لتحسين الأوزان يمكن أن يكون أكثر مرونة في إيجاد الحلول المثلى، كما أنه يضمن تحديث الأوزان بشكل مبتكر بعيداً عن تقنيات التحسين التقليدية.
- دالة الخطأ MSE: ملائمة لمهام تصنيف السلوك الطبيعي والشاذ بشكل دقيق.
- الدقة: تقدر الدقة بالقيمة 0.95 أما الدقة العامة فكانت 1.00، مما يشير إلى قدرة جيدة على تمييز الشذوذ.
- الاسترجاع: 1.00 يعكس قدرة عالية على اكتشاف الحالات الشاذة جميعها.
- AUC: 0.95 مما يدل على أن النموذج يعمل بشكل جيد في التمييز بين الأنشطة الطبيعية والشاذة.

التحليل النهائي للأفضلية والجودة العامة

- النموذج المقترح يقدم مزيجاً جيداً من الكفاءة في التدريب واكتشاف الشذوذ.
 - الدراسة [11] تعطي أداء أقل في الدقة من النموذج المقترح. لم تقدم توضيح لآلية عمل النموذج مما يجعل تحديد جودة النموذج صعبة. لكنها تعاني مع مشكلة عدم توازن البيانات.
 - الدراسة [31] تعتبر أقل كفاءة في النواحي جميعها مقارنةً مع النموذج المقترح. بالرغم من أنها قدمت صورة شاملة عن النموذج مقارنةً مع الدراسة [11]، ولكنها تعاني من مشكلة عدم التوازن في البيانات.
- أما بالمقارنة مع دراسات مختلفة بالتصميم أو البيانات عن نموذجنا المقترح فلنأخذ على سبيل المثال الدراسة [12] فهي تستخدم شبكة الـ LSTM عوضاً عن الشبكة الـ GRU. النموذج المقترح يتفوق على النموذج الثالث المصمم في الدراسة [12] والذي يستخدم عدد من الخلايا مقارب لما تم استخدامه في نموذجنا. نتائج النموذج الأول والثاني من الدراسة نفسها تتقارب مع النتائج التي حصلنا عليها في نموذجنا المقترح بالرغم من أنها تستخدم عدد خلايا أكبر بكثير وشبكة أقوى من حيث الذاكرة. بناءً على ما سبق يمكن أن نعتبر أن النموذج الذي قمنا باقتراحه أكثر كفاءة من النماذج المذكورة في الدراسة الأخيرة جميعها. كفاءة نموذجنا المقترح تأتي من كونه يستخدم شبكة أقل تعقيداً ونتائج مقارنة. من جهة أخرى بالنظر إلى الدراسة [39] والتي لم نتطرق لها ضمن الفصول السابقة، وذلك لأنها تختلف بعض الشيء عن موضوع دراستنا من حيث نوع البيانات والسياق التطبيقي. مع ذلك أدرجنا هذه الدراسة كمثال على التوجهات المختلفة في تحليل السلوك الشاذ. تقدم هذه الدراسة نموذجاً متقدماً في كشف الشذوذ لبيئات المدن الذكية باستخدام نظام متعدد النماذج (Multimodel-Based System, MBS). النموذج الأول يستخدم شبكة الـ LSTM والنموذج الثاني يعتمد على الشبكة ConvLSTM. أما الثالث فيقوم بتحليل الأنشطة التي يمارسها المستخدم يومياً. التقييمات النهائية للنظام المقترح في الدراسة [39] كانت على الشكل الآتي: Accuracy = 0.97، Precision = 0.97 وأخيراً AUC = 0.96. نلاحظ أنه على الرغم من أن الدراسة الرابعة تتفوق بالقيم جميعها على نموذجنا المقترح إلا أنها تعتمد على نماذج متعددة وتحليل معقد يتناسب مع بيانات المدن الذكية. من جهة أخرى فإن دراستنا تركز على بنية أبسط وأكثر فعالية في بيئة مغلقة. تساعد هذه المقارنة في إبراز مرونة نموذجنا، حيث بيئة دراستنا المحددة التي تعتمد على بيانات شبكة داخلية وسجلات دخول وخروج المستخدمين لا يناسبها نموذج الدراسة [39].

في النهاية، نستطيع القول إن النموذج الذي قمنا باقتراحه أثبت قدرته بشكل جيد جداً في كشف الشذوذ مع دقة جيدة وأداء ثابت. المقارنة السابقة والنتائج تثبت فعالية النموذج المقترح في مجال كشف الشذوذ. إدخال الـ GA ساهم في تحسين النموذج وتقليل تأثير مشكلة عدم التوازن في البيانات بالرغم من التعقيد الحسابي المرتفع قليلاً.

استخدام بيانات تحتوي على ميزات شائعة في الشبكات الواقعية مثل أوقات تسجيل الدخول والخروج وأجهزة المستخدمين يجعل النموذج قابل للتعميم أو استخدام بيانات حقيقية. صعوبة التنفيذ على بيانات حقيقية تكمن في معالجة البيانات المستمرة التي تصل بشكل متدرج. معالجة بيانات مستمرة يتطلب استخدام أدوات لتحليل الشبكة، تستطيع معالجة البيانات المتدفقة في الوقت الحقيقي. عند تطبيق النموذج المقترح على أنظمة واقعية تزيد من مخاطر الإنذارات الكاذبة نتيجة تغير الأنماط السلوكية فجأة. علاوة على ذلك تكلفة حسابية عالية عند تطبيق النموذج على بيانات ضخمة في الوقت الفعلي.

