الجمهورية العربية السورية
جامعة البعث
كلية الهندسة المعلوماتية
قسم هندسة البرمجيات ونظم المعلومات

تحليل أنظمة كشف الشُّذوذ في البيانات وتطويرها باستخدام التَعَلُّم العميق

دراسة أُعِدَّت لنيل درجة الدكتوراه في الهندسة المعلوماتية باختصاص هندسة البرمجيات ونظم المعلومات

إعـداد

المُهندس: علي لؤي ياسين

إشـراف

أ.د كمال السلوم /مشرف علمي/

أُستاذ في قسم هندسة البرمجيات ونظم المعلومات – كُليَّة الهندسة المعلوماتية – جامعة البعث
اختصاص بحوث عمليات

د. وسيم رمضان /مشرف مشارك/

مُدرس في قسم الاقتصاد الزراعي – كُليَّة الزراعة – جامعة البعث
اختصاص برمجة وحاسبات

1444هـ – 2022 م

تحليل أنظمة كشف الشُّذوذ في البيانات وتطويرها باستخدام التَعَلُّم العميق

جامعة البعث

كلية الهندسة المعلوماتية

الرقم: ١٤٦١/و

التاريخ: ٢/١٠/٢٠٢٢

بيان بإجراء التعديلات العلمية واللغوية

قام الطالب **علي لؤي ياسين** بتصحيح الملاحظات التي وردت في متن أطروحة الدكتوراه والتي أشار إليها الدكاترة أعضاء لجنة الحكم خلال مناقشة الأطروحة.

عضواً	عضواً	عضواً	عضواً	مشرفاً ورئيساً للجنة الحكم
د. إيفا حريقص	د. محمد ملحم	د. طارق الناصوري	أ. مرانيا لطفي	أ.د كمال الشلوم

رئيس قسم هندسة البرمجيات ونظم المعلومات

د. إيفا حريقص

شكر وتقدير

في البداية، الشكر والحمد لله، جلَّ في عُلاه، فإليه يُنسب الفضل كلهُ في إكمالِ هذا البحث – والكمال يبقى لله وحده –

أتوجّه بخالص الشكر والامتنان لأساتذتي الدكتور كمال السلوم والدكتور وسيم رمضان اللّذانِ لن تكفيَ حروفُ هذهِ الكلماتِ لإيفائِهم حقَّهم بصبرهم الكبيرَ عليَّ، ولتوجيهاتهمِ العلميَّةَ الّتي لا تُقدَّرُ بثمن؛ والّتي ساهمت على نحوٍ كبيرٍ في استكمالِ هذا البحث.

كما أتوجّه بخالصِ شكري وتقديري إلى كلِّ من ساعدني من قريبٍ أو من بعيدٍ على إنجازِ وإتمامِ هذا العمل.

حمص في 21 أيلول 2022م الموافق لـ 25 صفر 1444هـ

م. علي لؤي ياسين

الأبحاث المنجزة في مرحلة الدكتوراه

البحث الأول: مجلة جامعة البعث – سلسلة العلوم الهندسية الميكانيكية والكهربائية والمعلوماتية – **2021**

جامعة البعث
مجلة جامعة البعث

Al Baath University
Journal of Al Baath University

قبول نشر بحث
طالب دراسات عليا

الرقم: ٢٨١٨
التاريخ ٧ / ١٢ / 2021

طالـب الدراسـات العليـا: علي ياسين **الدكتور المشرف: كمال السلوم + د. وسيم رمضان**

كلية: الهندسة المعلوماتية – جامعة: البعث

نود إعلامكم بقبول بحثكم الموسوم:

تحديد التوليفة الأمثل من ضبط البارامترات الفائقة واختيار الميزات لتحسين أداء أنظمة كشف الشذوذ

للنشر في مجلة جامعة البعث بالمجلد **43** لعام **2021**

بعد أن تم تحكيمه من قبل مختصين.

نشكر لكم هذه المساهمة الطيبة ونتطلع إلى استمرار تواصلكم مع مجلتنا ومدها بما لديكم من جديد والاطلاع على الأبحاث المنشورة في المجلة على موقع المجلة والرابط المدونين في أسفل الصفحة.

موقع الجامعة www.albaath-univ.edu.sy والرابط magazine @ albaath-univ.edu.sy

رئيس تحرير مجلة جامعة البعث للعلوم الطبية والهندسية والأساسية والتطبيقية

أ.د. درغام سلوم

7-12-2021

مجلة جامعة البعث – سورية – حمص
تأسست عام 1983
ص. ب.: 77 فاكس: 2138071 31 963++
هاتف:(1132 1180) 9910 31 963++
www.albaath-univ.edu.sy

Journal of AL Baath University – Syria – Homs
Est. 1983
P.O. Box: 77 – Fax: ++963 31 2138071
Tel: ++963 31 9910 (1180 1132)
magazine @ albaath-univ.edu.sy

Al Baath University
Journal of Al Baath University

جامعة البعث
مجلة جامعة البعث

قبول نشر بحث
طالب دراسات عليا

الرقم: ٢٨٢
التاريخ ٩ / ٢ / 2022

طالـب الدراسـات العليـا: علي ياسين الدكتور المشرف: كمال السلوم + د. وسيم رمضان
كلية: الهندسة المعلوماتية – جامعة: البعث

نود إعلامكم بقبول بحثكم الموسوم:

تحديد عتبة التصنيف المثلىّ ديناميكياً في أنظمة الكشف المبكر عن الشذوذ القائمة على التعلم العميق

للنشر في مجلة جامعة البعث بالمجلد **44** لعام **2022**
بعد أن تم تحكيمه من قبل مختصين.

نشكر لكم هذه المساهمة الطيبة ونتطلع إلى استمرار تواصلكم مع مجلتنا ومدها بما لديكم من جديد والاطلاع على الأبحاث المنشورة في المجلة على موقع المجلة والرابط المدونين في أسفل الصفحة.

موقع الجامعة www.albaath-univ.edu.sy والرابط magazine @ albaath-univ.edu.sy

رئيس هيئة تحرير مجلة جامعة البعث

أ.د. ناصر سعد الدين

Journal of AL Baath University – Syria – Homs
Est. 1983
P.O. Box: 77 – Fax: ++963 31 2138071
Tel: ++963 31 9910 (1180 1132)
magazine @ albaath-univ.edu.sy

مجلة جامعة البعث – سورية – حمص
تأسست عام 1983
ص. ب.: 77 فاكس: 2138071 31 963++
هاتف:(1132 1180) 9910 31 963++
www.albaath-univ.edu.sy

البحث الثالث: مجلة Journal of Ambient Intelligence and Humanized Computing – مفهرسة ضمن الربع الأول **Q1** في قواعد بيانات **(Scopus)** – **2022**

Journal of Ambient Intelligence and Humanized Computing

(JAIHC) provides a high profile, leading edge forum for academics, industrial professionals, educators and policy makers involved in

ID:7204180932237

To;

Yassin. A,

Ramadan W,

Salloum K,

Subject: Publication of paper at "The Journal of Ambient Intelligence and Humanized Computing".

Dear author,

With greetings we are informing you that your manuscript has been accepted to be published in "The Journal of Ambient Intelligence and Humanized Computing".

Thank you very much for your patience and cooperation during the submission process. This certificate proves that your research "AEDT-ADS Anomaly Detection System Based on Dynamic Classification Threshold and Deep Learning" is officially accepted* initially, and you will be informed by the date of physical publishing by regular means.

*Please note that your paper is accepted scientifically, and it is still may be not published regarding any interfering matter.

Editor-in-Chief:
Vincenzo Loia

Managing Editor:
Carmen De Maio

May-9-2022

فهرس المحتويات

الملخص باللغة العربية ---------- V

الملخص باللغة الإنكليزية ---------- VII

قائمة الأشكال (List of Figures) ---------- IX

قائمة الجداول (List of Tables) ---------- XI

قائمة المصطلحات (List of Terms) ---------- XIV

قائمة الاختصارات (List of Acronyms) ---------- XXI

1- الفصل الأول: مقدمة ---------- 1

1-1- الشُذُوذ (Anomaly) ---------- 1

1-2- أنواع الشُّذُوذ (Types of Anomalies) ---------- 2

1-3- تحديات اكتشاف الشُّذُوذ (Anomaly Detection Challenges) ---------- 2

1-4- طرائق كشف الشُّذُوذ (Anomaly Detection Methods) ---------- 4

1-4-1- طرائق الكشف الإحصائية (Statistical Anomaly Detection) ---------- 4

1-4-2- طرائق تَعَلُّم الآلة (Machine Learning Methods) ---------- 6

1-4-3- طرائق التَّعَلُّم الْعَمِيق (Deep Learning Methods) ---------- 8

1-5- أنظمة كشف الشُّذُوذ (Anomaly Detection Systems) ---------- 11

1-6- مشكلة البحث ---------- 12

1-7- أهداف البحث ---------- 12

1-8- أَهَمِّيَّةُ البحث ---------- 13

1-9- فصول الأطروحة ---------- 13

2- الفصل الثاني: الخوارزميات المستخدمة ---------- 15

2-1- خوارزمية الغابات العشوائية (Random Forest Algorithm) ---------- 15

2-1-1- مصنفات الغابات العشوائية (Random Forests Classifiers) ---------- 15
2-1-2- البارامترات الفائقة للغابات العشوائية (Random Forest Hyperparameter) ----- 17
2-1-3- كشف الشذوذ القائم على الغابات العشوائية ---------- 18
2-2- خوارزمية آلة شعاع الدعم (Support Vector Machine Algorithm) ---------- 18
2-2-1- قابلية الفصل الخطي (Linearly Separable) ---------- 18
2-2-2- مفاهيم آلة شعاع الدعم (Support Vector Machine Concepts) ---------- 19
2-2-3- البارامترات الفائقة لشعاع الدعم (SVM Hyperparameter) ---------- 22
2-2-4- كشف الشذوذ القائم على آلة شعاع الدعم ---------- 23
2-3- شبكة الترميز الآلي (Autoencoder Network) ---------- 23
2-3-1 مفاهيم شبكة الترميز الآلي (Autoencoder Concepts) ---------- 23
2-3-2- أنواع شبكة الترميز الآلي(Types of Autoencoder) ---------- 25
2-3-3- كشف الشذوذ القائم على الترميز الآلي ---------- 26
2-4- الذاكرة قصيرة طويلة المدى (Long Short-Term Memory) ---------- 27
2-4-1- مفاهيم الذاكرة طويلة المدى (LSTM Concepts) ---------- 28
2-4-2- استخدام LSTM للتنبؤ بالشذوذ ضمن السلاسل الزمنية ---------- 29
2-5- شبكة الترميز الآلي ذات الذاكرة طويلة المدى (LSTM Autoencoder) ---------- 30
2-5-1- كشف الشذوذ القائم على LSTM Autoencoder ---------- 30
2-5-2- البارامترات الفائقة لشبكات التعلم العميقة ---------- 31
3- الفصل الثالث: مقاييس البحث وأدواتُهُ ---------- 34
3-1- مقاييس الأداء (Performance Metrics) ---------- 34
3-1-1- المقاييس الإحصائية (Statistical Metrics) ---------- 34
3-1-2- المقاييس البيانية (Graphic Metrics) ---------- 38
3-2- مجموعات البيانات البحثية (Research Datasets) ---------- 41
3-3- الاختبارات الإحصائية (Statistical Tests) ---------- 44
3-3-1- اختبار كولموغوروف – سميرنوف (Kolmogorov-Smirnov Tests) --------- 44
3-3-2- نظرية تشيبيشيف (Chebyshev's Theory) ---------- 46
3-3-3- القاعدة التجريبية (The Empirical Rule) ---------- 46

3-4- ضبط البارامترات الفائقة (Hyperparameter Tuning) ---------- 46

3-5- اختيار الميزات (Feature Selection) ---------- 47

3-6- الحزم والمكتبات المستخدمة (Used Packages and Libraries) ---------- 49

4- الفصل الرابع: الدراسة المرجعية ---------- 50

4-1- الطرائق الإحصائية (Statistical Methods) ---------- 51

4-1-1- نماذج الخليط الغوسي (Gaussian Mixture Models) ---------- 51

4-1-2- تحليل المكونات المستقلة (Independent Component Analysis) ---------- 51

4-1-3- النماذج القائمة على الانحدار (Regression Model-Based) ---------- 52

4-1-4- تحليل المكونات الرئيسية (Principal Component Analysis) ---------- 52

4-2- طرائق تعلم الآلة (Machine Learning Methods) ---------- 53

4-2-1- تقنيات كشف الشذوذ القائمة على التصنيف ---------- 53

4-2-2- تقنيات كشف الشذوذ القائمة على أقرب جار ---------- 55

4-2-3- تقنيات كشف الشذوذ القائمة على التجميع ---------- 56

4-2-4- النماذج الهجينة الكلاسيكية (Classic Hybrid Model) ---------- 56

4-3- طرائق التَعلُّم العميق (Deep Learning Methods) ---------- 58

4-3-1- طرائق تَعَلُّم التَمْثيلات الطبيعية (Learning Representations of Normality) --- 59

4-3-2- النماذج الهجينة العميقة (Deep Hybrid Model) ---------- 63

5- الفصل الخامس: تحليل أنظمة كشف الشذوذ ---------- 67

5-1- منهجية التحليل (Analysis Methodology) ---------- 67

5-2- بناء نظام الكشف (Detection System Creation) ---------- 74

6- الفصل السادس: نظام كشف الشذوذ المقترح ---------- 75

6-1- شبكة الترميز الآلي مع عتبة ديناميكية (Overall Procedure of AEDT) ---------- 75

6-2- النظام المقترح (Proposed System) ---------- 79

6-3- واجهة النظام(System GUI) ---------- 84

7- الفصل السابع: النتائج والمناقشة ---------- 88

7-1- تحليل أنظمة كشف الشُذُوذ الكلاسيكية---------- 88
7-1-1- تحليل أداء خوارزمية الغابات العشوائية في اكتشاف الشُّذُوذ ---------- 88
7-1-2- تحليل أداء خوارزمية آلة شعاع الدعم في اكتشاف الشُّذُوذ ---------- 96
7-2- نظام كشف الشُّذُوذ الْمُقْتَرَح (Proposed Anomaly Detection System) -------- 104
7-2-1- حالة النظام بدون ذاكرة AEDT-ADS ---------- 105
7-2-2- حالة النظام مع ذاكرة AEDTM-ADS ---------- 114
7-2-3-مقارنة أداء نظام كشف الشُّذُوذ الْمُقْتَرَح مع الأنظمة الأخرى---------- 130
8- الفصل الثامن: الخاتمة والدراسات المستقبلية ---------- 132
8-1- الخاتمة والاستنتاجات ---------- 132
8-2- الدراسات المستقبلية ---------- 137
9- قائمة المراجع ---------- 138

الملخص

يَتَأَثَّر تَحْلِيل البيانات في المجالات التطبيقية كافةً بالبيانات الشَّاذَّة التي يُمكن أَنْ تُؤثّر على نحوٍ أو آخر إلى شيء خارج نطاق البيانات الطبيعية. يُوجَد إسقاط كبير لمفهوم اكتشاف الشُّذُوذ ضِمْنَ تطبيقات العالم الحقيقي مثل اكتشاف العمليات الاحتيالية والعيوب الصناعية والاختراقات الشَّبَكِيَّة؛ وهذا ما يدعو إلى الحاجة إلى الاهتمام على نحوٍ أو آخر بالكشف عن تلك الحالات.

تَحْتَاج عَمَلِيَّة الكشف عن الحالات الشَّاذَّة إلى أساليب وأَنْظِمَة قَادِرَة عَلَى التَّعَامُل مَعَ التَّحَدِّيَاتِ الَّتِي تَفْرِضُهَا طبيعة المسألة وبخاصّة الْمُتَمَثِّلَة فِي الشُّحّ الْكَبِيرِ بِعَدَدِ الْحَالَاتِ الشَّاذَّة، وَتَكَيُّف السُّلُوكِ الشَّاذّ مَعَ السُّلُوكِ الطَّبِيعِيّ فِي بَعْضِ الْأَحْيَان، وَالْكَثِير مِنَ الْمُعَوِّقَات الْأُخْرَى الَّتِي تَجْعَل عَمَلِيَّةَ الْكَشْف عَمَلِيَّةً مُعَقَّدَةً، عَلَى عَكْسِ تِلْكَ الْمَجَالَاتِ الَّتِي تكون فِيهَا الْأَنْمَاط مُنْتَظِمَةً وَوَاضِحَةً.