5.6. خلاصة الفصل

في هذا الفصل، قدمنا نموذجاً جديداً لتحليل سلوك المستخدم باستخدام الـ GRU المدعومة بالـ GA لتحسين الأوزان. صممنا النموذج ليعمل بشكل مشابه لنهج التشفير التلقائي. تم إعادة بناء المدخلات واستخدام الخطأ الناتج في التمييز بين السلوك الطبيعي والشاذ. قيمنا النموذج باستخدام مقاييس متعددة مثل الدقة والاسترجاع، بالإضافة إلى معيار الـ AUC لقياس جودة التصنيف وكشف الشذوذ.

أظهرت النتائج أن نموذجنا المقترح يتميز بمعدل استرجاع مرتفع (100%)، مما يبين قدرته العالية على اكتشاف الحالات الشاذة جميعها. كما حقق الـ AUC بقيمة 0.95، مما يشير إلى أداء جيد في تمييز الأنماط الطبيعية عن غير الطبيعية. مع ذلك، لوحظ وجود نسبة من الإنذارات الخاطئة لارتفاع قيمة الـ FP، مما قد يتطلب مزيداً من التحسينات في ضبط العتبة المستخدمة لتحديد الشذوذ.

بالمقارنة مع الدراسات السابقة، فقد لاحظنا تفوق نموذجنا المقترح في بعض الجوانب مثل الكشف الفعال عن السلوكيات غير الطبيعية دون الحاجة إلى بيانات مصنفة، بفضل استخدام الـ GA في تحسين الأوزان. لا يزال هناك مجال لتطوير النموذج من خلال تقليل معدل الإنذارات الخاطئة وتحسين آلية استخراج الميزات.

بشكل عام، أثبت هذا النموذج فعاليته كأداة قوية في مجال تحليل سلوك المستخدم للكشف عن الشذوذ، مما يمهد الطريق لمزيد من الأبحاث في تطوير تقنيات ذكاء الصنعي أكثر دقة واستدامة في هذا المجال.

الفصل السابع

الخاتمة والرؤى المستقبلية

1.7. الخاتمة

في هذه الدراسة، قمنا بتطوير نموذج لتحليل سلوك المستخدم بناءً على شبكة الـ GRU العصبية، حيث يتم تحديث الأوزان باستخدام الـ GA. يهدف نموذجنا المقترح إلى تعلم سلوك المستخدم الطبيعي واكتشاف الشذوذ. بالنظر إلى عدم التوازن في البيانات، إذ تفوق السجلات الطبيعية بكثير السجلات الشاذة، ركزنا على تحسين قدرة النموذج على اكتشاف الشذوذ مع تقليل تأثير عدم التوازن في البيانات. لقد حقق البحث أهدافه من خلال تطوير نموذج قادر على تصنيف السلوكيات واكتشاف الأنماط الشاذة ضمن الشبكة والحفاظ على توازن جيد بين معدلات الاكتشاف والدقة. الأمر الذي يعزز من إمكانية استخدامه في بيانات حقيقية لرصد التهديدات الأمنية.

2.7. الاستنتاجات والتوصيات والرؤى المستقبلية

فيما يلي بعض الملاحظات الناتجة من تحليل قدرات النموذج وقد وضعناها على شكل استنتاجات. بهدف استمرارية التطوير والحصول على نموذج أفضل قمنا بوضع بعض الحلول والمقترحات التي يمكن العمل عليها.

الاستنتاجات:

1. أظهر النموذج كفاءة عالية في اكتشاف السلوك الشاذ فقد حقق معدل استرجاع مرتفع لهذه الفئة، مما يجعله مناسباً لاكتشاف التهديدات الأمنية الحساسة في الشبكات.
2. استخدام الخوارزمية الجينية ساهم في تحسين جودة الأوزان. بتخفيف تأثير عدم التوازن في البيانات ظهر تحسين أداء النموذج. الخوارزمية الجينية تساعد في الحصول على أوزان أفضل مع تجنب مشاكل الاشتقاق التي تحول دون الوصول للحل الأمثل.
3. على الرغم من تحقيق معدل عالٍ لاكتشاف الشذوذ ومعالجة مشكلة عدم التوازن، إلا أن دقة الفئة الشاذة يمكن تحسينها لتقليل الإنذارات الخاطئة. إمكانية التحسين في الدقة تفتح المجال للأبحاث الجديدة.
4. لوحظ أن التعقيد الحسابي في تنفيذ الـ GA مرتفع قليلاً.
5. يمكن تطبيق النموذج على بيانات حقيقية ولكن يوجد بعض التحديات مثل الكلفة العالية للموارد.

التوصيات والرؤى المستقبلية:

1. تحسين الدقة للفئة الشاذة لتقليل الإنذارات الخاطئة عن طريق تجربة استراتيجيات مثل:
 - إعادة ضبط العتبة المستخدمة في التصنيف.
 - تحسين دالة اللياقة في الخوارزمية الجينية.
 - تجربة تعديلات على بنية النموذج مثل عدد الوحدات والخلايا في شبكة الـ GRU.
2. دمج بعض الخوارزميات الأخرى مع النموذج مثل Isolation Forest وذلك لتحسين النتائج.
3. تجربة النموذج على بيانات حقيقية لتقييم قدرة النموذج على التعميم. يتم ذلك من خلال استخدام تقنية إعادة التدريب لضبط الأوزان مع بيانات قد تحوي أنماطاً جديدة. لتخفيف تكلفة الموارد يمكن تقسيم البيانات الحقيقية المستمرة إلى نوافذ زمنية صغيرة وتحليل النشاط في كل نافذة على حدة.
4. توسيع نطاق البيانات بإضافة ميزات أخرى مثل استخدام البريد الإلكتروني، مشاركة الملفات، تصفح الإنترنت، الطباعة وغيرها من الأنشطة والسلوكيات الإضافية.
5. دمج النموذج مع نظام تنبيهات ذكي مع واجهة تفاعلية. عرض التهديدات المكتشفة مع إرسال إشعار مباشر عند حدوث شذوذ عالي الخطورة.
6. فيما يخص التعقيد الحسابي للـ GA:
 - يمكن تقليل عدد الأجيال إلى 25 جيل بدلاً من 40.
 - تقليل نسبة الطفرة إلى 3%، مما يساهم في تقليل عدد التعديلات العشوائية غير الضرورية.
 - تقليل عدد الأفراد في كل جيل مع الحفاظ على جودة التحسين.
 - استغلال المعالجة المتوازية لتسريع عمليات التقييم داخل الأجيال. تساعد التعديلات هذه في تسريع عملية التطور الجيني مع الحفاظ على استقرار الأوزان وتوازن النموذج.

قائمة المصطلحات (List of Terms)

A	
Accuracy	الدقة
Activation Function	تابع التفعيل
Anomaly	شذوذ
Anomaly Data	بيانات شاذة
Anomaly Detection	كشف الشذوذ
Artificial Intelligence	الذكاء الصناعي
Autoencoder	المشفّر التلقائي

B	
Back Propagation	المسار الخلفي
Baseline	الخط الأساسي
Batch Size	حجم الدفعة
Bias	الانحياز
Big Data	بيانات ضخمة

C	
Chromosome	الصبغي
Classification	التصنيف
Clustering	العنقدة (التجميع)
Confusion Matrix	مصفوفة الارتباك
Crossover	التقاطع
Cyber Attack	هجوم سيبراني
Cyber Security	الأمن السيبراني
Cyber Space	الفضاء السيبراني

D	
Dataset	مجموعة بيانات
Deep Learning	التعلم العميق
Deep Neural Network	الشبكة العصبية العميقة

E	
Entity	الكيان
Epochs	الدورات
Evolutionary Algorithms	الخوارزميات التطورية

F	
False Negative	سلبي خاطئ
False Positive	إيجابي خاطئ
False Positive Rate	معدل الإيجابي الخاطئ
Features	ميزات
Feed-Back	تغذية راجعة
Feed-Forward	تغذية أمامية
Fitness Function	دالة اللياقة
Forward Propagation	المسار الأمامي

G	
Gated Recurrent Unit	الوحدة متكررة البوابة
Generation	جيل
Genetic Algorithm	خوارزمية جينية
Genes	جين

H	
Hidden Layers	الطبقات الخفية
Hyperplane	المستوي الفائق

I	
Information Security	أمن المعلومات
Input Layer	طبقة المدخلات
Inputs Reconstruction	إعادة بناء المدخلات
Intrusion Detection Systems	أنظمة كشف التسلل
Intrusion Prevention Systems	أنظمة منع التسلل

L	
Long (Short) Term Memory Network	الشبكة ذات الذاكرة طويلة (قصيرة) المدى
Loss Function	معادلة الخطأ

M	
Machine Learning	تعلم الآلة
Max Margin	الهامش الأقصى
Mutation	طفرة

N	
Network	شبكة
Network Security	أمن الشبكة
Neural Network	الشبكة العصبية
Normal	طبيعي

O	
Outputs Layer	طبقة المخرجات

P	
Precision	الدقة
Proposed Model	النموذج المقترح

R	
Recall	الاسترجاع
Recurrent Neural Network	الشبكة العصبية المتكررة
Reinforcement Learning	التعلم المعزز

S	
Security	الأمن
Security Analytics	تحليلات الأمن
Security Information and Event Management	المعلومات الأمنية وإدارة الأحداث
Selection	الاختيار
Seme Supervised Learning	التعلم شبه الخاضع لإشراف
Shallow Neural Network	الشبكة العصبية الضحلة
Supervised Learning	التعلم بإشراف
Support Vector Machine	آلة شعاع الدعم

T	
Threshold	العتبة
Training Data	بيانات التدريب
True Negative	سلبي صحيح
True Positive	إيجابي صحيح
True Positive Rate	معدل الإيجابي الصحيح

U	
Unsupervised Learning	التعلم بغير إشراف
User Behavior Analysis	تحليل سلوك المستخدم

W	
Weights	الأوزان

قائمة الاختصارات (List of Acronyms)

Artificial Intelligence	AI
Computer Emergency Response Team	CERT
Confusion Matrix	CM
Deep Learning	DL
Deep Neural Network	DNN
False Negative	FN
False Positive	FP
False Positive Rate	FPR
Genetic Algorithm	GA
Genetic Gated Recurrent Unit	GGRU
Gated Recurrent Unit	GRU
Intrusion Detection Systems	IDS
Intrusion Prevention Systems	IPS
Long Short-Term Memory	LSTM
Machine Learning	ML
Mean Absolute Error	MAE
Mean Square Error	MSE
Recurrent Neural Network	RNN
Security Information and Event Management	SIEM
Support Vector Machine	SVM
True Negative	TN
True Positive	TP
True Positive Rate	TPR
User Behavior Analysis	UBA