يُوجَد الْعَدِيد مِنْ أَنْظِمَةِ كَشْف الشُّذُوذ الْمَعْمُولِ بِهَا حَالِيَّاً، إِلَّا أَنَّ الْأَنْظِمَة الْقَائِمَة عَلَى طَرَائِقِ التَّعَلُّمِ الْعَمِيق هِي الْأَكْثَر فَعَالِيَة لَما تَلْعَبه مِنْ دَوْرٍ مُهِمّ فِي التَّخْفِيفِ مِنْ آثَارِ التَّحَدِّيَاتِ الْمُرْتَبِطَةِ بِعَمَلِيَّةِ الْكَشْف، وَأَهَمُّهَا كَشْف الشُّذُوذ فِي الْبَيَانَاتِ عَالِيةِ الْأَبْعَاد. وَعَلَى الرَّغْم مِنْ ذَلِكَ، تُوَاجِه هَذِهِ الْأَنْظِمَة مَجْمُوعَةً مِنَ الصُّعُوبَاتِ الَّتِي تَحُدُّ مِنْهَا، مِثْل دِرَاسَة الْمِيْزَات الْأَكْثَر أَهَمِّيَّةً فِي اِكْتِشَافِ الشُّذُوذ، وَاِخْتِيَار قِيَم البارامترات الْفَائِقَة الْأَفْضَل؛ إِضَافَةً إِلَى دِرَاسَةِ تَوْزِيعِ الْبَيَانَات وَتَحْدِيد عَتَبَة التصنيف (الْكَشْف) لِفَصْلِ الْبَيَانَاتِ الطَّبِيعِيَّةِ عَنِ الْبَيَانَاتِ الشَّاذَّة على نحوٍ دينَاميكِي، وَأَخِيراً وَلَيْسَ آخراً تَنَوُّعُ الْحَالَات الشَّاذَّة.

تَتَلَخَّصُ الْمُسَاهَمَةُ الْمُقَدَّمَةُ ضِمْنَ هَذِه الدِّرَاسَة فِي ثَلاثة اِتِّجَاهَاتٍ: **الاتجاه الأول**، تَحْلِيل أَنْظِمَة كَشْف الشُّذُوذ بِهَدَفِ دِرَاسَة كَفَاءة هَذِه الْأَنْظِمَة مِنْ حَيْث زَمَنُ التَّدْرِيب وَنِسْبَةُ الْكَشْف. تَوَصَّلَت الدِّرَاسَة إِلَى أَنَّ أَفْضَل أَدَاء لِأَنْظِمَةِ كَشْف الشُّذُوذ يكون عِنْدَ اِخْتِيَار الْمَيْزَات الْأَكْثَر أَهَمِّيَّةً مَتْبُوعاً بِضَبْطِ البارامترات الْفَائِقَة. فَقَدْ سَاهَمَ اِسْتِخْدَام التَّرْتِيب الْمُحَدَّد عَلَى عَدَدٍ مِنَ الْأَنْظِمَة فِي تَقْلِيصِ كُلٍّ مِنَ الزَّمَنِ الْمُسْتَغْرَقِ لبنَائِهَا بِنِسَبٍ تَتَرَاوَحُ بَيْنَ **51.5%** و**60.2%**، ومعدل الإيجابيات الخاطئة (FPR) بين **1%** و**35%**، بالإضافة إلى زيادة في كشف الحالات الشَّاذَّةِ بَيْنَ **1%** و**6%** وذلك بالنظر إلى مساحة السطح تحت منحني الدقة والاسترجاع (AUCPR)، كما أنّ هناك تَحسِين في مُعْظَمِ قِيَمِ مقاييس الأداء.

الاتجاه الثاني، بِنَاءُ نِظَامٍ مُتَكَامِلٍ لِكَشْف الشُّذُوذ فِي الْبَيَانَاتِ قَادِرٍ عَلَى تَجَاوُزِ أَهُمِ التَّحَدِّيَات الَّتِي تَوَاجه أَنْظِمَة الْكَشْف الْحَالِيَّة. اِقْتَرَحَتِ الدِّرَّاسَة نَظَّام كَشْفِ الشُّذُوذِ AEDT(M)–ADS وهو اختصار لـ : **A**uto–**E**ncoder with a **D**ynamic **T**hreshold (LST**M**)– **A**nomaly **D**etection **S**ystem.

يَعْتَمِد نِظَام كَشْف الشُّذُوذ الْمُقْتَرَح عَلَى شَبَكَة الترميز الْآلِي مَعَ عَتَبَة ديناميكِيَّة (AEDT) الْمُقْتَرَحَةِ ضِمْنَ الدِّرَاسَة، وَهِي نُسْخَةٌ مُعَدَّلَةٌ مِنْ شَبَكَةِ الترميز الْآلِي التَّقليدِيَّة بِإِضَافَةِ مَرَاحِلَ تُعَزِّز مِنْ آلِيَّةِ الْاِكْتِشَاف وَتُحَدِّدُ عَتَبَة التصنيف المُتَغَيِّرَة بِمُرُورِ الْوَقْتِ على نحوٍ ديناميكِي. كَمَا أَنَّ الْهَدَف مِنْ إِمْكَانِيَّةِ إِضَافَةِ وحدة الذَّاكِرَة قصيرة طَوِيلَة الْمُدَى (LSTM) هُوَ اِلْتِقَاط التَّبعيَات الزَّمَنِيَّة لِتَسَلْسُلِ الشُّذُوذ خِلَالَ فَتْرَةٍ زَمَنِيَّةٍ مُعَيَّنَةٍ، وَاِكْتِشَافُهَا قَبْلَ حُدوثِهَا بِوَقْتٍ مُنَاسِبٍ.

يَتَمَتَّع النِّظَام الْمُقْتَرَح بِقُدْرَتِهِ عَلَى اِكْتِشَافِ الْمِيْزَات غَيْر الْمُرْتَبِطَة خَطّياً، وَتَحْدِيدِ عَتَبَة التصنيف على نحوٍ ديناميكِي، وَمُعَالَجَة أَنْوَاع الشُّذُوذ الْمُخْتَلِفَة. كَمَا اِسْتَطَاعَ النِّظَام عِنْدَ إِسْقَاطِهِ عَلَى تَطْبِيقَاتٍ حَقِيقِيَّةٍ التَّفَوُّقَ عَلَى أَنْظِمَةِ كَشْف الشُّذُوذ الْأُخْرَى. فَقَدِ اِرْتَفَعَتْ نِسْبَةُ الْكَشْف عَنِ الشُّذُوذ (الْعَمَلِيَاتِ الْاِحْتِيَالِيَّة) ضِمْنَ المُنَاقَلَات المَالِيَّة الأوروبية بِمِقْدَار **2%** إلى **36%** مُقَارَنَةً بِبَاقِي الْأَنْظِمَة وَذَلِكَ بِالنَّظَر إِلَى مِقْيَاس الاِسْتِرْجَاع (Recall). كَذَلِكَ اِرْتَفَعَتْ نِسْبَة الْكَشْف عَنِ الْحَالَاتِ الشَّاذَّة (كَسر الْوَرَقِ) فِي مُعَامِل اللُّبّ وَالْوَرَق قَبْل حُدوثِهَا بِوَقْتٍ مُنَاسِبٍ بِمِقْدَار **27%** على الأقل. أَضِفْ إِلَى ذَلِكَ أَنَّ جَمِيعَ الْأَنْظِمَة الْحَالِيَّة تَسْتَخْدِم عَتَبَة تَصْنِيف ثَابتة، عَلَى عَكْسِ النِّظَام الْمُقْتَرَح الَّذِي يَسْتَخْدِم عَتَبَة ديناميكِيَّة. مِمَّا يُؤَكِّدُ عَلَى تَفَوُّقِ النِّظَام الْمُقْتَرَح عَلَى بَاقِي الْأَنْظِمَةِ الْأُخْرَى.

الاتجاه الثالث، تَطْوِيرُ وَاجِهَاتٍ تَخَاطُبِيَّةٍ لِلنِّظَام الْمُقْتَرَح لِبَيَانِ إِمْكَانِيَّةِ اِسْتِثْمَارِهِ مُبَاشرَةً فِي أَيِّ تَطْبِيقٍ مِنْ تَطْبِيقَاتِ الْعَالَمِ الْحَقِيقِيّ بَعْدَ مُلَاءَمَتِهِ لِيُنَاسِب الْبَيَانَاتِ الْمُدْخَلَةِ.

الكلمات المفتاحية: البيانات الشاذة، كشف الشذوذ، أنظمة كشف الشذوذ، التعلم العميق، الميزات، البارامترات الفائقة، عتبة التصنيف، شبكة الترميز الآلي مع عتبة ديناميكية، الذاكرة قصيرة طويلة المدى.

Abstract

Data analysis in various application fields is affected by anomalous data that can, in one way or another, point to something outside the normal data range. There is a major projection of the concept of anomaly detection within real-world applications such as fraud detection, industrial defects, and network intrusions; This calls for the need to pay attention, in one way or another, to the detection of such cases.

The process of detecting anomalies requires methods and systems capable of dealing with the challenges posed by the nature of the issue, especially the great rarity in the number of anomalies, the adaptation of anomalous behavior to normal behavior, and many other obstacles that make detection a complex process. Unlike those areas where patterns are uniform and clear.

There are many current anomaly detection systems in place, but systems based on deep learning methods are the most effective, as they play an important role in mitigating the challenges associated with detection, the most important of which is the detection of anomalies in high-dimensional data. However, these systems face a range of difficulties, such as selecting the most important features of anomaly detection and selecting the best hyperparameter values; In addition to the study of data distribution and the determination of a classification threshold (detection) to dynamically separate normal data from anomalous data, and last but not least the diversity of anomalies.

The contribution made in this study is summarized in three directions: **The first direction** is the analysis of anomaly detection systems to study the efficiency of these systems in terms of training time and detection rate. The study concluded that the best performance of anomaly detection systems is when the selection of the most important features is followed by setting the hyperparameters. The use of the specified arrangement on a number of systems has reduced both the time taken to build them by **51.5**% to **60.2%,** the FPR rate between **1%** and **35%,** and an increase in anomalies detection between **1%** and **6%**, given the surface area under the accuracy and retrieval curve (AUCPR), there is also an improvement in most performance metrics' values.

The second direction is to build an integrated system for anomaly detection in data capable of overcoming the most important challenges facing existing detection systems. This study proposed AEDT(M)-ADS, an abbreviation for **A**uto-**E**ncoder with a **D**ynamic **T**hreshold (LST**M**)- **A**nomaly **D**etection **S**ystem. The proposed anomaly detection system is based on the autoencoder network with a dynamic threshold (AEDT) proposed within the study, a modified version of the traditional autoencoder network with additional stages that enhance the detection mechanism and dynamically determine the variable rating threshold over time. The goal of the LSTM capability is to capture the time dependencies of the anomaly sequence within a given period and detect it in time before it occurs.

The proposed system can detect features that are not linearly correlated, dynamically determine a classification threshold, and handle different anomalies. When applied on real applications, the system also outperformed other anomaly detection systems. In European financial transfers, anomalies (fraudulent transactions) detected

were up **2%** to **36%**, compared to other systems, given the recall metric. The detection rate of anomalies (paper breakage) in pulp and paper mills has also risen by at least **27%** in advance of their occurrence. In addition, all current systems use a fixed classification threshold, as opposed to the proposed system which uses a dynamic threshold. This confirms the superiority of the proposed system over other systems.

The third direction, develop user interfaces to the proposed system to show that it can be directly invested in any real-world application after it is adapted to fit the input data.

Keywords: Anomalous Data - Anomaly Detection – Anomaly Detection Systems – Deep Learning – Features – Hyperparameter – Classification Threshold – Autoencoder with Dynamic Threshold – Long Short-Term Memory.

قائمة الأشكال List of Figures

الشكل 1-1 توزيع الحالات الشَّاذَّة ---------- 1
الشكل 1-2 تأثير أبعاد البيانات على كشف الشُّذُوذ ---------- 4
الشكل 1-3 الشُّذُوذ العام والمحلي- تحديات الطرائق الإحصائية ---------- 5
الشكل 1-4 طرائق تَعلُّم الآلة المستخدمة في كشف الشذوذ ---------- 6
الشكل 1-5 طرائق إعادة تكوين العينات ---------- 8
الشكل 1-6 تصنيف طرائق التَّعَلُّم الْعَمِيق الْمُسْتَخْدَمَة في كشف الشُّذُوذ – وتَحَدِّيَاتِ الكشف الَّتِي تَعَالُجِهَا كُلَّ طريقة ---------- 11
الشكل 2-1 مصنف غابة عشوائية ---------- 16
الشكل 2-2 فصل البيانات خطياً باستخدام المستوي الفائق ---------- 19
الشكل 2-3 مجموعة بيانات غير قابلة للفصل خطياً ---------- 20
الشكل 2-4 تصنيف آلة شعاع الدعم لبيانات غير قابلة للفصل خطياً ---------- 20
الشكل 2-5 مبدأ عمل نواة RBF ---------- 21
الشكل 2-6 تأثير التنظيم ضمن آلة شعاع الدعم في تصنيف البيانات ---------- 22
الشكل 2-7 معمارية شبكة الترميز الآلي ---------- 24
الشكل 2-8 بنية الذاكرة قصيرة طويلة المدى ---------- 28
الشكل 2-9 آلية عمل شبكة LSTM-Autoencoder ---------- 31
الشكل 3-1 مصفوفة الارتباك ---------- 35
الشكل 3-2 حالات منحني ROC ---------- 40
الشكل 3-3 حالات منحني PR ---------- 41
الشكل 3-4 التوزيع التراكمي النظري والتجريبي للبيانات ---------- 45
الشكل 4-1 تصنيف طرائق كشف الشذوذ. المصدر: الدراسة الحالية ---------- 50
الشكل 5-1 منهجية التحليل المقترحة. المصدر: الدراسة الحالية ---------- 68
الشكل 5-2 استخدام 10-Fold cross validation في تدريب المصنفات ---------- 69
الشكل 5-3 خطوات بناء نظام كشف الشذوذ بالاعتماد على نتائج التحليل ---------- 74
الشكل 6-1 إجرائية شبكة AEDT المقترحة. المصدر: الدراسة الحالية ---------- 77
الشكل 6-2 نظام كشف الشذوذ المقترح. المصدر: الدراسة الحالية ---------- 78
الشكل 6-3 الكشف المبكر بإزاحة نقطة البيانات إلى الأعلى بمقدار 1 ---------- 81
الشكل 6-4 الواجهة الرئيسية لنظام كشف الشذوذ المقترح ---------- 85

الشكل 6-5 ضبط إعدادات النظام- تحديد خوارزمية الكشف ---------- 85
الشكل 6-6 ضبط إعدادات النظام- استيراد تدفقات البيانات الحالية ---------- 86
الشكل 6-7 تحديد حالة الدخل الحالي- حالة طبيعية ---------- 86
الشكل 6-8 تحديد حالة الدخل الحالي- حالة شاذة ---------- 87
الشكل 7-1 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام الغابات العشوائية وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات الأوروبية) ---------- 92
الشكل 7-2 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام الغابات العشوائية وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات المجردة) ---------- 95
الشكل 7-3 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام آلة شعاع الدعم وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات الأوروبية) ---------- 99
الشكل 7-4 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام آلة شعاع الدعم وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات المجردة) ---------- 102
الشكل 7-5 مقارنة أداء خوارزمية الغابات العشوائية وآلة شعاع الدعم في اكتشاف الشُذُوذ – حالة البيانات الأوروبية ---------- 103
الشكل 7-6 مقارنة أداء خوارزمية الغابات العشوائية وآلة شعاع الدعم في اكتشاف الشُذُوذ – حالة البيانات المجردة ---------- 104
الشكل 7-7 العلاقة بين نوع المعاملة وكمية المبلغ المصروف ---------- 105
الشكل 7-8 العلاقة بين نوع المعاملة ووقت حدوثها ---------- 115
الشكل 7-9 تأثير حجم النافذة الزمنية على أداء AEDTM-ADS – البيانات الأوروبية ---------- 119
الشكل 7-10 تأثير حجم النافذة الزمنية على أداء AEDTM-ADS – بيانات كسر الورق---------- 128
الشكل 7-11 مقارنة أداء AEDT(M)-ADS بالأنظمة الأخرى – البيانات الأوروبية ---------- 130
الشكل 7-12 مقارنة أداء AEDT(M)-ADS بالأنظمة الأخرى – بيانات كسر الورق ---------- 131

قائمة الجداول List of Tables

الجدول 3-1 وصف بيانات الاحتيال الأوروبية ---------- 42
الجدول 3-2 وصف بيانات الاحتيال المجردة ---------- 43
الجدول 3-3 وصف بيانات كسر الورق---------- 44
الجدول 4-1 تقنيات كشف الشذوذ القائمة على تَعلُّم الآلة ---------- 57
الجدول 4-2 مقارنة بين طرائق الكشف العميقة والكلاسيكية ---------- 65
الجدول 5-1 الأهمية النسبية لميزات مجموعة بيانات الاحتيال الأوروبية ---------- 71
الجدول 5-2 الأهمية النسبية لميزات مجموعة بيانات الاحتيال المجردة ---------- 71
الجدول 5-3 مجال القيم لبارامترات الغابة العشوائية ---------- 73
الجدول 5-4 مجال القيم لبارامترات آلة شعاع الدعم---------- 73
الجدول 6-1 مجال قيم البارامترات الفائقة لخوارزميةAEDT ---------- 82
الجدول 6-2 مجال قيم البارامترات الفائقة لخوارزمية LSTM-AEDT ---------- 82
الجدول 7-1 نتائج البحث العشوائي لبارامترات الغابة العشوائية – السيناريو الأول (البيانات الأوروبية) --- 89
الجدول 7-2 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات الأوروبية – السيناريو الأول---------- 89
الجدول 7-3 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الأول---------- 89
الجدول 7-4 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني ---------- 90
الجدول 7-5 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الثاني (البيانات الأوروبية) -- 91
الجدول 7-6 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني ---------- 91
الجدول 7-7 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الأول (البيانات المجردة) --- 92
الجدول 7-8 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المجردة – السيناريو الأول ---------- 93
الجدول 7-9 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الأول ---------- 93
الجدول 7-10 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني ---------- 94

الجدول 7-11 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الثاني (البيانات المجردة) -- 94
الجدول 7-12 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني ---------- 95
الجدول 7-13 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الأول (البيانات الأوروبية) -- 96
الجدول 7-14 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات الأوروبية – السيناريو الأول---------- 96
الجدول 7-15 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الأول---------- 97
الجدول 7-16 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني ---------- 98
الجدول 7-17 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الثاني (البيانات الأوروبية) -- 98
الجدول 7-18 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني ---------- 98
الجدول 7-19 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الأول (البيانات المجردة) -- 100
الجدول 7-20 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المجردة – السيناريو الأول ---------- 100
الجدول 7-21 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الأول ---------- 100
الجدول 7-22 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني ---------- 101
الجدول 7-23 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الثاني (البيانات المجردة)-- 101
الجدول 7-24 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني ---------- 102
الجدول 7-25 نتائج البحث العشوائي لشبكة AEDT – حالة البيانات الأوروبية---------- 106
الجدول 7-26 بنية شبكة AEDT – البيانات الأوربية ---------- 106
الجدول 7-27 حجم مساهمة الميزات في أداء النظام - أهمية ميزات البيانات الأوروبية---------- 107
الجدول 7-28 نتائج اختبار كولموغوروف سميرنوف – البيانات الأوروبية ---------- 107
الجدول 7-29 نتائج أداء AEDT-ADS – البيانات الأوروبية ---------- 108
الجدول 7-30 نتائج البحث العشوائي لشبكة AEDT – حالة بيانات كسر الورق ---------- 110
الجدول 7-31 بنية شبكة AEDT – بيانات كسر الورق ---------- 110

الجدول 7-32 حجم مساهمة الميزات في أداء النظام - أهمية ميزات بيانات كسر الورق ---------- 111
الجدول 7-33 نتائج اختبار كولموغوروف سميرنوف – بيانات كسر الورق---------- 111
الجدول 7-34 نتائج أداء AEDT-ADS – بيانات كسر الورق---------- 112
الجدول 7-35 تحليل التكلفة والفائدة لنظام AEDT-ADS- بيانات كسر الورق ---------- 114
الجدول 7-36 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 3$ – البيانات الأوروبية ---------- 115
الجدول 7-37 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 5$ – البيانات الأوروبية ---------- 116
الجدول 7-38 بنية شبكة LSTM-AEDT – البيانات الأوروبية ---------- 116
الجدول 7-39 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 3$ – البيانات الأوروبية -------- 117
الجدول 7-40 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 5$ – البيانات الأوربية --------- 118
الجدول 7-41 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 3$ – بيانات كسر الورق ---------- 120
الجدول 7-42 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 5$ – بيانات كسر الورق ---------- 121
الجدول 7-43 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 7$ – بيانات كسر الورق ---------- 121
الجدول 7-44 نتائج البحث العشوائي لشبكة LSTM-AEDT عند حجم نافذة $m = 9$ – بيانات كسر الورق ---------- 122
الجدول 7-45 بنية شبكة LSTM-AEDT – بيانات كسر الورق ---------- 122
الجدول 7-46 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 3$ – بيانات كسر الورق-------- 123
الجدول 7-47 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 5$ – بيانات كسر الورق-------- 124
الجدول 7-48 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 7$ – بيانات كسر الورق-------- 126
الجدول 7-49 نتائج أداء AEDTM-ADS عند حجم نافذة $m = 9$ – بيانات كسر الورق-------- 127
الجدول 7-50 تحليل التكلفة والفائدة لنظام AEDTM-ADS- بيانات كسر الورق ---------- 129

List of Terms قائمة المصطلحات

-A-

Accuracy	الدقة
Accuracy Paradox	تناقض الدقة
Activation Function	تابع التنشيط
Area Under the Curve	مساحة السطح تحت المنحني
Attention Machine	آلة الانتباه
Autoencoder Network	شبكة الترميز الآلي
Autoencoder with a Dynamic Threshold	شبكة الترميز الآلي مع عتبة ديناميكية
Anomaly	الشذوذ
Anomaly Detection	كشف الشذوذ
Anomaly Detection System	نظام كشف الشذوذ
Analysis Methodology	منهجية التحليل
Anomaly Score Learning	التعلم القائم على درجة الشذوذ

-B-

Backpropagation	الانتشار الخلفي
Bagging	التعبئة
Batch Size	حجم الدفعة

-C-

Categorical Data Encoding	ترميز البيانات الفئوية
Candidate Combinations	التكوينات المرشحة
Cell State	حالة الخلية
Chebyshev's Theory	نظرية تشيبيشيف
Chi-Square	مربع كاي
Classification	التصنيف
Clustering	التجميع
Collective Anomalies	الشذوذ الجماعي
Combination	توليفة

Confusion Matrix	**مصفوفة الارتباك**
Contextual Anomalies	**الشذوذ في السياق**
Convolutional Neural Networks	**الشبكات العصبونية الالتفافية**
Cross Validation	**التحقق من الصحة المتقاطع**

–D–

Data Imbalance	**بيانات غير المتوازنة**
Data Instance	**مثيل البيانات**
Dataset	**مجموعة البيانات**
Standardization Data	**تَقيِيس البيانات**
Decision Trees	**أشجار القرار**
Decision Nodes	**عقدة الحذر**
Decoder	**مفكك الترميز**
Deep Learning	**التعلّم العميق**
Detection Time	**زمن الكشف**
Dimension Reduction	**تقليل الأبعاد**
Dropout Rate	**معدل التسريب**
Dynamic Threshold	**عتبة ديناميكية**

–E–

Eigenvectors	**المتجهات الذاتية**
Embedded Methods	**طرائق التضمين**
Empirical Cumulative Distribution	**التوزيع التراكمي التجريبي**
Empirical Rule	**القاعدة التجريبية**
Ensemble Technique	**تقنيات التجميع**
Encoder	**المُرَمِّز**
Epoch	**حقبة**

–F–

Failure Rate	**معدل الفشل**
False Negatives	**السلبيات الخاطئة**
False Positives	**الإيجابيات الخاطئة**
Features	**الميزات**

Feature Engineering	**هندسة الميزات**
Features Extraction	**استخراج الميزات**
Feature Importance	**أهمية الميزة**
Feature Reduction	**اختزال الميزات**
Feature Selection	**اختيار الميزات**
Feed-Forward	**تغذية متقدمة**
Filter Methods	**طرائق التصفية**
Forget Gate	**بوابة النسيان**
Fully-Connected Network	**شبكة متصلة بالكامل**
Forget Gate	**بوابة النسيان**

-G-

Gated Recurrent Units	**الوحدة المتكررة ذات البوابات**
Gaussian Mixture Models	**نماذج الخليط الغاوسي**
Generative Adversarial Networks	**شبكات الخصومة التوليدية**
Genetic Algorithm	**الخوارزمية الجينية**
Gini Impurity	**شائبة جيني**
Graphic Metrics	**المقاييس البيانية**
Grid Search	**البحث الشبكي**

-H-

High Dimension Data	**البيانات عالية الأبعاد**
Hybrid Models	**النماذج الهجينة**
Hyperparameter	**البارامترات الفائقة**
Hyperparameter Tuning	**ضبط البارامترات الفائية**
Hyperplane	**المستوي الفائق**

-I-

Impurity Nodes	**العقد الشائبة**
Independent Component Analysis	**تحليل المكونات المستقلة**
Information Gain	**ربح المعلومات**
Input Gate	**بوابة الإدخال**

-K-

Kernel	**نواة**
Kolmogorov-Smirnov test	**اختبار كولموغوروف سميرنوف**

-L-

Label Encoding	**ترميز التسمية**
Latent Space	**الفضاء الكامن**
Latent Variables	**المتغيرات الكامنة**
Leaf Nodes	**العقد الورقية**
Learning Rate	**معامل التعلّم**
Learning Representations of Normality	**تعلم التمثيلات الطبيعية**
Likelihood Models	**النماذج الاحتمالية**
Separable Linearly	**قابلية الفصل الخطي**
Local Outlier Factor	**المعامل الخارجي المحلي**
Logistic Regression	**الانحدار اللوجستي**
Loss Function	**تابع الخسارة**

-M-

Machine Learning	**التعلّم الآلي**
Magnitude Measures	**مقياس الحجم**
Majority Class	**صف الأغلبية**
Majority Voting	**تصويت الأغلبية**
Mean Squared Error	**متوسط الخطأ التربيعي**
Minority Class	**صف الأقلية**
Missing Values	**القيم مفقودة**
Multivariate	**متعددة المتغيرات**

-N-

Nearest Neighbor	**أقرب جار**
Neural Networks	**الشبكات العصبية**
Nodes	**عقد**
Nonparametric Tests	**اختبارات غير معلميه**
Normal Distribution	**التوزيع الطبيعي**

-O-

One Class Models	**نماذج الصف الواحد**
Output Gate	**بوابة الإخراج**
Overfitting	**الملائمة الزائدة**
Oversampling	**توسيع العينات**

-P-

Parametric Tests	**اختبارات معلميه**
Particle Swarm Optimization	**تحسين عناصر السرب**
Performance Evaluation	**تقييم الأداء**
Performance Metrics	**مقاييس الأداء**
Point Anomalies	**شذوذ نقطة**
Precision	**الدقة**
Precision-Recall Curves	**منحنيات الدقة والاسترجاع**
Preprocessing	**المعالجة المسبقة**
Principal Component Analysis	**تحليل المكونات الرئيسية**
Prior-Driven Models	**النماذج المشتقة مسبقاً**
Probability Distribution	**التوزيع الاحتمالي**

-R-

Random Forest	**الغابات العشوائية**
Random Search	**البحث العشوائي**
Ranking Models	**نماذج الترتيب**
Recall	**الاسترجاع**
Receiver Operating Characteristic	**خصائص المستقبل التشغيلية**
Reconstruction Error	**خطأ إعادة البناء**
Recurrent Neural Networks	**الشبكات العصبونية التكرارية**
Regression Model-Based	**النماذج القائمة على الانحدار**
Regularization	**التنظيم**
Relative Importance	**الأهمية النسبية**
Resampling	**إعادة تكوين العينات**
Restricted Boltzmann Machine	**آلة بولتزمان المقيدة**

Root Node	**عقدة الجذر**

–S–

Supervised Learning	**التعلّم بإشراف**
Support Vector Machine	**آلة شعاع الدعم**
Semi–Unsupervised Learning	**تعلم شبه خاضع للإشراف**
Statistical Methods	**الطرائق الإحصائية**
Sequential Data	**البيانات المتسلسلة**
Statistical Metrics	**المقاييس الإحصائية**
Statistical Tests	**الاختبارات الإحصائية**
Significance Level	**معامل الثقة**
Sparse Autoencoder	**شبكة الترميز الآلي المتناثرة**
Sparsity Penalty	**عقوبة التناثر**
Stacked Autoencoder	**شبكة الترميز الآلي المكدسة**
Sliding Window	**النوافذ المنزلقة**
Split the Data	**تقسيم البيانات**

–T–

Temporal Dependencies	**التبعيات الزمنية**
Time Series	**سلال زمنية**
Transfer Learning	**نقل التعلم**
Theoretical Cumulative Distribution	**التوزيع التراكمي النظري**
Time Window Processing	**معالجة النوافذ الزمنية**
Threshold Tradeoff	**تفاضل العتبة**
True Positives	**الإيجابيات الحقيقية**
True Negatives	**السلبيات الحقيقية**
Training Set	**مجموعة التدريب**
Testing Set	**مجموعة الاختبار**

–U–

Unsupervised Learning	**التعلّم بدون إشراف**
Under–Sampling	**تقليص العينات**
Undercomplete Autoencoder	**شبكة الترميز الآلي غير المكتملة**

–V–

Validation Set	**مجموعة التحقق**

–W–

Wrapper Method	**طرائق التغليف**

List of Acronyms قائمة الاختصارات

(ADS)	Anomaly Detection System
(ADT)	Anomaly Detection Techniques
(AE)	Auto-Encoder
(AEDT)	Autoencoder with a Dynamic Threshold
(AEDTM-ADS)	AEDT LSTM - Anomaly Detection System
(AM)	Attention Machine
(AUC)	Area Under the Curve
(AUROC)	Area Under The ROC
(CNN)	Convolutional Neural Networks
(CV)	Cross Validation
(DL)	Deep Learning
(DLN)	Deep Learning Networks
(DT)	Decision Trees
(FDS)	Fraud Detection System
(FN)	False Negatives
(FP)	False Positives
(FPR)	False Positive Rate
(GAN)	Generative Adversarial Networks
(KNN)	K-Nearest Neighbor
(LOF)	Local Outlier Factor
(LSTM)	Long Short-Term Memory Networks
(MCC)	Matthews Correlation Coefficient
(ML)	Machine Learning
(MSE)	Mean Squared Error
(NN)	Neural Networks
(PCA)	Principal Component Analysis
(RBF)	Radial Basis Function
(RBM)	Restricted Boltzmann Machine
(ReLU)	Rectified Linear Activation
(RNN)	Recurrent Neural Networks

(ROC)	**Receiver Operating Characteristic**
(SVM)	**Support Vector Machine**
(Tanh)	**Hyperbolic Tangent**
(TN)	**True Negatives**
(TP)	**True Positives**

الفصل الأول

المقدمة

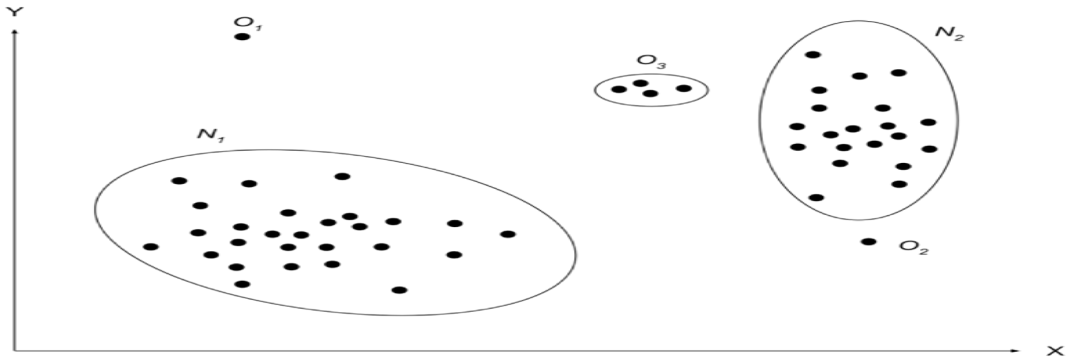
نتيجة ازدياد كَمِ البيانات الْمُتَوَافِرِ فِي كُلّ مكان على نحوٍ كبير في الآونة الأخيرة (حيث من المتوقع أن يصل إنتاج البيانات إلى Zettabytes +200 بحلول عام 2025) [1]، أَصْبَحَ الحاجةُ ضروريةً لتحليل مجموعات البيانات في العالم الحقيقي بأشكالها كافةً، وَاِسْتِخْرَاج أنماط البيانات الْخَفِيَّة وَالْمُعَقَّدَة، لاستخدامها في العديد من المجالات المُختَلِفة.

يَتَأَثَّرُ تَحْلِيل البيانات في مُخْتَلِف المجالات التطبيقية بالبيانات الشَّاذَّة التي يُمكن أَنْ تشير على نحوٍ أو آخر على شيء خارج نطاق البيانات الطبيعية، ومن ثَمَّ فالتحليل السليم للبيانات للحصول على المعلومات الصحيحة والدقيقة والمعبرة عن الحالة الطبيعية يجب أن يُمَيِّز بين البيانات الطبيعية وغير الطبيعية. وهذا ما يدعو إلى الحاجة إلى الاهتمام على نحوٍ أو آخر بالكشف عن الشُّذُوذ.

1-1- الشُذُوذ (Anomaly)

لا يوجد تعريف موحّد لِلشُّذُوذ ولهذا السبب اِعتَمَدَت الدراسة على التعريف الآتي الذي يُعْتَبر الأكثر استخداماً وقرباً مِنْ مَفْهُومِهَا. الشُّذُوذ هو مجموعة أنماط البيانات التي لا تَتَوَافق على نحوٍ جيد مع السلوك الطبيعي للبيانات [2].

لِتَوْضِيح مفهوم الشُّذُوذ على نحوٍ بسيط، يُمْكِنُ دِرَاسَة مجموعة من نقاط البيانات التي تَقَع ضِمْنَ جملة الإحداثيات الثنائية الآتية.



الشكل 1-1 توزيع الحالات الشَّاذَّة

تُعْتَبِر المجموعتان $N1, N2$ مناطق ذات بيانات طبيعية، لأن غالبية الملاحظات تَقَع ضِمْنَ هذه المناطق. بينما تُعدّ النقاط $o1, o2$ حالات شَاذَّة، لأنها تَبتَعِد عن مناطق توزيع البيانات الطبيعية (تَسْلُك سلوكاً مغايراً للبيانات الطبيعية).