المراجع

- [1] دخيل، ناصر. (2022). ما هو الأمن السيبراني وما أهميته؟. استرجع من <https://academy.hsoub.com/devops/security/%D9%85%D8%A7-%D9%87%D9%88-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%88%D9%85%D8%A7-%D8%A3%D9%87%D9%85%D9%8A%D8%AA%D9%87%D8%9F-r664/>
- [2] سابا، غسان. (2018). الشبكات الحاسوبية. الجمهورية العربية السورية: الجامعة الافتراضية السورية.
- [3] سعيدي، خليل، وبن مهدي، مرزوق. (2022). الذكاء الاصطناعي كتوجه حتمي لحماية الأمن السيبراني. مجلة دراسات في حقوق الانسان، 6(1)، 37-25.
- [4] السمان، مني عبد الله. (2020). متطلبات تحقق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. المملكة العربية السعودية: جامعة الملك سعود.
- [5] الشمري، صالح بن عبدالله. (2021). أمن الشبكات والأمن السيبراني. المملكة العربية السعودية: العطاء الرقمي.
- [6] العضيبيات، آية. (2022، 24 نيسان). استرجعت من <https://e3arabi.com/technology/%D8%AA%D8%AD%D9%84%D9%8A%D9%84%D8%A7%D8%AA-%D8%B3%D9%84%D9%88%D9%83-%D8%A7%D9%84%D9%85%D8%B3%D8%AA%D8%AE%D8%AF%D9%85-%D9%88%D8%A7%D9%84%D9%83%D9%8A%D8%A7%D9%86-%D8%A8%D8%A7%D9%84%D8%A3%D9%85%D9%86/>
- [7] عويشق، إباء. (2018). مقدمة في الشبكات. الجمهورية العربية السورية: الجامعة الافتراضية السورية.
- [8] المطيري، خالد ظاهر. (2022، تموز). دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي. مجلة البحوث الفقهية والقانونية. (38)، 1666-969.
- [9] Abolwafa, A. E. (2022, May). A survey of Deep Learning Algorithms and its Application. Nile Journal of Communication & Computer Science, 3(1).
- [10] Akutota, T., & Choudhury, S. (2017, October). Big Data Security Challenges: An Overview and Application of User Behavior Analytics. International Research Journal of Engineering and Technology (IRJET), 4(10), 1544-1548

- [11] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., & Yassin, W. (2020, March). New insider threat detection method based on recurrent neural networks. *Indonesian Journal of Electrical Engineering and Computer Science*, 17(3). 1474-1479.
DOI: 10.11591/ijeecs.v17.i3.pp1474-1479
- [12] Alshehri, A., Khan, N., Alowayr, A., & Alghamdi, M. Y. (2022, 27February). Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics. *Computer Systems Science & Engineering*, 44(2). 1679-1689.
DOI: 10.32604/csse.2023.026526
- [13] Bartz-Beielstein, T., Branke, J., Mehnen, J., & Mersmann, O. (2014). Overview: Evolutionary Algorithms. *WIREs Data Mining Knowl Discov*, 4. 178-195.
DOI:10.1002/widm.1124
- [14] Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly Detection: A Survey*. USA: University of Minnesotur.
- [15] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, 21(6).
<https://doi.org/10.1186/s12864-019-6413-7>
- [16] Davies, V. (2021). *The history of cyber security*. Retrieved from <https://cybermagazine.com/cyber-security/history-cybersecurity>
- [17] Faozi, J., & Colliot, O. (2023). *Classic machine learning algorithms*. Paris: hal.
<https://hal.science/hal-03830094v1>
- [18] Geron, A. (2019, June). *Hands-on Machine Learning with Scikit-Learn, Keras & Tensorflow*. USA:O'Reilly Media.
- [19] Ghosh, M., Arunachalam, T. (2021). *Introduction to Artificial Intelligence*. India. 10.1007/978-981-16-0415-7-2
- [20] Hochreiter, S., & Schmidhuber, J. (1997). LONG SHORT-TERM MEMORY. *NEURAL COMPUTATION*, 9(8). 1735-1780.
- [21] *Insider Threat Test Dataset*. (2016, 28November). Retrieved from [Insider Threat Test Dataset \(cmu.edu\)](https://insider-threat-test-dataset.cmu.edu)
- [22] IOS. (1994). Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

<https://www.iso.org/standard/20269.html>

[23] Jakkula, V. (n.d.). *Tutorial on Support Vector Machines (SVM)*. Washington: Washington State University.

[24] Jawed, H., Ziad, Z., Khan, M. M., & Asrar, M. (2018). Anomaly detection through keystroke and tap dynamics implemented via machine learning algorithms. *Turkish Journal of Electrical Engineering and Computer Sciences*, 26(4). 1698-1709.

<https://doi.org/10.3906/elk-1711-410>

[25] Kecman, V. (2005). *Support Vector Machines - An Introduction*. (pp. 1-47). New Zealand: Auckland.

[26] Li, Y., & Liu, Q. (2021, November). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7. 8176-8286.

<https://doi.org/10.1016/j.egy.2021.08.126>

[27] Marshal, P. (2016). *Algorithms and Artificial Intelligence*. USA: SAGA PUBLICATION.

[28] Mathew, T.V. (n.d.). *Genetic Algorithm*. Mumbai: Indian Institute of Technology Bombay.

[29] Mohsen, S. (2023, 21April). Recognition of human activity using GRU deep learning algorithm. *Multimedia Tools and Applications*, 82. 47733-47749.

<https://doi.org/10.1007/s11042-023-15571-y>

[30] Muliukha, V., Lukashin, A., Utkin, L., Popov, M., & Meldo, A. (2020, 2-4 October). *Anomaly Detection Approach in Cyber Security for User and Entity Behavior Analytics System*. European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning.