1-2- أنواع الشُّذُوذ (Types of Anomalies)

يوجد أنواع مختلفة للشُّذُوذ [2]، لكنها تُصَنَّف على نحوٍ رئيسي ثلاثَ فئاتٍ، وهي:

1. **شذوذ النقطة (Point Anomalies)**: يَحْدُث عندما يكون عنصر واحد مختلف تماماً عن جميع العناصر المُتَبَقّيَة. يوجد إسقاط كبير لهذا النوع في العالم الحقيقي، مثل اكتشاف الاحتيال ضِمْنَ بطاقات الائتمان على أساس المبلغ المصروف.
2. **شذوذ السياق (Contextual Anomalies)**: يَحْدُث عندما يَسْلُك العنصر سلوكاً غير طبيعي في سياق محدد. يسمى أيضاً بالشُّذُوذ الشرطي (Conditional Anomaly) ويكون شائعاً في بيانات السلاسل الزمنية. أحد الأمثلة على شذوذ السياق، هو أن إنفاق مبلغ 100 دولار على الطعام يومياً خلال موسم الأعياد أمر طبيعي؛ لكن قد يَبدُو الأمر غريباً خارج الموسم.
3. **الشُّذُوذ الجماعي (Collective Anomalies)**: يَحْدُث عندما تكون مجموعة من العناصر مرتبطٌ بعضُها ببعضٍ، مختلفة تماماً عن باقي العناصر. على سبيل المثال إذا قام شخص بعملية سحب من جهاز الصراف الآلي، فإن هذا السلوك بحد ذاته غير شَاذّ؛ لكن إِذَا تَكَرَّرَتْ عمليات السحب عِدَّةَ مَرَّاتٍ متتالية، فَقَدْ يُنْظَرُ إليها على أنها حالة شَاذَّة.

يَجِبُ التنبيه على أنه يُمكن رَبط جميع الحالات السابقة بعضِها ببعضٍ، بمعنى أنه يُمكن أن يُصبح شُّذُوذ النقطة حالة سياقية إذا طبَقنا عليه مفهوم السياق، ويُمكن أن تُصبح جماعية إذا درسنا مجموعة من النقاط الفردية ضِمْنَ منطقة مُعَيَّنَة.

1-3- تحديات اكتشاف الشُّذُوذ (Anomaly Detection Challenges)

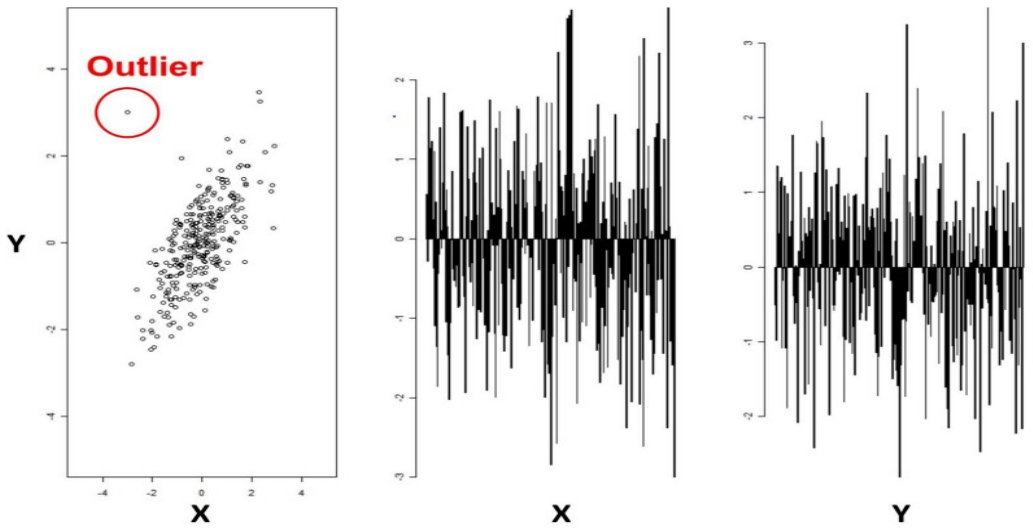
تَهَدف عملية الكشف عن الحالات الشَّاذَّة [3] إلى تَحَديد كُلّ نقاط البيانات التي تَسْلُك سلوكاً مختلفاً عن باقي نقاط المجموعة. يُمْكَنْ أن تَنتُج الحالات الشَّاذَّة عن خطأ في البيانات؛ ولكنها تَدَلّ أيضاً على عمليات أساسية جديدة لم تكن معروفة مسبقاً وغالباً ما تَكَون حرجة في مجموعة واسعة من التطبيقات. يوجد إسقاط كبير لمفهوم اكتشاف الشُّذُوذ في تطبيقات العالم الحقيقي كتطبيقات اكتشاف الاحتيال المالي، والاختراقات الشبكية، والأمراض النادرة، واكتشاف العيوب الصناعية، وغيرها من الأمثلة التي تَدَلّ على أن البيانات الشَّاذَّة تُمَثّل حالات يجب التوقف عندها، ودراسة أسبابها ونتائجها المُحتَمَلة على النظام

الْمَدْرُوس. تُعْتَبِر تلك الحالات جذابة لمحلل البيانات، لذلك يُعدّ اكتشافها عملية مهمة وميزة أساسية في أنظمة صنع القرار.

تُوجَدُ مجموعة من التَّحَدِّيَات [4] التي تَجعَل من عملية اكتشاف الشُّذُوذ عملية مُعَقَّدَة، على عكس تلك المجالات التي تَكَون فيها الأنماط مُنتَظمة وواضحة. يُعالج اكتشاف الشُّذُوذ الأحداث النادرة وغير المتوقعة، وهذا بدوره يؤدي إلى بعض التعقيدات الفريدة الخاصة بالمجال وهي:

1. **نقص المعرفة (Lack of Knowledge)**: تَرْتَبِطُ الحالات الشَّاذَّة بالعديد من الأشياء المجهولة، كالحالات ذات السلوكيات المفاجئة، وتوزيع الحالات الشَّاذَّة التي تَبْقَى غير معروفة حتى تَحَدث فعلاً.
2. **عدم تجانس الشُّذُوذ (Heterogeneous Anomaly)**: قَدْ تَسْلُك بعض حالات الشُّذُوذ سلوكاً مختلفاً تماماً عن الحالات الشَّاذَّة الأخرى.
3. **ندرة وعدم توازن البيانات (Rarity and Data Imbalance)**: تُمثّل الحالات الشَّاذَّة عادةً بيانات نادرة، على عكس الحالات الطبيعية التي غالباً ما تَمثّل النسبة الأكبر من البيانات. ومن ثَمَّ فإنه من المستحيل، جمع كمية كبيرة من الحالات الشَّاذَّة الْمُصَنَّفَة.
4. **تكيّف الأنماط الشَّاذَّة (Adaptation of Anomalous Patterns)**: يَتَكَيَّف في بعض الأحيان السلوك الشَّاذُّ مع السلوك الطبيعي للبيانات، ومن ثَمَّ يُسَبِّب ذلك صعوبة في تَحْديد الحالات الشَّاذَّة واكتشافها.
5. **البيانات عَالِيَّة الْبُعْد (High Dimension Data)**: يُعْتَبِر الكشف عن الحالات الشَّاذَّة في حالة البيانات ثنائية البعد أمراً بسيطاً؛ لكن بالمقابل نَجِد أَنَّهُ لا يمكن تحديد الحالات الشَّاذَّة مباشرةً من خلال فحص متغير واحد (انظر إلى الأشكال في يمين **الشكل 1–2**) حيث يصعب تحديد المجال الطبيعي لقيم المتغير، ومن ثَمَّ تُصْبِح المشكلة أكثر تعقيداً عندما تَتَضَمَّن البيانات عشرات أو مئات المتغيرات، وهذا ما يحدث في كثير من التطبيقات العملية لكشف الشُّذُوذ.
6. **الأنواع المختلفة للشُّذُوذ (Diverse Types of Anomaly)**

يوجد مجموعة متنوعة من أنماط الشذوذ والتي ذُكِرَت سابقاً، وهي شذوذ النقطة وشذوذ السياق والشذوذ الجماعي.



الشكل 1-2 تأثير أبعاد البيانات على كشف الشُّذُوذ

1-4- طرائق كشف الشُّذُوذ (Anomaly Detection Methods)

تُرَكِّزُ طرائق كشف الشُّذُوذ على تَحْدِيد كُلِّ النقاط التي تَسْلُك سلوكاً مغايراً للمفهوم العام الطبيعي، وتَخْتَلِف بعضُها عن بعضٍ بآلية تَمْثيلِ مخرجات الحالات الشَّاذَّة [2]، والتي تكون على نحوٍ عام بإحدى الطريقتين الآتيتين:

1. درجة (Score): تَعْتَمِدُ الطرائق التي تَسْتَنِدُ إلى مفهوم الدرجة، على إعطاء كُلِّ نقطة بيانات درجة شُذُوذ، لِيَتِمّ بعد ذلك تَصْنِيف البيانات وفقاً تِلْكَ الدرجات، حيث تملكُ النقاط الشَّاذَّة درجة شُذُوذ عالية.
2. تَمْثيل ثنائي (Binary): تُسْنِد هذه الطرائق إلى نقاط البيانات تسمية (Label) ثنائية (شَاذَّة أو طبيعية).

يَنْدَرِج تحت هاتين الطريقتين مجموعة من الأساليب والطرائق، وهي كما يلي وفقاً لتسلسل ظهورها التاريخي.

1-4-1- طرائق الكشف الإحصائية (Statistical Anomaly Detection)

تُعَدُّ التقنيات الإحصائية هي الطرائق الأساسية والتقليدية للكشف عن الشُّذُوذ. تَعْتَمد هذه الطرائق على مبدأ عام واحد، وهو دراسة البيانات الطبيعية أولاً، ثَمَّ حساب درجة انحراف كُلّ نقطة في تَدَفُّقَات البيانات عن الوضع الطبيعي، حيث يَكُون للنقاط الشَّاذَّة درجة انحراف عالية. فعلى سبيل المثال، تُستخدَمُ نظرية مربع كاي (Chi-Square) الشهيرة للكشف عن الشُّذُوذ [5]. تَعْتَمِدُ هذه النظرية على إنشاء ملف

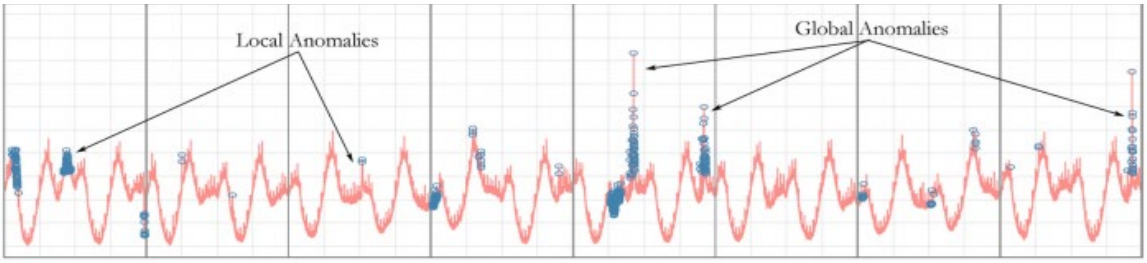
للبيانات الطبيعية في نظام كشف الشُّذُوذ، ثُمَّ يُحَدِّد النظام جميع الأحداث التي لها درجات انحراف عالية عن الوضع الطبيعي كأحداث شَاذَّة.

يُمْكِن أيضاً استخدام المتوسط (Mean) والانحراف المعياري (Standard Deviation) لإيجاد الحالات الشَّاذَّة، حَيْثُ تُعْتَبَر جميع النقاط التي تَبْتَعِد عن المتوسط بمقدار انحراف معياري مُعَيَّن نقاطاً شَّاذَّة؛ لكن في حالة البيانات التي تُمَثِّل سلسلة زمنية فإن ذلك لن يفي بالغرض لأن القِيَم غير ثابتة. حيث يُعْتَمَد في تلك الحالة على وجود نافذة مُتَحركة (Rolling Window)، لحساب المتوسط عبر نقاط بيانات السلسلة الزمنية، ويُسمّى ذلك المتوسط المتحرك (Moving Average) [2].

يوجد مجموعة من التَّحَدِّيَات التي تواجه الطرائق الإحصائية، وَتَحُدُّ من استخدامها في تطبيقات كشف الشَّذُوذ وهي [6]:

1. تَحْتَوِي البيانات في أغلب الحالات على ضجيج، يَكُون له سلوك مشابه للسلوك الشَاذَّ، ومن ثَمَّ يسبب ذلك صعوبة في تحديد الحالات الشَّاذَّة بدقة.
2. تَنْقَسِمُ الحالات الشَّاذَّة إلى شُّذُوذ محلي (Local) وشَذُوذ عام (Global)، حيث يَكُون من السهل الكشف عن الشَّذُوذ العام من خلال الطرائق الإحصائية، على عكس الشُّذُوذ المحلي الذي له أنماط شبيهة بالبيانات الطبيعية.
3. صعوبة دراسة العلاقات والأنماط الْخَفِيَّة ضِمْنَ البيانات.
4. تَزَايَدَ كميات البيانات الْمُوَلّدَة، أَدَّى إلى قُصُور هذه الطرائق على نحوٍ كبير، وذلك لأنها تَحْتَاج إلى تدخل بشري في كُلّ مرحلة من مراحل عمل النظام.

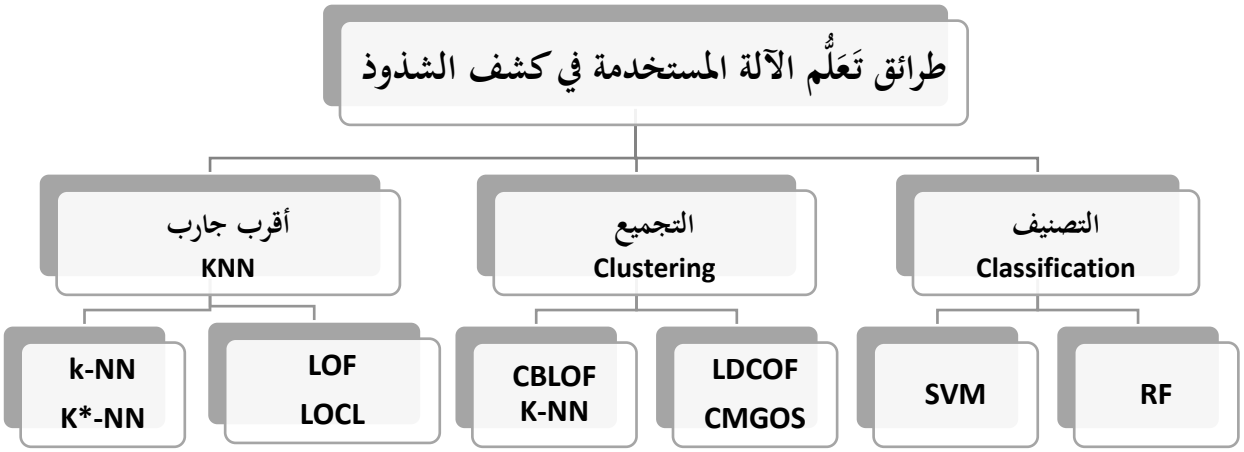
يوضح الشكل الآتي صعوبة تطبيق الطرائق الإحصائية، في اكتشاف الحالات الشَّاذَّة المُتَداخلة مع الحالات الطبيعية (الشُّذُوذ المحلي)، وكما يبدو واضحاً تقعُ النقاط الشاذة المحلية في مناطق قريبة من البيانات الطبيعية.



الشكل 1-3 الشُّذُوذ العام والمحلي- تحديات الطرائق الإحصائية

1-4-2- طرائق تَعَلُّم الآلة (Machine Learning Methods)

توَجّه الباحثون ضِمْنَ مجال اكتشاف الشُّذُوذ إلى استخدام تقنيات تَعَلُّم الآلة، كما هو الحال في العديد من المجالات المختلفة؛ لتفادي القصور الحاصل في الطرائق الإحصائية. يُوجد مجموعة واسعة من طرائق تَعَلُّم الآلة المستخدمة في مجال كشف الشُّذُوذ، وتَنْدَرِج تحت ثلاث فئات رئيسية هي: التصنيف (Classification)، التَّجْمِيع (Clustering)، أقرب جار (Nearest Neighbor).



الشكل 1-4 طرائق تَعَلُّم الآلة المستخدمة في كشف الشذوذ

- **LOF:** Local Outlier Factor
- **CBLOF:** Cluster-Based Local Outlier Factor
- **LDCOF:** Local Density Cluster based Outlier Factor
- **CMGOS:** Clustering-based Multivariate Gaussian Outlier Score
- **RF:** Random Forest
- **SVM:** Support Vector Machine

تَنْتَمِي خوارزميات التصنيف إلى التَعَلُّم الخاضع للإشراف (Supervised Learning)، وتَنْتَمِي خوارزميات التَّجْمِيع وأقرب جار إلى التَعَلُّم غير الخاضع للإشراف (Unsupervised Learning).