[31] Nepal, S., & Joshi, B. (2021, October). User Behavior Analytics for Insider Threat Detection using Deep Learning. *Proceeding of 10th IOE Graduate Conference*, 10. 232-238.

[32] Prowse, D. L. (2018). *Cert Guide*. USA: Pearson Education.

[33] Raaghav, S. (2022). *User and Entity Behavior Analytics(UEBA)*. Retrieved from <https://www.manageengine.com/active-directory-360/manage-and-protect-identities/iam-library/auditing/user-and-entity-behaviour-analytics-ueba.html>

- [34] Raguvir, S., & Babu, S. (2020, 10-12 March). *Detecting Anomalies in Users - An UEBA Approach*. Proceedings of the International Conference on Industrial Engineering and Operations Management. UAE: IEOM Society International.
- [35] Rajasekar, V., Prenalatha, J., & Dhanaraj, R. (2022, March). System Assurances. *Modeling and Management*. 333-354.
<https://doi.org/10.1016/B979-0-333-90240-3.1000019-9>
- [36] Rayaprolu, A. (2020). *How Much Data is Created Every Day in 2024*. Retrieved from
<https://techjury.net/blog/how-much-data-is-created-every-day/>
- [37] *Security analytics shares up hope for breach*. (2019, 13February). Retrieved from
<https://web.archive.org/web/20190212184120/https://www.enterpriseinnovation.net/article/security-analytics-shores-hope-breach-detection-192448485>
- [38] Taye, M. M. (2023). *Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions*. Jordan: Philadelphia University.
- [39] Tian, Z., Luo, C., LU, H., Su, S., Sun, Y., & Zhang, M. (2020, September). User and Entity Behavior Analysis under Urban Big Data. *ACM/IMS Transactions on Data Science*,1(3).
- [40] Whitley, D. (1998, October). A Genetic Algorithm Tutorial. *Statistics and Computing*.
 DOI: 10.1007/BF00175354
- [41] Williams, R. J., & Zipser, D. (1989). A Learning Algorithms for Continually Running Fully Recurrent Neural Networks. *Neural Computation*, 1. 270-280.
- [42] Zolait, A., & Sakitin, M. (2018). *The role of User Entity Behavior Analytics to detect network attacks in real time*. International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, Bahrain.

الملحق

برمجة النموذج المقترح باستخدام لغة البرمجة Python ومحرر الأكواد Visual Studio Code

المرحلة الأولى للنموذج

```
import pandas as pd
from datetime import datetime

# حساب مدة الجلسة بين وقت تسجيل الدخول والخروج
def count_time(logon_time, logoff_time):
    return( logoff_time-logon_time).total_seconds()/3600

# حساب يوم الأسبوع من تاريخ معين
def find_weekday(time):
    return time.strftime('%A')

# قراءة البيانات باستخدام pandas من ملف csv
def log_feature(file_input):
    df=pd.read_csv(file_input,
names=['id','date','user','pc','activity'],skiprows=1)
    # تحويل date الى datetime
    df['date']=pd.to_datetime(df['date'],format='%m/%d/%Y %H:%M:%S')
    return df

# مطابقة سجلات logon مع logoff
def mach_logon_logoff(df):
    session = []
    df = df.sort_values(by='date') # فرز السجلات حسب التاريخ
    logon_dict = {} # قاموس لتخزين أوقات تسجيل الدخول
    for index, row in df.iterrows():
        key = (row['user'], row['pc']) # المفتاح هو المستخدم والجهاز
```

```

if row['activity'].lower() == 'logon': # التحقق من النشاط إذا كان Logon
    logon_dict[key] = row['date'] # إضافة وقت تسجيل الدخول إلى القاموس
elif row['activity'].lower() == 'logoff': # التحقق من النشاط إذا كان Logoff
    if key in logon_dict: # مسبقاً للمستخدم والجهاز Logon التحقق إذا كان هناك وقت
        logon_time = logon_dict[key]
        logoff_time = row['date']
        duration = count_time(logon_time, logoff_time) # حساب المدة
        weekday = find_weekday(logon_time) # العثور على اليوم

    # إضافة الجلسة إلى القائمة
    session.append({
        'User': row['user'],
        'Pc': row['pc'],
        'logontime': logon_time.strftime('%d/%m/%Y %H:%M:%S'),
        'logofftime': logoff_time.strftime('%d/%m/%Y %H:%M:%S'),
        'Duration': duration,
        'Weekday': weekday
    })

    print(f"Session added: {session[-1]}") # طباعة الجلسة المضافة

    del logon_dict[key] # حذف دخول المستخدم بعد معالجته
else:
    print(f"Logoff without Logon: {key}") # طباعة رسالة في حالة وجود
    سابق Logon بدون Logoff
    return pd.DataFrame(session)

# حفظ البيانات المعالجة في ملف
def save_processed_logs(processed_df, file_output):
    processed_df.to_csv(file_output, index=False)
    print(f"Data saved to {file_output}")

```

الخطوة الأساسية لمعالجة البيانات

```
def data_preprocess(file_input,file_output):  
    df=log_feature(file_input)  
    processed_df=mach_logon_logoff(df)  
    save_processed_logs(processed_df,file_output)
```

file_input='D:\\logon.csv' # مسار الملف الأساسي

file_output='D:\\ processed_logon.csv' # مسار الملف الأول للمعالجة

```
data_preprocess(file_input,file_output)
```

المرحلة الثانية للنموذج

```
import pandas as pd
```

```
from sklearn.preprocessing import MinMaxScaler, LabelEncoder
```

```
import numpy as np
```

تحميل البيانات

```
data = pd.read_csv('D:\\ processed_logon.csv')
```

datetime تحويل التواريخ إلى كائنات

```
data['logontime'] = pd.to_datetime(data['logontime'], format='%d/%m/%Y %H:%M:%S')
```

```
data['logofftime'] = pd.to_datetime(data['logofftime'], format='%d/%m/%Y %H:%M:%S')
```

حساب الفارق الزمني (عدد الثواني منذ بداية اليوم)

```
data['logontime'] = data['logontime'].dt.hour * 3600 + data['logontime'].dt.minute  
* 60 + data['logontime'].dt.second
```

```
data['logofftime'] = data['logofftime'].dt.hour * 3600 +  
data['logofftime'].dt.minute * 60 + data['logofftime'].dt.second
```

التطبيع الكامل للقيم العددية

```
scaler = MinMaxScaler()
```

```
numerical_columns = ['Duration', 'logontime', 'logofftime']
```

```

data[numerical_columns] = scaler.fit_transform(data[numerical_columns])

# [0, 1] ترميز القيم الفئوية وتحويلها إلى نطاق
categorical_columns = ['User', 'Pc', 'Weekday']
for column in categorical_columns:
    label_encoder = LabelEncoder()
    data[column] = label_encoder.fit_transform(data[column])
    # [0, 1] تطبيع القيم الفئوية إلى نطاق
    data[column] = MinMaxScaler().fit_transform(data[column].values.reshape(-1, 1))

# الاحتفاظ بالترتيب الأصلي عن طريق الحفاظ على index
data.reset_index(drop=True, inplace=True)

# حفظ البيانات المعالجة في ملف
data.to_csv('D:\\normalized_logon.csv', index=False)
print(" save the normalizid data in:'normalized_logon.csv'")

# تقسيم البيانات إلى تدريب واختبار (70% تدريب، 30% اختبار) مع الاحتفاظ بالترتيب
train_data = data.iloc[:int(0.7 * len(data))]
test_data = data.iloc[int(0.7 * len(data)):]

# حفظ بيانات التدريب والاختبار في ملفات CSV
train_data.to_csv('D:\\train_data.csv', index=False)
test_data.to_csv('D:\\test_data.csv', index=False)
print("The training and testing data have been saved in CSV files.")

# تحويل البيانات إلى الشكل ثلاثي الأبعاد (سجل-سجل دون خلط)
train_sequences = train_data.to_numpy().reshape(-1, 1, train_data.shape[1]) # كل
سجل بشكل مستقل
test_sequences = test_data.to_numpy().reshape(-1, 1, test_data.shape[1])

```

```
# حفظ بيانات التدريب والاختبار في ملفات NPY
np.save('D:\\train_data.npy', train_sequences)
np.save('D:\\test_data.npy', test_sequences)
print(f"The training ({len(train_sequences)}) and testing ({len(test_sequences)})
data have been saved in NPY files.")
```

المرحلة الثالثة للنموذج

```
import numpy as np
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Dense, GRU
import pygad
import pygad.kerasga
import matplotlib.pyplot as plt

# تحميل بيانات التدريب
train_data = np.load('D:\\train_data.npy')

# بناء النموذج باستخدام Keras
model = Sequential()
model.add(GRU(24, input_shape=(train_data.shape[1], train_data.shape[2]),
return_sequences=True, activation='tanh'))
model.add(GRU(12, return_sequences=False, activation='tanh'))
model.add(Dense(8, activation='tanh'))
model.add(Dense(6, activation='tanh'))
model.add(Dense(train_data.shape[2], activation='sigmoid'))

# تلخيص النموذج
model.summary()
print("Model built successfully")

# تحويل النموذج إلى PyGAD-compatible باستخدام KerasGA
```

```

keras_ga = pygad.kerasga.KerasGA(model=model, num_solutions=8)

# قائمة لتخزين قيم الخطأ لكل جيل
error_list = []

# دالة حساب الخطأ (fitness function)
def fitness_function(ga_instance , solution, solution_idx ):
    print(f"Start Fitness Calculation for Solution {solution_idx}")
    global train_data, keras_ga

    # تعيين الأوزان الحالية للنموذج
    model_weights = pygad.kerasga.model_weights_as_matrix(model=model,
weights_vector=solution)
    model.set_weights(model_weights)

    # التنبؤ ومعالجة البيانات في دفعات لتقليل الذاكرة
    batch_size = 1024
    mse_list = []
    for i in range(0, train_data.shape[0], batch_size):
        batch_data = train_data[i:i+batch_size]
        predictions = model.predict(batch_data, verbose=0)
        mse_batch = np.mean(np.square(batch_data - predictions), axis=(1, 2))
        mse_list.extend(mse_batch)

    # حساب الخطأ (MSE)
    loss = np.mean(mse_list)
    print(f"End Fitness Calculation for Solution {solution_idx}:",loss)
    return -loss # لأن PyGAD يحاول زيادة قيمة fitness

# وظيفة تستدعى بعد كل جيل
def on_generation(ga_instance):