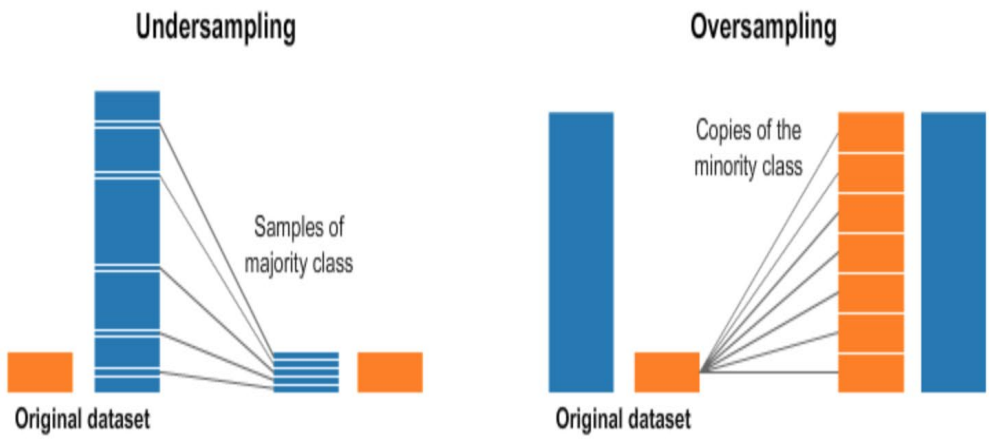
يَتمُّ تَدْرِيب نظام كشف الشُّذُوذ باستخدام خوارزميات التصنيف، بالاعتماد على بيانات مُصَنَّفَة مسبقاً إلى بيانات طبيعية وشَاذَّة. بينما في الأنظمة التي تَعْتَمِدُ على خوارزميات التَّجْمِيع، تَتَجَمَّع البيانات المتشابهة ضِمْنَ عناقيد، وتكون جميع النقاط التي لا تَنْتَمِي لهذه العناقيد هي نقاطاً شَاذَّةً. أما بالنسبة إلى خوارزميات أقرب جار فإنها تَفْتَرِض أَنَّ جميع نقاط البيانات الطبيعية تكون متجاورةً، بينما النقاط الشَّاذَّة تكون بعيدة.

ساعدَ استخدام تقنيات تَعَلُّم الآلة في بناء أنظمة كشف الشُّذُوذ على [7]:

1. اكتشاف بعض الاستراتيجيات الجديدة المرتبطة بالسلوك الشَاذّ.
2. اكتشاف بعض الأنماط الْمُعَقَّدَة وَالْخَفِيَّة في البيانات.
3. دَمَج ملاحظات المحققين تلقائياً لتحسين دقة الكشف، على عكس الطرائق التقليدية التي تَتَطَلَّب مراجعة القواعد، ومن ثَمَّ تَسْتَغْرِق وقتاً أطول.

على النَّقِيضِ من ذلك، اِصْطَدَمَت هذه التقنيات بما يسمى مشكلة البيانات غير المتوازنة (Unbalanced Data)، التي يُهَيْمِنُ فِيهَا صف البيانات الأغلبية الطبيعية (Majority Class) على صف الأقلية الشَّاذَّة (Minority Class). تفْرِضُ مُعْظَم تقنيات تَعَلُّم الآلة أن البيانات موزعة على نحوٍ شبه متساوٍ؛ لكن لا ينطبق ذلك على البيانات غير المتوازنة، مِمَّا يُسَبِّب صعوبة في إنشاء نماذج ذات كفاءة عالية نظراً لشح البيانات الشَّاذَّة في مجموعات البيانات. يُؤَدِّي كُلُّ ذلك إلى خلق ما يسمى بمشكلة تَنَاقُض الدِّقَّة (Accuracy Paradox)، بمعنى آخر تكون دقة تصنيف البيانات الطبيعية أكبر من دقة تصنيف البيانات الشَّاذَّة، لذلك يفشل النموذج في التنبؤ بالحالات الشَّاذَّة، لأن غالبية بيانات التدريب تُمَثِّل بيانات طبيعية. نَقِيس الأمر ذاتهُ على جميع تطبيقات كشف الشُّذُوذ.

طُوِّر العديد من الأساليب للتغلب على هَذِهِ التَّحَدِّيَات والتخفيف من آثارها، يُمكن تنفيذها في مرحلة ما قبل المعالجة (Pre–Processing). تسمى هذه الأساليب إعادة تكوين العينات (Resampling Methods)، وتعمل على إعادة توازن صفوف البيانات. ومع ذلك، خَلَقَتْ هَذِهِ الأساليب تَحَدِّيَاتٍ أخرى [8] تَتَمَثَّلُ في: 1) فقدان البيانات المفيدة التي ربما تكون مهمة لعملية الكشف عند استخدام تقنيات تَقْليصِ العينات (Under–Sampling)، 2) ملاءَمة زائدة (Overfitting) عند استخدام تقنيات تَوْسِيع العينات (Over–Sampling)، بسبب النسخ المتماثل للعينات والَّذِي يُؤَدِّي بدوره إلى تداخل بين الصفوف. يَبْقَى السُّؤَال: هل يجب علينا إعادة التوازن إلى مجموعة البيانات للحصول على أكبر قدر ممكن من البيانات لكلا الصفين؟ أم ينبغي أن يظل صف الأغلبية هو الأكثر تَمْثِيلاً؟ إذا كان الأمر كذلك، فما النسب التي يجب أَنْ نُحَقِّقَهَا لتوازن البيانات؟ لذلك يجب استخدام هذه التقنيات بحذر وَأَنْ نَقُومَ بِعَرْضِ النسب الحقيقية لكلا الصفين، يضاف إلى ذلك أن نأخذ بعين الاعتبار مَا تعنيه نتائج النموذج. يُوضّحُ **الشكل 1–5** مفهوم كل من تقنيتي تَقْليصِ العينات وتَوْسِيع العينات.



الشكل 1-5 طرائق إعادة تكوين العينات

1-4-3- طرائق التَّعَلُّم الْعَمِيق (Deep Learning Methods)

نَتِيجَة تَحَدِّيَات كشف الشُّذُوذ الْمَذْكُورَةِ أعْلَاه والتي خلقتها طبيعة المشكلة الْمُعَقَّدَة، كان لا بد من التوجه في الآونة الأخيرة إِلَى بَنَّاء أنظمة كشف الشُّذُوذ بالاعتماد على التَّعَلُّم الْعَمِيق. يأتي ذلك لِمَا تُوَفِّرُهُ هذه الطرائق من أداة قوية في التعامل مع مشكلة اكتشاف الشُّذُوذ، حيث اِسْتَطَاعَتْ أَنْ تَلْعَبَ دوراً مهماً في التخفيف من آثار تلك التَّحَدِّيَاتِ وَمِنْهَا:

1. انخفاض معدل اِسْتِرْجَاع البيانات الشَّاذَّة (Low Anomaly Data Recall Rate)

تُعَانِي معظم طرائق كشف الشُّذُوذ [4] من صعوبة اِسْتِرْجَاع (اكتشاف) جميع الحالات الشَّاذَّة، وبخاصةٍ تلك التي لها سلوك مشابه للسلوك الطبيعي. بالإضافة إِلى تَحْدِيد الْعَدِيدِ مِنَ الحالات الطبيعية على أنها حالات شَّاذَّة، مِمَّا يُسَبِّب ارتفاعاً في معدلات الإنذارات الكاذبة. يُعدُّ كُلّ من تقليل الإنذارات الكاذبة، وتحسين معدلات الْاِسْتِرْجَاع للشُّذُوذ، أَحَدَ أَهم التَّحَدِّيَات التي يَصْعُبُ تَحْقِيقُهَا، ولا سيما بالنسبة إلى التكلفة الكبيرة الَّتِي يُسَبِّبُهَا فَشَل اكتشاف الحالات الشَّاذَّة.

2. كشف الشُّذُوذ في البيانات عَالِيَّة الأبعاد (High-Dimensional Data)

كان اكتشاف الشُّذُوذ في بيانات عَالِيَّة الأبعاد مشكلة كبيرة لفترة طويلة من الزمن [9]، إذ تُصبح خصائص البيانات الشَّاذَّة مَخْفِيَّة في فضاء عالي الأبعاد. ظَلّت الطرائق القائمة على اختيار الميزات (Feature Selection) [10] حلاً مباشراً لهذه المشكلة؛ لكن وجود علاقات غير خطية وغير متجانسة

حَدّ من فعالية هذه الطرائق. بالإضافة إلى صعوبة اكتشاف الحالات الشَّاذَّة المرتبط بعضها ببعض، مثل العلاقات الزمانية، وغيرها من علاقات الترابط.

3. التَّعَلُّم الفعال للحالات الشَّاذَّة (Efficient Learning Anomaly)

نظراً لصعوبة جَمَع بيانات الشُّذُوذ الْمُسَمَّاة (Labeled) وتكلفتها، فإنه غالباً ما يكون التَّعَلُّم الخاضع للإشراف (Supervised Learning) غير عملي في اكتشاف الشُّذُوذ. تَرَكَّزَت الجهود البحثية في العقد الماضي، على استخدام طرائق التَّعَلُّم غير الخاضع للإشراف (Unsupervised Learning)، التي لا تَتَطلب أي بيانات تدريب مُصَنَّفَة (مُسَمَّاة)؛ لَكِن بِالْمُقَابِل تَعْتَمِد عَلَى وضع فرضية حول توزيع البيانات الشَّاذَّة من دون معرفة شاملة وَمُسَبقَةٍ بِهَا، ومن دون أن تكون هذه الفرضية صحيحة دائماً. مِنْ جِهَةٍ أُخْرَى، يُمْكِن الْإِسْتِفَادَة من البيانات الطبيعية الْمُصَنَّفَة مسبقاً، بالاعتماد على التَّعَلُّم شبه الخاضع للإشراف (Semi–Supervised Learning) [4]، الَّذِي يَعْتَمِدُ على البيانات الطبيعية الْمُسَمَّاة فقط في أثناء عملية التدريب. مِمَّا جَعَلَهُ يُشَكِّلُ اتجاهاً بحثياً في الآونة الأخيرة ضِمْنَ مجال كشف الشُّذُوذ، إذ ساعد عَلَى تَجَاوُز مشكلة شَحّ البيانات الشَّاذَّة في نماذج التصنيف، ومشكلة عدم شمولية الحالات الشَّاذَّة في نماذج التَّجْمِيع.

4. الكشف عن حالات الشُّذُوذ الْمُعَقَّدَة (Detection of Complex Anomalies)

تُسْتَخْدَم معظم طرائق كشف الشُّذُوذ الحالية للكشف عن حالات شذوذ النقطة، إذ إنها تفشل في اكتشاف كُلّ مَنْ شُذُوذ السياق والشذوذ الجماعي، وذلك لأن هذه الأنواع للشُّذُوذ تَتَكَيَّف على نحوٍ أكبر مع الأنماط الطبيعية للبيانات. تَتَمَثَّل أحَد التَّحَدِّيَات في بناء أنظمة لكشف الشُّذُوذ قادرة على التعامل مع كُلّ مَنْ شُذُوذ السياق والشُّذوذ الجماعي.

5. تفسير الشُّذُوذ (Anomaly Explanation)

يُعْتَبِر تَفْسِير الشُّذُوذ في الْعَدِيدِ من التطبيقات الحرجة أمراً هاماً. تُرَكِّزُ مُعْظَمُ أنظمة كشف الشُّذُوذ الحالية على اكتشاف الحالات الشَّاذَّة، من دُونَ تَقْديم تَفْسِير حول السبب المؤدي لتلك الحالات. فَقَدْ يَكُون لِتَفْسِير الحالات الشَّاذَّة الْمُكْتَشَفَة في بعض التطبيقات أهمية دقة الكشف نفسها. تُوَفِّر طرائق التَّعَلُّم الْعَمِيق بعض الخيارات لتوحيد الشُّذُوذ وتَفْسِيره في إطار عمل واحد، مِمَّا يُؤَدِّي إِلى تَفْسِير أكثر واقعية للأشكال الشَّاذَّة التي رَصْدَتِهَا أنظمة كشف الشُّذُوذ؛ لكنه ما يزال يُمَثِّل تَحَدِّيَاً رئيسياً لتحقيق التوازن الجيد بين قابلية التَّفْسِير وفعالية النظام.

6. تحديد عَتَبَة التصنيف ديناميكياً (Selecting the Classification Threshold)

تَتَطَلَّب أنظمة كشف الشُّذُوذ أن تكون قادرة على اختيار عَتَبَة التصنيف (الكشف)، لِلْفَصْلِ بين الحالات الطبيعية والشَّاذَّة. تَخْتَلِف خصَائِص أنظمة كشف الشُّذُوذ وأهدافها حسب مجال التطبيق. ففي بعض التطبيقات، يَكُون لِاسْتِرْجَاع أكبر عدد ممكن من الحالات الشَّاذَّة أهمية أكبر من دقة الكشف. أما بالنسبة إلى التطبيقات الحرجة فإن دقة الكشف لَا تَقُل أهمية عن الحالات الشَّاذَّة المكتشفة. لذلك يَتِمّ اختيار العَتَبَة تجريبياً على نحوٍ ثابت (Static) بناءً على هدف التطبيق؛ لَكِن ما يَزَال اختيار الْعَتَبَة يُمَثِّل تحدياً رئيسياً في أنظمة كشف الشُّذُوذ الحالية، حيث لَا يُمْكِنُهَا اختيار قِيمَة الْعَتَبَة على نحوٍ ديناميكي، بِمَا يَتَنَاسَب مَعَ تَغَيُّر حَجم بيانات التطبيق وطبيعتها.

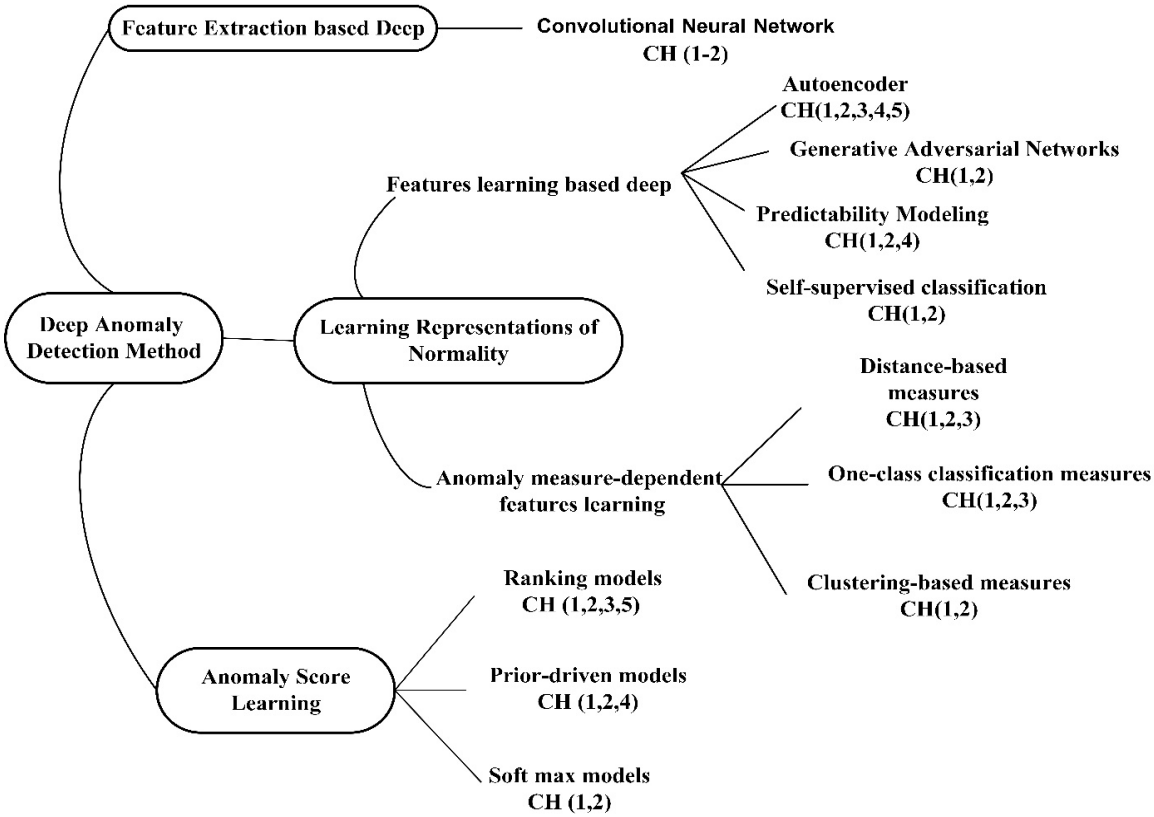
تَتَفَوَّق طرائق التَّعَلُّم الْعَمِيق على طرائق الكشف السابقة بِقُدْرَتِهَا عَلَى التَّعَامُل مَعَ كُلّ التَّحَدِّيَات السابقة إلى حَدٍّ ما. لذلك تكون قادرة على تَحْقِيق اِسْتِرْجَاع أعلى للحالات الشَّاذَّة، وَتَعْلّم الأنماط والعلاقات الْمُعَقَّدَة في البيانات عَالِيَّة الْأَبْعَاد والسلاسل الزمنية، فَضْلًا عَنْ قُدْرَتِهَا على التَّعَامُل مَعَ جميع أنواع الشُّذُوذ.