```

```

best_solution, best_solution_fitness, _ = ga_instance.best_solution()
error_list.append(-best_solution_fitness) # تخزين قيمة الخطأ
print(f"Completed Generation {ga_instance.generations_completed}")
print(f"Best fitness in generation {ga_instance.generations_completed}: {-best_solution_fitness}")

# إعداد الخوارزمية الجينية
ga_instance = pygad.GA(
    num_generations=40,
    num_parents_mating=4,
    fitness_func=fitness_function,
    initial_population=keras_ga.population_weights,
    sol_per_pop=8,
    mutation_percent_genes=5 ,
    allow_duplicate_genes=False,
    on_generation=on_generation # استدعاء الدالة بعد كل جيل
)

# تشغيل الخوارزمية الجينية
ga_instance.run()
print("Genetic algorithm completed")

# استخراج أفضل حل (أوزان النموذج)
best_solution, best_solution_fitness, _ = ga_instance.best_solution()
model_weights = pygad.kerasga.model_weights_as_matrix(model=model,
weights_vector=best_solution)
model.set_weights(model_weights)

# حفظ النموذج مع الأوزان المثلى
model.save('D:\\gru_model_genetic.keras')
print("Model saved as gru_model_genetic")

```

```

# رسم دالة الخطأ بعد إتمام الخوارزمية
plt.plot(error_list)
plt.title("Error Reduction per Generation")
plt.xlabel("Generation")
plt.ylabel("Error")
plt.savefig("D:\\error_plot_final.png") # حفظ الرسم في ملف
plt.show() # لعرض الرسم

```

المرحلة الرابعة للنموذج

```

import numpy as np
import pandas as pd
from tensorflow.keras.models import load_model
import matplotlib.pyplot as plt
import seaborn as sns

# تحميل النموذج المحفوظ وبيانات الاختبار
model = load_model('D:\\gru_model_genetic.keras')

test_data = np.load('D:\\test_data.npy').astype(np.float32) # تقليل استهلاك الذاكرة
# باستخدام float32

# التنبؤ وإعادة بناء المدخلات
batch_size = 1024
reconstructed_data = []

# معالجة البيانات على دفعات لتقليل استهلاك الذاكرة
for i in range(0, test_data.shape[0], batch_size):
    batch_data = test_data[i:i+batch_size]
    reconstructed_batch = model.predict(batch_data, verbose=0)
    reconstructed_data.extend(reconstructed_batch)

```

```

reconstructed_data = np.array(reconstructed_data, dtype=np.float32) # تقليل
استهلاك الذاكرة باستخدام float32

# حساب الخطأ لكل سجل على دفعات
mse_per_record = []

for i in range(0, test_data.shape[0], batch_size):
    batch_data = test_data[i:i+batch_size]
    reconstructed_batch = reconstructed_data[i:i+batch_size]
    mse_batch = np.mean(np.square(batch_data - reconstructed_batch), axis=(1,
2))
    mse_per_record.extend(mse_batch)

mse_per_record = np.array(mse_per_record)

# حساب المتوسط والانحراف
Std_error = np.std(mse_per_record)
Mean_error = np.mean(mse_per_record)
print(f"std Error: {Std_error}")
print(f"Mean Error: {Mean_error}")

# تصنيف السجلات بناءً على الخطأ فقط (بدون العتبة)
# (0) إذا كان الخطأ كبيراً، فإن السجل سيكون شاذاً (1)، وإذا كان صغيراً، فإن السجل سيكون غير شاذ
initial_labels = np.where(mse_per_record > Mean_error + 2*Std_error , 1, 0) #
تصنيف مبدئي بناءً على الخطأ

# حفظ النتائج المبدئية (التصنيف بناءً على الخطأ فقط)
initial_results = pd.DataFrame({
    "Error": mse_per_record,
    "Initial Label": initial_labels
})

```

```

initial_results.to_csv("D:\\initial_test_results.csv", index=False)
print("Initial test results saved to D:\\initial_test_results.csv")

# تحديد العتبة باستخدام النسبة المئوية (مثلاً: 80%)
threshold = np.percentile(mse_per_record, 95)
print(f"Selected Threshold: {threshold}")

# إعادة التصنيف بناءً على مقارنة الخطأ مع العتبة
final_labels = np.where(mse_per_record > threshold, 1, 0) # إذا كان الخطأ أكبر من العتبة،
# السجل شاذ

# حفظ النتائج النهائية بعد مقارنة الخطأ بالعتبة
final_results = pd.DataFrame({
    "Error": mse_per_record,
    "Final Label": final_labels
})

final_results.to_csv("D:\\final_test_results.csv", index=False)
print("Final test results saved to D:\\final_test_results.csv")

# بيانات الخطأ حسب الفئات
normal_errors = mse_per_record[final_labels == 0]
anomalous_errors = mse_per_record[final_labels == 1]

# يدويًا KDE توليد
x_vals = np.linspace(min(mse_per_record), max(mse_per_record), 1000)
kde_normal = gaussian_kde(normal_errors)
kde_anomalous = gaussian_kde(anomalous_errors)

# الكثافات
density_normal = kde_normal(x_vals)
density_anomalous = kde_anomalous(x_vals)

# قيمة صغيرة لتحديد التقاطع الحقيقي (0.01 > منطقة التداخل: حيث الكثافتان
intersection_mask = (density_normal > 0.01) & (density_anomalous > 0.01)