- **تَصْنِيف طرائق التَّعَلُّم الْعَمِيق (Categorization of Deep Learning)**

يُمْكِن تَصْنِيف طرائق التَّعَلُّم الْعَمِيق في الكشف عن الشُّذُوذ إلى ثلاث فئات رَئِيسِيَّةٍ [11]، ضمنها أحد عشر نموذجاً مختلفاً. وهذه الفئات هِي وَفْقَ الآتي:

1. اِسْتِخْرَاج الميزات (Features Extraction)
2. تَعَلُّم التَمْثِيلات الطبيعية (Learning Representations of Normality)
3. التَّعَلُّم القائم على درجة الشُّذُوذ (Anomaly Score Learning)

يُوضِح الْمُخَطَّط الهرمي في **الشكل 1-6** الفئات الثلاث مع فروعها، بالإضافة إِلَى التَّحَدِّيَات الَّتِي تُعَالِجُهَا تِلْكَ الْمَنْهَجِيَّات. لِيَظْهَر تَفَوَّق شبكة الترميز الآلي (Autoencoder) ضمن فئة تَعلُّم التَمْثِيلات الطبيعية، وذلك من خلال عَدَدِ التَّحَدِّيَات الَّتِي تُعَالِجُهَا (التَّحَدّي 1-5)؛ لَكن بِالْمُقَابِل يبقى تحديد عَتَبَةِ التَّصْنِيف على نحوٍ ديناميكي أحد أهم التحديات التي ما زال العمل قائماً عليها، وهو الْأَمْر ذاته الَّذِي تُعَانِي مِنْهُ جميع طرائق كشف الشُّذُوذ القائمة على التَّعَلُّم الْعَمِيق.



الشكل 1-6 تصنيف طرائق التَّعَلُّم الْعَمِيق الْمُسْتَخْدَمَة في كشف الشُّذُوذ – وتَحَدِّيَاتِ الكشف الَّتِي تَعَالُجِهَا كُلَّ طريقة [11]

- Distance-based measures as Deep Networks based Random Distance [12]
- One-class measures as combine one-class SVM with CNN [13]
- Clustering-based measures as deep autoencoding Gaussian mixture model [14]
- Rankin models as combine Random Forest with Deep Learning [15]
- Prior-driven models as Bayesian inverse reinforcement learning [16]
- Soft max models as Deep Networks based likelihood [17]

1-5- أنظمة كشف الشُّذُوذ (Anomaly Detection Systems)

يَبْقَى السؤال: كيف يُمْكِنُنَا تَحْدِيد فِيمَا إذا كانت نقاط البيانات طبيعية أو شَاذَّة فِي تَدَفُّقَات البيانات؟ يَتِمُّ ذَلِك من خلال بناء أنظمة كشف الشُّذُوذ، وهي أجهزة أو برامج تَقوم بِمُرَاقِبَة البيانات الْمُتَعَلِّقَة بِمَجَالِ مُعَيَّن لِتَحْدِيد الحالات الشَّاذَّة والمُختَلِفة عن السلوك الطبيعي بِاِسْتِخْدَام طرائق كشف الشُّذُوذ.

أَصْبَحَ مَنِ الْوَاضِحِ مِمَّا سَبْق تَوَجُّه أنظمة كشف الشُّذُوذ الحالية إِلَى اِسْتِخْدَام طرائق التَّعَلُّم الْعَمِيق، لَمَّا تَلعَّبَهُ مِنْ دَوْر مُهِمّ فِي مُعَالَجَة معظم التَّحَدِّيَاتِ الْمُتَعَلِّقَةِ باكتشاف الشُّذُوذ. اِسْتَخْدَمَتْ طرائق الكشف

الْعَمِيقَة فِي مجال واسع من تطبيقات العالم الحقيقي ومنها: تَحْدِيدُ السُّلُوك الشاذ للمستخدم ضِمْنَ تطبيقات الشبكة [18]، وكشفُ الاحتيال ضِمْنَ بطاقات الائتمان [19]، وتشخيصُ الحالات المرضية النادرة [20]، واكتشافُ العيوب الصناعية [21]. عَلَى النَّقِيضِ مِنْ ذَلِكَ، تواجه هذه الأنظمة مجموعة من التحديات التي تضعف من فعاليتها على نحوٍ كبير. ولعلَّ أهمها دراسة الميزات (Features) الأكثر أهمية في اكتشاف الشُّذُوذ، واختيار قِيَم البارامترات الفائقة (Hyperparameters) الأفضل وبخاصّةٍ مع ازدياد عددها؛ إضافةً إلى دراسة توزيع البيانات وتَحْدِيدِ عَتَبَةِ التصنيف على نحوٍ ديناميكي، وأخيراً تنوع الحالات الشاذة. يُشكّل كل ما سبق تحدياً كبيراً لبناء نظام كشف شذوذ متكامل قادر على تجاوز التَّحَدِّيَات المطروحة.

1-6- مشكلة البحث

كما تَمَّ إيضاحه سابقاً ومع الازدياد المُسْتَمِرّ لِحَجْم البيانات وأبعادها، ما زلت الحالات الشاذة ضمن البيانات تُمثل إشكالية هامة تحتاج إلى دراسة وتحليل مستمرين لمواجهتها. حيث تُمثل هذه الحالات دلالات مهمة جداً في مجالات واسعة من التطبيقات الحرجة، مثل العمليات الاحتيالية والأمراض النادرة وغيرها. ما زالت أيضاً الأنظمة الحالية للكشف عن الشُّذُوذ تعاني من بعض القصور والصُعُوبة الكبيرة في العديد من الجوانب كاختيار الميزات (Features Selection) الأكثر أهمية في تصنيف الحالات الشَّاذَّة، وضبط البارامترات الفائقة (Hyperparameters Tuning) الخاصة بهذه الأنظمة، وَتَحْدِيدِ عَتَبَةِ التَّصْنِيف على نحوٍ ديناميكي بِمَا يَتَنَاسَبُ مَعَ حَجم بيانات النظام الْمُحَدَّد وطبيعتها. بالإضافة إلى ذلك فَإِنَّ تَنَوُّع حالات الشُّذُوذ، فَرَضَ عَلَى الأنظمة ضَرُورَةَ التَّعَامُل مَعَ جميع هذه الحالات، وَبِخَاصَّةٍ تِلْكَ الْمُرْتَبِطَةِ بِتَسَلْسُلٍ زَمَنِيّ مُعَيَّنٍ.

نَتِيجَةً لكُلّ مَا سَبْق كان لا بُدَّ مِنْ ضَرُورَةِ التَّوَجُّهِ إلى تطوير أنظمة كشف شُذُوذ، قَادِرَة عَلَى حَلّ التَّحَدِّيَات السابقة مِمَّا يُسهم فِي تَحْسِينِ أداء هذه الأنظمة، لما لَهَا مَنْ دَوْرٍ مُهِمّ في المجالات التَّطْبِيقِيَّة الْمُخْتَلِفَة.

1-7- أهداف البحث

يَهْدُف البحث على نحوٍ أساسي إلى تطوير نظام متكامل لاكتشاف الشُّذُوذ في البيانات قادر على تجاوز التحديات المطروحة وبخاصّةٍ المتمثلة بتحديد عَتَبَة التَّصْنِيف ديناميكياً للتفريق بين البيانات الطبيعية والشاذة، بالإضافة إلى تحديد الميزات الأكثر أهمية، واختيار البارامترات الفائقة الأمثل لعمل هذا النظام.

ويتم ذلك من خلال تَحقِيق الآتي:

1. مُنَاقَشَة الاتجاهات التكنولوجية الأخيرة في أنظمة كشف الشُّذُوذ.

2. تَقديم دراسة تحليلية لأهم أنظمة كشف الشُّذُوذ في البيانات باستخدام خوارزميات مختلفة.
   - تَأْثِير تَرْتِيب إِجْرَائِيَات ضبط البارامترات الفائقة واختيار الميزات على أداء هذه الأنظمة.
3. تَطْوِير نظام ديناميكي لكشف الشُّذُوذ باستخدام التَّعَلُّم الْعَمِيق يَكُونُ قَادِراً على:
   - اكتشاف الحالات الشَّاذَّة الجديدة.
   - تَحْدِيد عَتَبَة التَّصْنِيف ديناميكياً من دُونَ وَضْع فَرَضِيَّاتِ حَوْلَ تَوْزِيع البيانات وحجمها.
   - تَحْدِيد الميزات الأكثر أهمية في تَصْنِيفِ الحالات الشَّاذَّة.
   - تَحْدِيد قِيَم البارامترات الفائقة اللازمة لعمل هذه الأنظمة على نحوٍ أَفَضْل.
   - مُعَالَجَة أنواع الشَّذُوذ (حالات شُذوذ نقطة، اِلْتِقَاطَ التَّبِعِيَات الزَّمنيَّة لِتَسَلْسُل شُذُوذ السياق).
4. إثبات كفاءة النِّظَامِ الْمُقْتَرَحِ من خلال إسقاطه على تطبيقات حقيقية.

1-8- أَهَمِّيَّةُ البحث

بالإضافة لما يقدمه هذا البحث من تعريف وتحليل شامل لمفهوم الشُّذُوذ وأنظمته، وكيفية معالجته وتأثيره على مختلف المجالات العملية. يقدّم البحث نظاماً متكاملاً لكشف الشُّذُوذ، يمكن تطبيقه مباشرةً ضمن مؤسسات وقطاعات مختلفة مهتمة باكتشاف الحالات غير الطبيعية كالبنوك وأنظمة التأمين الصحي وغيرها الكثير.

كما يمكن علمياً الاستفادة من الخوارزمية المقترحة لدمجها بأنظمة كشف شذوذ أخرى، لمساعدتها على تحديد عتبات التصنيف على نحوٍ آلي.

اِعتَمَدَت الدراسة لحل مشكلة البحث على استخدام تقنيات التَّعَلُّم الْعَمِيق، وتحديداً شبكة الترميز الآلي مع عَتَبَة ديناميكية المقترحة ضمن الدراسة (Autoencoder with a Dynamic Threshold)، والذاكرة قصيرة طويلة المدى (Long Short-Term Memory) كطرائق لكشف الشُّذُوذ، وعلى تقنية البحث العشوائي (Random Search) لتَحْدِيد قِيَم البارامترات الفائقة. تَمَّت تَجْرِبَة النظام الْمُقْتَرَح على كُلّ من اكتشاف حالات فشل آلة الورق في معامل صناعة اللب والورق، واكتشاف العمليات الاحتيالية في بطاقات الائتمان. كَمَا تَمَّ تَقْيِيم النظام بِاِسْتِخْدَام مجموعة من مقاييس الأداء الخاصة بكشف الشُّذُوذ.

1-9- فصول الأطروحة

تتألف الأطروحة من ثمانية فصول على الشكل الآتي:

- **الفصل الأول:** المقدمة.
- **الفصل الثاني:** يتضمن شرحاً عن طرائق الكشف المستخدمة في الدراسة.

- **الفصل الثالث:** يتضمن شرحاً لأهم مقاييس الأداء في أنظمة كشف الشُّذوذ؛ إضافةً إلى مجموعات البيانات البحثية المستخدمة.
- **الفصل الرابع:** يتضمن عرضاً للدراسات المرجعية السابقة.
- **الفصل الخامس:** يتضمن المنهجية المتبعة في الدراسة لتحليل عمل أنظمة كشف الشُّذُوذ.
- **الفصل السادس:** يتضمن عرضاً لخوارزمية الكشف المقترحة AEDT؛ إضافةً إلى نظام كشف الشذوذ الْمُقْتَرَح AEDTM–ADS ضمن هذه الدراسة.
- **الفصل السابع:** يتضمن عرضاً لأهم النتائج ومناقشتها.
- **الفصل الثامن:** يتضمن الخاتمة والاستنتاجات والتوصيات.

مساهمات الأطروحة:

تتلخص المساهمة المقدمة ضمن ثلاثة اتجاهات: **الأول**، تحليل أنظمة كشف الشُّذُوذ المعمول بها حالياً بِهَدَف تحديد كفاءة هذه الْأَنْظِمَة من حيث زمن التدريب ونسبة الكشف. **الثاني**، بناء نظام متكامل لكشف الشُّذُوذ في البيانات قادر على تجاوز أهم التحديات المطروحة. **الثالث**، تطوير واجهات تخاطبية للنظام الْمُقْتَرَح لبيان إمكانية استثماره مباشرةً في أي تطبيق من تطبيقات العالم الحقيقي بعد ملاءمته ليناسب البيانات المدخلة.

الأبحاث المنجزة ضمن الدكتوراه:

"تحديد التوليفة الأمثل من ضبط البارامترات الفائقة واختيار الميزات لتحسين أداء أنظمة كشف الشذوذ" – مجلة جامعة البعث للعلوم الهندسية – المجلد /43/ لعام 2021

"تحديد عتبة التصنيف المثلى ديناميكياً في أنظمة الكشف المبكر عن الشذوذ القائمة على التعلم العميق" – مجلة جامعة البعث للعلوم الهندسية – المجلد /44/ لعام 2022

"AEDT-ADS Anomaly Detection System Based on Dynamic Classification Threshold and Deep Learning". Journal of Ambient Intelligence and Humanized Computing (JAIHC). (2022).

الفصل الثاني

الخوارزميات المستخدمة

يتضمن هذا الفصل شرحاً عن خوارزميات تَعلُّم الآلة الكلاسيكية والعميقة المستخدمة في هذه الدراسة. تندرج الغابات العشوائية وآلة شعاع الدعم تحت خوارزميات تَعَلُّم الآلة الكلاسيكية، بينما شبكة الترميز الآلي والذاكرة قصيرة طويلة المدى هي شبكات عصبونية عميقة.

2-1- خوارزمية الغابات العشوائية (Random Forest Algorithm)

تُعدّ خوارزمية الغابات العشوائية [22] من طرائق التَعَلُّم الخاضع للإشراف. تتكون الغابة من مجموعة من أشجار القرار (Decision Trees). الهدف من شجرة القرار هو إنشاء نموذج يتنبأ بقيمة متغير مستهدف من خلال تَعلُّم قواعد قرار بسيطة يَتِمُّ استنتاجها من ميزات البيانات. يَتُّم تدريب الغابات العشوائية باستخدام مفهوم التعبئة (Bagging). تتمثل إحدى الميزات الكبيرة للغابات العشوائية في إمكانية استخدامها لكل من مسائل التصنيف والانحدار، تركز الدراسة الحالية على استخدام الغابات العشوائية في مهام التصنيف.

باختصار: تعمل الغابات العشوائية على بناء مجموعة من أشجار القرار، ودمجها معاً باستخدام تقنيات التجميع (Ensemble Technique) للحصول على تنبؤ أكثر دقة.

2-1-1- مصنفات الغابات العشوائية (Random Forests Classifiers)

يستخدم التصنيف في الغابات العشوائية تقنية التعبئة المعروفة أيضاً باسم " Bootstrap Aggregation" والتي تقوم باختيار مجموعة جزئية عشوائية مع الاستبدال من بيانات التدريب (مما يعني أنه يمكن اختيار نفس العينة عدة مرات، سحب مع إعادة)، تُعرف الخطوة السابقة باسم Bootstrap. يَتِمُّ في كل مرة اختيار عينة جديدة Bootstrap Sample لعملية تدريب الأشجار، للوصول في نهاية الأمر إلى مجموعة من الأشجار المدربة. يعتمد الناتج النهائي على تصويت الأغلبية (Majority Voting) لجميع النماذج (الناتج النهائي هو الذي تختاره غالبية أشجار القرار)، تُعرف الخطوة الأخيرة باسم التجميع (Aggregation).

- **بناء مصنفات الغابات العشوائية**

إن الغابات العشوائية هي مجموعة من أشجار القرار، وكل شجرة قرار تتكون من ثلاث أنواع من العقد، عقد القرار (Decision Nodes) والعقد الورقية (Leaf Nodes) وعقدة الجذر (Root Node).

تُمثل هذه العقد ميزات مجموعة البيانات، باستثناء العقد الورقية التي تمثل ناتج الشجرة. تُقسم مجموعة بيانات التدريب إلى فروع (يمثل كل فرع سؤالاً تصنيفي جوابهُ "نعم" أو "لا"؟ بناءً على قيمة العقدة)، ويستمر التقسيم في الفروع حتى يَتِمُّ الوصول إلى عقدة ورقية لا يمكن عندها الفصل [23].

بفرض لدينا مجموعة البيانات X ، ونريد بناء شجرة قرار ($iTree$). بدايةً يَتِمُّ اختيار مجموعة عينات عشوائية من X حيث $S(X) \in X$، ثم يَتِمُّ تقسيم مجموعة العينات هذه إلى مجموعتين فرعيتين غير فارغتين [24] وفق المعادلة الآتية:

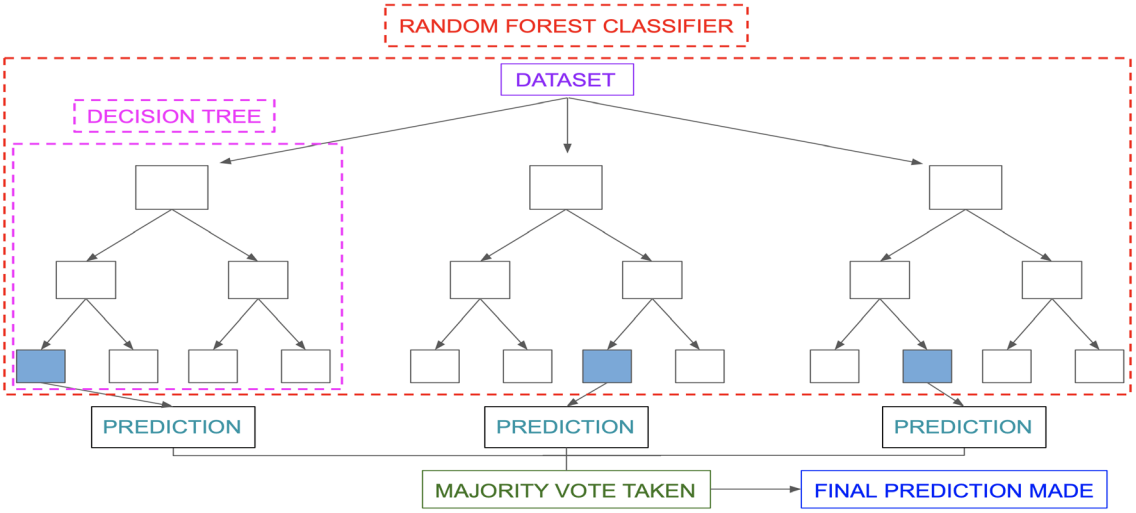
$$S(X)_L = \{x \in S(X)\} \text{ and } S(X)_R = S(X) / S(X)_L \qquad (2\text{-}1)$$

يستمر تقسيم كل مجموعة فرعية حتى تصبح مفردة (Singleton)، لينتج في نهاية الأمر شجرة ثنائية عدد عقدها يساوي $2s - 1$. باختيار عينات عشوائية جديدة من X، ينتج مجموعة متنوعة من أشجار القرار (غابة). بالتالي يَتِمُّ تحديد الصف الذي تنتمي إليه البيانات، بالاعتماد على تصويت الأغلبية.

كيف يَتِمُّ اختيار الميزات للعقد؟ إن الاختلاف الرئيسي بين الغابات العشوائية وأشجار القرار، هو في اختيار الميزات. تختار شجرة القرار الميزة التي لها أعلى قيمة ربح للمعلومات (Information Gain) من بين جميع الميزات كما في المعادلة (2-2) ، بالمقابل فإن الغابات العشوائية تختار الميزة التي لها أعلى قيمة ربح ضمن مجموعة جزئية عشوائية من الميزات، مع إمكانية اختيار الميزة من مجموعات مختلفة (سحب مع إعادة)، وهذا يفرض تنوع أشجار القرار في الغابات العشوائية، مما يعطي استقراراً أكثر للخوارزمية. يوضح **الشكل 2-1** مصنف غابة عشوائية بسيط.

$$\text{gain} = E(Y) - E(Y/X) \qquad (2\text{-}2)$$

E: تابع الانتروبي، X: المتغير المستقل، Y : المتغير الهدف



الشكل 2-1 مصنف غابة عشوائية

2-1-2- البارامترات الفائقة للغابات العشوائية (Random Forest Hyperparameter)

فيما يلي عرض للبارامترات الفائقة [25] المستخدمة في تدريب الغابات العشوائية:

1. الحد الأعظمي لعمق الشجرة (Maximum Depth of Tree)

يحدد أقصى عمق يُمكن أن تصل إليه الشجرة، وإذا لم يَتِمُّ ضبط قيمة هذا البارامتر فسوف يَتِمُّ التوسع في الشجرة حتى تصبح جميع الأوراق نقية، أو تحتوي على عينات أقل من الحد الأدنى للعينات المطلوبة للتقسيم.

2. الحد الأدنى للعينات المطلوبة للتقسيم (Min of Samples to Split)

يحدد الحد الأدنى لعدد العينات المطلوبة لتقسيم عقدة داخلية (عقدة قرار). فإذا كان عدد العينات الموجودة في عقدة داخلية أقل من الحد الأدنى، فإنه عندئذ لا يحدث الانقسام وتصبح العقدة الداخلية عقدة ورقية.

3. عدد الأشجار (Number of Trees)

يُمثل عدد أشجار القرار التي تتضمنها الغابة. يؤدي وجود عدد كبير من الأشجار إلى زيادة في الأداء وجعل التنبؤات أكثر استقراراً؛ لكنه يؤدي إلى بطء في عملية الحساب.

4. العدد الأعظمي للميزات (Max Number of Features)

تُمثل الحد الأعظمي لعدد الميزات التي تأخذها الخوارزمية بعين الاعتبار عند اختيار العقد، وبمعنى آخر حجم المجموعة الجزئية للميزات.

5. الحد الأدنى للعينات ضمن الأوراق (Min of Samples to be at Leaf)

تُمثل الحد الأدنى لعدد العينات الموجودة في كل ورقة. فإذا كان ينتج عن الانقسام عقدة ورقية، لديها عدد عينات أقل من الحد الأدنى للعينات ضمن الأوراق، فعندئذ لا يحدث الانقسام وتصبح العقدة الداخلية عقدة ورقية، ولو كان عدد العينات المطلوبة لتقسيم عقدة داخلية كافياً أم لا.

6. Bootstrap

يُجِيب هذا البارامتر عن السؤال الآتي: هل سوف يتم الاعتماد على كامل مجموعة التدريب أو مجموعة جزئية منها عند بناء الأشجار؟ إن إسناد قيمة True للبارامتر، يعني استخدام مجموعة جزئية من بيانات التدريب.

2-1-3- كشف الشذوذ القائم على الغابات العشوائية

إن اعتماد الغابات العشوائية على مجموعات جزئية من الميزات في كل مرة عند بناء أشجار القرار أدى إلى اختزال فضاء أبعاد البيانات (عدد الميزات). وبذلك عزز القدرة على التعامل مع بيانات عالية الأبعاد. ولعلَّ ذلك أهم ما تتطلبه أنظمة كشف الشذوذ. لكن على الجانب الآخر، يجب التنبيه على أنه، في البيانات غير المتوازنة من المحتمل جداً أن تحتوي Bootstrap Sample على عدد قليل من عينات صف الأقلية أو لا تحتوي عليها. سيؤدي ذلك إلى شجرة ذات أداء ضعيف للتنبؤ بصف الأقلية. يُمكن التخفيف من آثار ذلك من خلال موازنة البيانات قبل عملية تغذية الشجرة بها؛ لكنه قد يؤدي إلى ضياع بعض نقاط البيانات المهمة للتصنيف. يمكن أيضاً إجراء التحقق من الصحة المتقاطع (Cross Validation) عند تدريب الخوارزمية للتخفيف من آثار المشكلة.

يَتِمُّ تحديد صف عينات البيانات سواء كانت شاذة أم طبيعية من خلال احتساب عدد الأصوات لجميع الاشجار، واعتماد نتيجة سلوك العينة لصالح الصف الأكثر تصويتاً.

$$\text{score}_{\text{forest}}(x) = \begin{Bmatrix} \text{normal, if most of score}_{\text{iTree}}(x) \text{ is normal} \\ \text{anomaly, f most of score}_{\text{iTree}}(x) \text{ is anomaly} \end{Bmatrix} : i = 1..n \quad (2\text{-}3)$$

2-2- خوارزمية آلة شعاع الدعم (Support Vector Machine Algorithm)

تعد خوارزمية آلة شعاع الدعم (SVM) [26] واحدة من أكثر خوارزميات تَعلُّم الآلة شيوعاً والمستخدمة على نطاق واسع، بسبب بساطة فكرة عملها وأناقتها رياضياً من جهة، وسهولة استخدامها من جهة أخرى.

تقوم فكرة الخوارزمية على الفصل بين الصفوف داخل فضاء البيانات، بمستوٍ يسمى المستوى الفائق (Hyperplane). لكي تتمكن SVM من إيجاد ذلك المستوى، لا بد من أن تكون البيانات قابلة للفصل الخطي (Linearly Separable).

2-2-1- قابلية الفصل الخطي (Linearly Separable)

تكون البيانات قابلة للفصل خطياً [27]، إذا تمكنا من فصلها إلى مجموعتين مختلفتين، ضمن فضاء أحادي أو ثنائي أو ثلاثي البعد، بنقطة أو مستقيم أو مستوٍ على الترتيب.

إن البيانات في التطبيقات الحقيقية كالكشف عن الشذوذ، تقع ضمن فضاءات ذات أبعاد أعلى، ونتيجة لذلك يأتي مفهوم المستوي الفائق.

- **المستوي الفائق (Hyperplane)**

إن فصل البيانات عالية الأبعاد رياضياً، يتم بالاعتماد على المستوى الفائق وفق المعادلة الآتية:

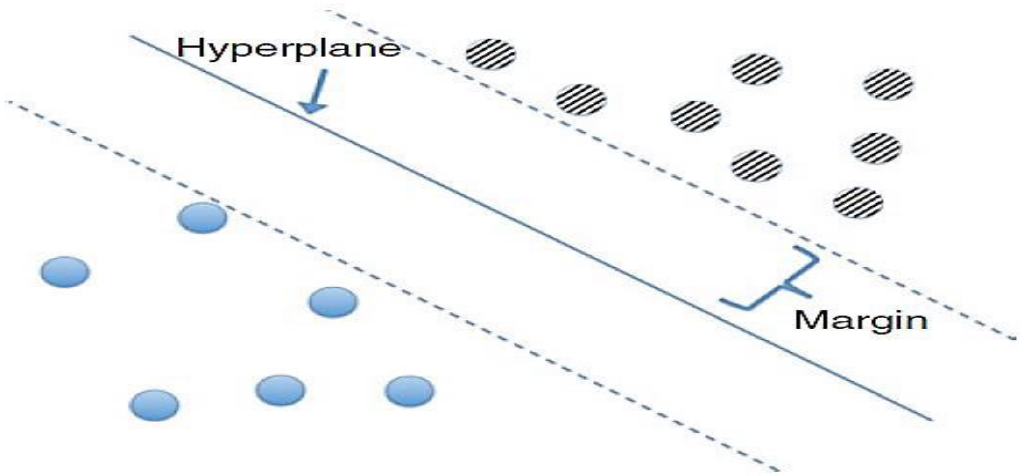
$$f(x) = w.x + b = 0 \qquad (2\text{-}4)$$

w : شعاع عامودي على المستوي الفائق، b : تَقِيس مدى انزياح هذا الشعاع عن المركز

x: نقطة بيانات

2-2-2- مفاهيم آلة شعاع الدعم (Support Vector Machine Concepts)

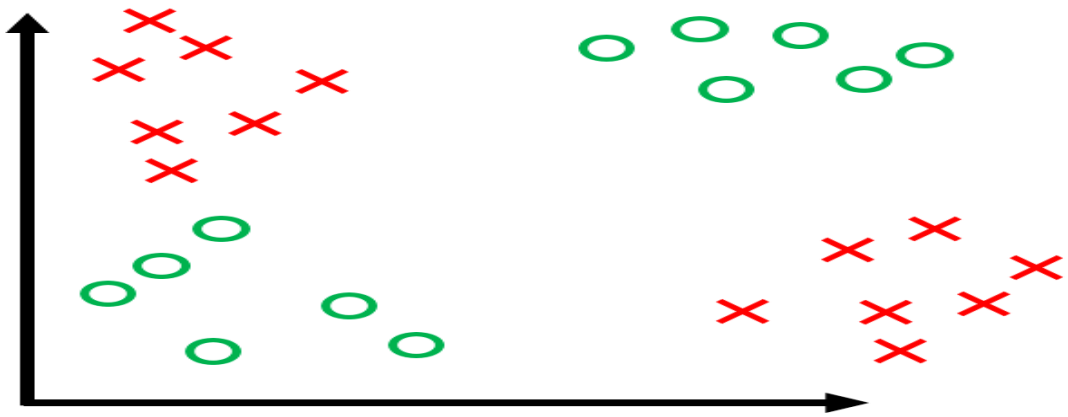
تسعى الخوارزمية إلى إيجاد أفضل مستوٍ فائق قادر على فصل البيانات إلى مجموعتين مختلفتين، من خلال إيجاد قيم w و b التي تُعظّم الهامش (Margin) بين المستوي ونقاط البيانات، حيث تُصنّف نقطة البيانات x وفقاً لإشارة f في المعادلة (2-4). يوضح الشكل الآتي فصل البيانات خطياً باستخدام المستوي الفائق.



الشكل 2-2 فصل البيانات خطياً باستخدام المستوي الفائق

ماذا لو كانت البيانات غير قابلة للفصل خطياً؟ يوضح **الشكل 2-3** مثالاً على هذه الحالة، إذ تفشل خوارزمية SVM التقليدية في إيجاد مستوٍ فائق يفصل نقاط البيانات على نحوٍ صحيح.

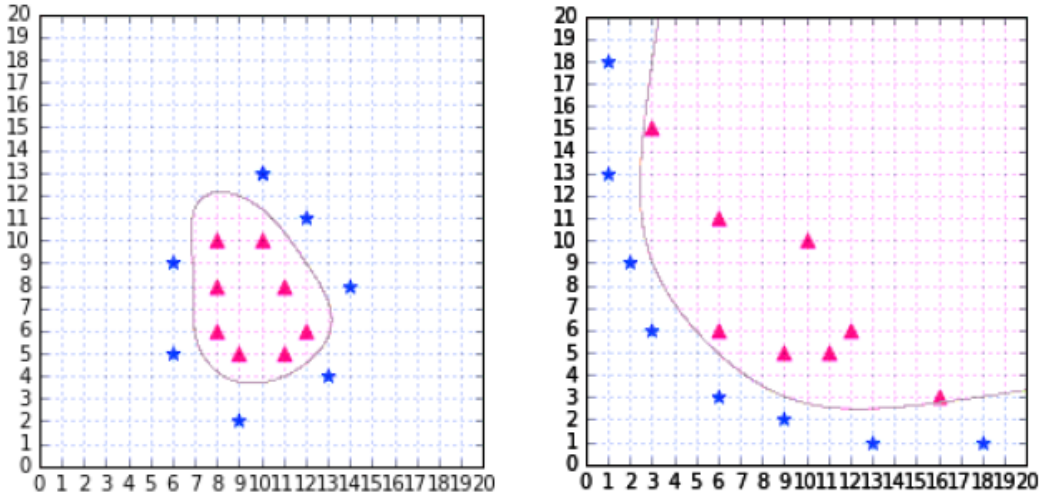
يَتِمُّ حل المشكلة السابقة [26] بإجراء تعديل رياضي على الخوارزمية، يسمى نوى آلة شعاع الدعم (Kernel SVM)، وهو عبارة عن تعميم لخوارزمية آلة شعاع الدعم، يسمح لها بتصنيف البيانات التي لا يمكن فصلها خطياً.



الشكل 2-3 مجموعة بيانات غير قابلة للفصل خطياً

- **نوى آلة شعاع الدعم (Kernel SVM)**

تعتمد نوى SVM على الفكرة الرياضية الآتية: حين نقول عن مجموعة بيانات إنها غير قابلة للفصل، فهذا يعني أنها غير قابلة للفصل ضمن الفضاء الأصلي الذي تنتمي له، لكنها قد تكون قابلة للفصل في فضاء ذي بعدٍ مختلف. يأتي هنا دور النوى إذ إنها تستخدم تابعاً ما ϕ ، يقوم بعملية إسقاط (Mapping) لنقاط البيانات من الفضاء الأصلي ذي d بُعد إلى فضاء جديد ذي n بُعد، بشرط أن تكون قابلة للفصل خطياً فيه. يوضح **الشكل 2-4** تصنيف آلة شعاع الدعم لبيانات غير قابلة للفصل خطياً على نحوٍ صحيح.