```

```

intersection_range = x_vals[intersection_mask]
min_intersection = intersection_range.min()
max_intersection = intersection_range.max()

# ترتيب البيانات
sorted_indices = np.argsort(mse_per_record)
sorted_errors = mse_per_record[sorted_indices]
sorted_labels = final_labels[sorted_indices]

# تلوين حسب منطقة التداخل
colors = []
for error, label in zip(sorted_errors, sorted_labels):
    if min_intersection <= error <= max_intersection:
        colors.append('yellow') # تداخل كثافي فعلي
    else:
        colors.append('blue' if label == 0 else 'red')

# الرسم
plt.figure(figsize=(14, 6))
plt.scatter(range(len(sorted_errors)), sorted_errors, c=colors, alpha=0.6,
s=10)

plt.title(" Scatter Plot of All Errors with Overlap Region")
plt.xlabel("Sorted Record Index")
plt.ylabel("Reconstruction Error")
plt.legend(handles=[
    plt.Line2D([0], [0], marker='o', color='w', label='Normal (0)',
markerfacecolor='blue', markersize=8),
    plt.Line2D([0], [0], marker='o', color='w', label='Anomalous (1)',
markerfacecolor='red', markersize=8),
    plt.Line2D([0], [0], marker='o', color='w', label='Overlap Region ',
markerfacecolor='yellow', markersize=8)
])

plt.tight_layout()
plt.savefig("D:\\Scatter_Anomalies_vs_Normal.png")
plt.show()

```

```

# رسم توزيع الخطأ
plt.figure(figsize=(10, 6))

plt.hist(mse_per_record, bins=50, color='blue', alpha=0.7,
label='Reconstruction Error')

plt.axvline(x=np.percentile(mse_per_record, 95), color='red', linestyle='--',
label='Threshold (95th Percentile)')

plt.title("Error Distribution")
plt.xlabel("Reconstruction Error")
plt.ylabel("Frequency")
plt.legend()

plt.savefig("D:\\error_distribution.png") # حفظ الرسم
plt.show()

```

المرحلة الخامسة للنموذج

```

import pandas as pd

import matplotlib.pyplot as plt

from sklearn.metrics import roc_curve, auc, confusion_matrix,
classification_report

# تحميل النتائج
initial_results = pd.read_csv("D:\\initial_test_results.csv") # تصنيف الخطأ فقط
final_results = pd.read_csv("D:\\final_test_results.csv") # تصنيف بناءً على العتبة

# استخراج الخطأ والتصنيفات
initial_labels = initial_results["Initial Label"].values
final_labels = final_results["Final Label"].values
mse_per_record = final_results["Error"].values

# حساب مصفوفة الارتباك (Confusion Matrix)
cm = confusion_matrix(initial_labels, final_labels)
print(f"Confusion Matrix:\n{cm}")

```

```

#(Precision, Recall, F1-Score) حساب تقرير التصنيف
report = classification_report(initial_labels, final_labels)
print(f"Classification Report:\n{report}")

# منحنى ROC بناءً على العتبة المحددة
fpr, tpr, thresholds = roc_curve(final_labels, initial_labels)
roc_auc = auc(fpr, tpr)

# رسم منحنى ROC
plt.figure(figsize=(8, 6))
plt.plot(fpr, tpr, color='blue', label=f"ROC Curve (AUC = {roc_auc:.2f})")
plt.plot([0, 1], [0, 1], color='gray', linestyle='--')
plt.title("Receiver Operating Characteristic (ROC) Curve")
plt.xlabel("False Positive Rate")
plt.ylabel("True Positive Rate")
plt.legend(loc="lower right")
plt.savefig("D:\\roc_curve.png") # حفظ منحنى AUC
plt.show()

```

التعقيد الحسابي علماً أن:

n عدد السجلات، g عدد الأجيال، p عدد أفراد كل جيل، t عدد الميزات.

المرحلة الأولى: $O(n \cdot \log(n))$

المرحلة الثانية: $O(n)$

المرحلة الثالثة: $O(n \cdot g \cdot p)$

المرحلة الرابعة: $O(n \cdot t)$

المرحلة الخامسة: $O(n)$

Abstract

As is known, it has become almost impossible to imagine a world without the Internet according to Statista, there were 4.66 billion active users globally in 2021, accounting for 59.5% of the global population.

When billions of people use the Internet, an enormous amount of data moves between different IP addresses, systems, networks and devices. Among these people are threat actors such as Cyber-criminal and Hackers who are capable of compromising an organization's security system. It has become difficult to identify security threat since traditional methods such as manually checking log entries have become obsolete. especially along with the development and the rapid expansion of the Internet Network and the valuable data in it contain which become more exposed to attackers. Therefore, there is an increasing need to security whereupon, developed methods of protection began to emerge such as Network Anomaly Classifications and Detection System then the meaning of Cyber Security crystallized. There are many Anomalies Detection System but system based on Deep Learning methods are the more effective. In general, Artificial Intelligence techniques could make the use of Anomaly Detection System a lot easier.

UBA is a Cyber Security technique used to Anomaly Detection using Artificial Intelligence that flag behavior that could indicate a Cyber-Attack.

This thesis explains the concept of both Cyber Security and Artificial Intelligence. The technique of User Behavior Analysis is discussed theoretically and practically by explaining previous studies. Finally, a hybrid model for network anomaly detection using artificial intelligence algorithms and Genetic Algorithm is proposed.

Keywords: Anomaly Data, Anomaly Detection, Artificial Intelligence, Cyber Security, UBA, Neural Network, Genetic Algorithm.

Damascus University

Faculty of Sciences

Department of Mathematics

Section of Applied Mathematics and Informatics



A study of the UBA by Using AI Algorithms for Network Anomaly Detection

Submitted in Fulfillment of the Requirements for the Master
Degree in Applied Mathematics and Informatics

by: Manwella SAFAR

Supervisor: Dr. Mohamad Firas ALHALABI

2024-2025