الشكل 2-4 تصنيف آلة شعاع الدعم لبيانات غير قابلة للفصل خطياً

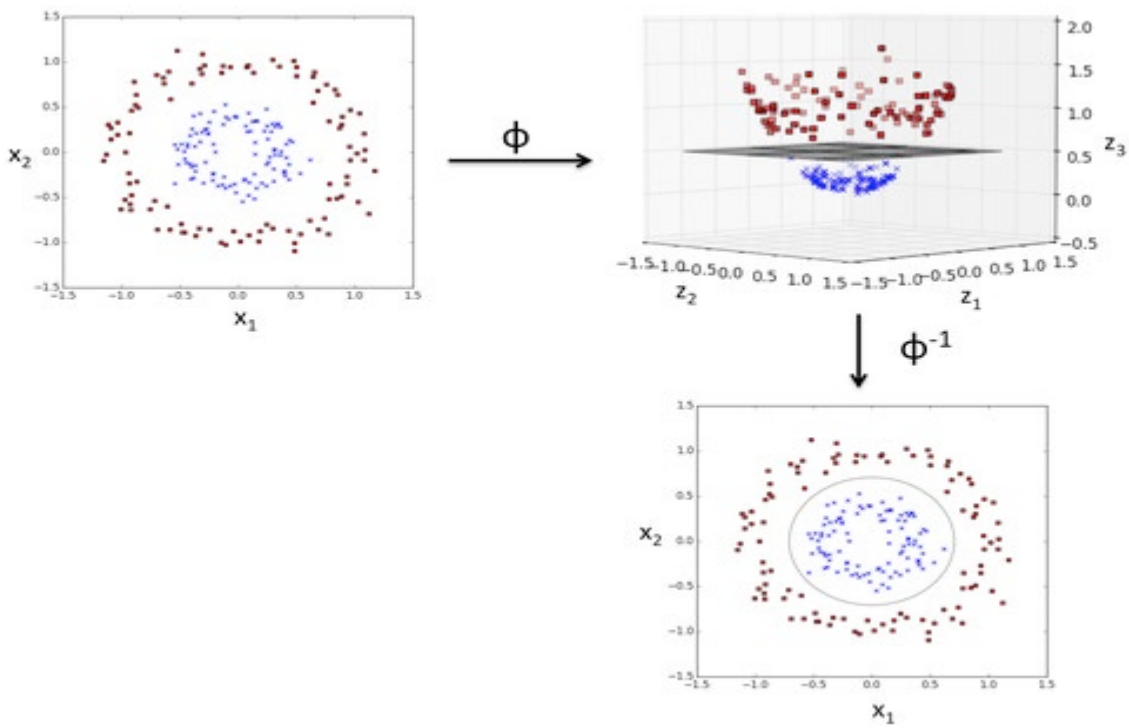
يوجد مجموعة من نوى SVM أكثرها شيوعاً (Polynomial Kernel، Gaussian Kernel، RBF: Radial Basis Function، Sigmoid Kernel) ويعد اختيار النواة الصحيحة أمراً بالغ الأهمية. إن عملية الإسقاط غير المناسبة، تؤدي إلى نتائج سيئة للغاية في أداء الخوارزمية. يُمكن اتباع القاعدة العامة لاختيار النوى المناسبة وهي: "التحقق دائماً فيما إذا كانت مجموعة البيانات خطية، عندئذٍ يَتِمُّ استخدام نواة خطية مما يوفر كلفة في المعالجة الحاسوبية". ليس الأمر كذلك مع النواة RBF على سبيل المثال والتي تعتبر نواة غير خطية، فهي أكثر تعقيداً من حيثُ كلفةُ التدريبِ والإسقاطِ إلى فضاء ذي أبعاد جديدة. يوضح **الشكل 2-5** مبدأ عمل نواة RBF حيث يمكن ضمنها استخدام حدود القرار الخطي لفصل الصفوف الخاصة بمشكلة التصنيف، بينما تكون الصيغة الرياضية على النحو الآتي:

$$\oplus\,(x_1, x_2) = \exp\left(-\frac{\left|\left|x_1 - x_2\right|\right|^2}{2\sigma^2}\right) \qquad (2\text{-}5)$$

---

x_1, x_2: نقاط بيانات

σ: عرض منطقة التشابه بين نقاط البيانات (متحول gamma)



الشكل 2-5 مبدأ عمل نواة RBF

يكافئ مبدأ عمل نواة Sigmoid في SVM شبكة عصبونية مكونة من طبقتين، إذ يتم تحويل الدخل إلى نطاق بين الصفر والواحد، لذلك لا يمكن استخدامها إلا من أجل المصنفات الثنائية. بينما تكون الصيغة الرياضية على النحو الآتي:

$$\oplus\,(x,y) = \tanh(\alpha x^{T} y + c) \qquad (2\text{-}6)$$

α : الميل ويساوي $1/N$، حيث N بعد البيانات

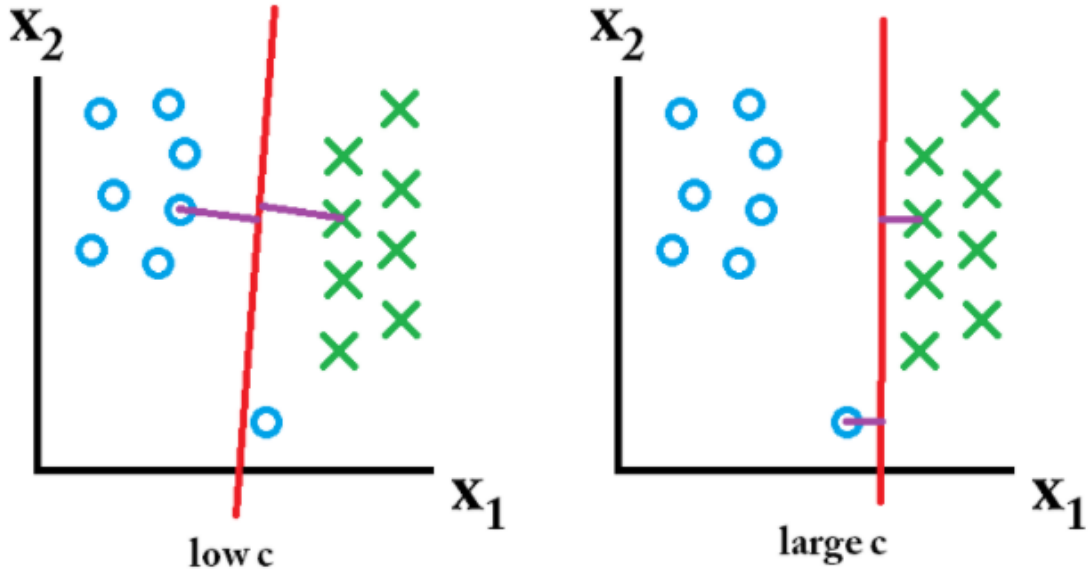
c: مقدار التسامح في تخطي تصنيف نقاط البيانات

2-2-3- البارامترات الفائقة لشعاع الدعم (SVM Hyperparameter)

فيما يلي عرض للبارامترات الفائقة [28] المستخدمة في تدريب آلة شعاع الدعم

1. التنظيم (Regularization)

تحدد قيمة هذه البارامتر مدى السماح لخوارزمية SVM في تخطي تصنيف نقاط التدريب، وبناءً على قيمة البارامتر يَتِمُّ تحديد حجم الهامش للمستوي. تختار الخوارزمية من أجل قيم كبيرة للبارامتر، أصغر هامش للمستوي لا يسمح بتخطي الكثير من نقاط التدريب، لذلك تصنف الخوارزمية جميع نقاط البيانات على نحوٍ صحيح. على العكس من ذلك، تؤدي القيم الصغيرة للبارامتر إلى اختيار الخوارزمية لهامش كبير للمستوي، حتى لو أخطأ المستوي في تصنيف العديد من نقاط البيانات. يوضح الشكل الآتي دور البارامتر في تصنيف نقاط البيانات.



الشكل 2-6 تأثير التنظيم ضمن آلة شعاع الدعم في تصنيف البيانات

2. Gamma

يحدد متحول Gamma مدى تأثير عينة التدريب في إيجاد المستوي الفائق الأمثل. إن قيمة Gamma المرتفعة، تأخذ في الاعتبار النقاط القريبة لإيجاد المستوي، بينما تأخذ القيمة المنخفضة، في الاعتبار النقاط الموجودة على مسافات أكبر.

2-2-4- كشف الشذوذ القائم على آلة شعاع الدعم

تُعتَبر SVM خوارزمية فعالة في مسألة اكتشاف الشذوذ نظراً لإمكانية استخدام نواة مناسبة في حال كانت البيانات غير قابلة للفصل خطياً من جهة، وقدرتها على التعامل مع البيانات ذات الأبعاد العالية (وهي سمة عامة لأغلب مسائل كشف الشذوذ) من جهة أخرى، فهي تحاول إيجاد المستوي الفائق الأفضل بناءً على عامل تعظيم الهوامش الفاصلة بين صفي البيانات وليس على عدد الميزات المستخدمة. إن البيانات الشاذة تُصنَّف بالاعتماد على إشارة تابع المستوي الفائق بالشكل الآتي:

$$\begin{Bmatrix} (w, x_i) + b \geq 0 \rightarrow y_i = 0 \text{ (normal)} \\ (w, x_i) + b < 0 \rightarrow y_i = 1 \text{(anomaly)} \end{Bmatrix} \qquad (2\text{-}7)$$

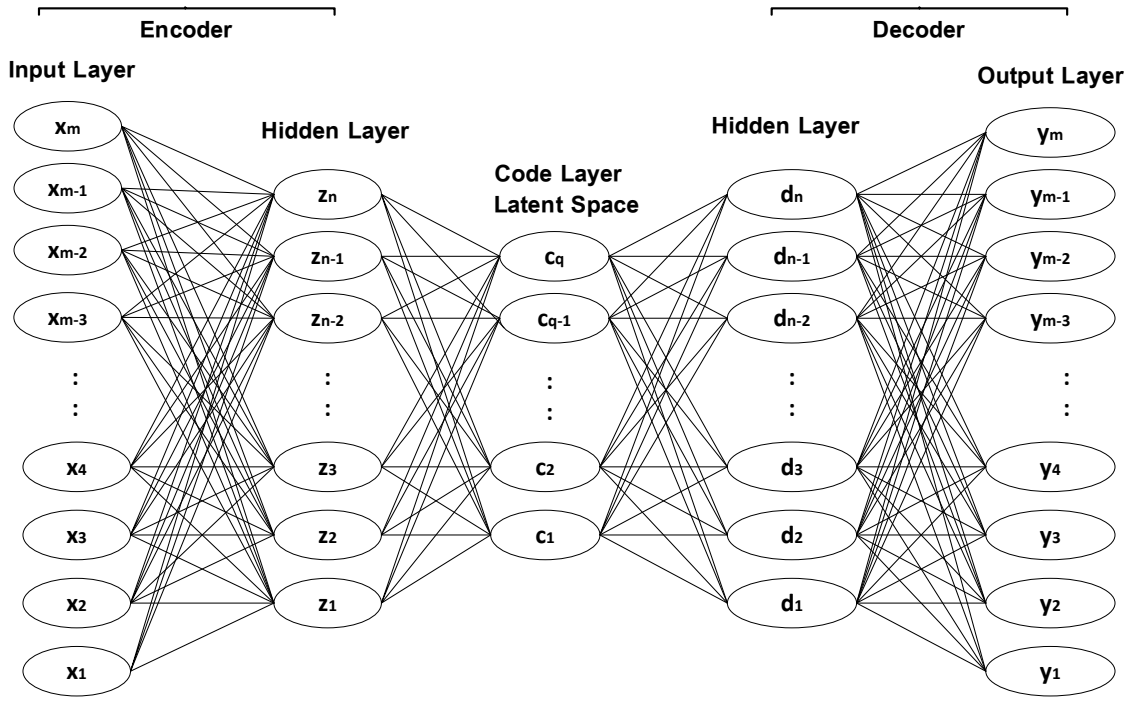
2-3- شبكة الترميز الآلي (Autoencoder Network)

هي شبكة عصبونية متعددة الطبقات، شبه خاضعة للإشراف (Semi-Unsupervised)، ذات تغذية متقدمة (Feed-Forward) [29]. تتكون من طبقة إدخال، وطبقة إخراج، ومُرَمِّز (Encoder)، ومفكك ترميز (Decoder)، وفضاء كامن (Latent Space). يَتِمُّ تغذية دخل الشبكة بشعاع مكوَن من ميزات (Features) مجموعة بيانات الدخل، ومن ثم تعمل الشبكة على إعادة إنتاج هذا الشعاع في طبقة الخرج. يَتَلَخَّص عمل المُرَمِّز في ضغط شعاع الدخل إلى الفضاء الكامن، بينما يقوم مفكك الترميز بفك ضغط التمثيل المُرَمَّز من الفضاء الكامن إلى طبقة الخرج. يَتِمُّ تدريب الشبكة بالاعتماد على خوارزميات الانتشار الخلفي (Backpropagation)، وتابع خسارة (Loss Function) لحساب الفرق الناتج عن إعادة بناء شعاع الدخل في طبقة الخرج.

2-3-1- مفاهيم شبكة الترميز الآلي (Autoencoder Concepts)

نَفرِض بدايةً عند تصميم بنية شبكة Autoencoder وجود مشكلة عنق الزجاجة (Bottleneck) في المنتصف مما يفرض تمثيل مضغوط للمدخلات الأصلية؛ لذلك تُعتبر الشبكة مناسبة جداً في مجموعات البيانات ذات الأبعاد الكبيرة حيث تَعمل على اختزال البيانات في بُعد أصغر مع الاحتفاظ بالمعلومات الرئيسية لهيكلية البيانات.

وكما ذكرنا سابقاً، الشبكة تتكون من ثلاثة مكونات رئيسية [29] هي: المُرَمِّز، الترميز (Code)، مفكك الترميز. كما تحتاج إلى ثلاث أشياء: طريقة الترميز، طريقة فك الترميز، وتابع الخسارة. يوضح الشكل الآتي معمارية شبكة الترميز الآلي.



الشكل 2-7 معمارية شبكة الترميز الآلي

يُعتبر المُرَمِّز ومفكك الترميز شبكة عصبونية عميقة ذات تغذية متقدمة، ومتصلة بالكامل (Fully-Connected) فيما بينها. يقوم المُرَمِّز بضغط البيانات الأصلية إلى بُعدٍ أصغر، بينما يَعمل مفكك الترميز على فك ترميز البيانات المضغوطة وإعادة بنائها إلى بُعدها الأصلي. يُمثل الترميز طبقة واحدة في الشبكة بحجم اختياري يَتِمُّ تحديده قبل عملية التدريب (يسمى أيضاً عنق الزجاجة). حيث يَتَحَكم حجم هذه الطبقة بِبُعد المدخلات المضغوطة التي يَتِمُّ تغذيتها إلى وحدة فك الترميز.

تُمرر بيانات الإدخال عبر المُرَمِّز، لضغط البيانات إلى بُعد بحجم n (حجم طبقة المُرَمِّز) كمرحلة أولى، ويمكن إضافة الترميز لضغطها إلى بُعد أصغر q $(n > q)$. تمثل المعادلة الآتية طبقة المُرَمِّز.

$$z = \sigma(W_{enc}x + b_{enc}) \qquad (2\text{-}8)$$

W: مصفوفة بحجم $m * n$ تمثل الأوزان بين طبقة الدخل وطبقة المُرَمِّز

b: متجهة بحجم n تمثل تحيز (bias) طبقة المُرَمِّز

x: متجهة بحجم m تمثل دخل طبقة المُرَمِّز

σ: تابع تنشيط طبقة المُرَمِّز

يقوم مفكك الترميز الذي له بنية مماثلة للمُرَمِّز، بإعادة إنتاج الدخل في طبقة الخرج، كما في المعادلة الآتية:

$$y = \sigma(W_{dec}d + b_{dec}) \qquad (2\text{-}9)$$

يجب أن يكون لطبقتي الدخل والخرج نفس عدد العصبونات m، بينما يمكن تعديل أحجام الطبقات في الوسط كما نريد.

تهدف الشـــبكة في أثناء عملية التدريب إلى تصـــغير تابع الخســـارة لخطأ إعادة البناء (Reconstruction Error). يَقِيس خطأ إعادة البناء الفرق بين المدخلات والمخرجات الحالية لشـــبكة الترميز الآلي، إن متوسط الخطأ التربيعي (Mean Squared Error) هو التابع الأكثر استخداماً كتابع للخسارة.

$$L = \frac{1}{m}\sum_{i=1}^{m}(x_i - \hat{x}_i)^2 \qquad (2\text{-}10)$$

x_i : شعاع الدخل لعينة البيانات i، $\hat{x}_i$ شعاع الخرج لعينة البيانات i

2-3-2- أنواع شبكة الترميز الآلي (Types of Autoencoder)

بناءً على ما سبق، توجد مجموعة من القواعد التي يجب مراعاتها في بنية شبكة الترميز الآلي:

1. **عدد الطبقات:** يمكن اختيار عمق الشبكة (عدد الطبقات) كما نريد، ويعتمد ذلك على حجم البيانات.
2. **عدد العقد في كل طبقة:** يتناقص عدد العقد في كل طبقة بَعد المُرَمِّز ويزداد مرة أخرى في وحدة فك الترميز، ولكن هذا غير ضروري ويمكن أن نختار عدد العقد في كل طبقة وفقاً للحالة.
3. **حجم طبقة الترميز:** كُلَّما كان عدد العقد أقل في هذه الطبقة كان الضغط أكبر.

يؤدي كل خيار من الخيارات السابقة التي يمكن اعتبارها بارامترات فائقة، إلى أنواع مختلفة من شبكة الترميز الآلي [30]، وفيما يلي عرض للأنواع التي اعتمدت عليها الدراسة.

1. شبكة الترميز الآلي غير المكتملة (Undercomplete Autoencoder)

تتميز شبكة الترميز الآلي غير المكتملة بأن عدد العصبونات في الطبقة المخفية، أقل من عدد العصبونات في طبقة الدخل. ولذلك إن الهدف من هذه الشبكة، التقاط أهم الميزات الموجودة في البيانات، من خلال إجبار الشبكة على تَعلُّم التمثيل المضغوط للبيانات.

2. شبكة الترميز الآلي المتناثرة (Sparse Autoencoder)

تحتوي شبكة الترميز الآلي المتناثرة على عدد عُقد في الطبقة المخفية أكثر من طبقة الدخل؛ لكنها تبقى قادرة على التقاط أهم الميزات.

تُطبَّق عقوبة الانتثار (Sparsity Penalty) على الطبقة المخفية – قيمة صغيرة جداً أكبر من الصفر – لِمنع الشبكة من حفظ المدخلات ونسخها في طبقة الخرج (ملاءمة الشبكة للبيانات). تضاف هذه القيمة إلى خطأ إعادة البناء، كما في المعادلة الآتية.

$$L = \|x - g(f(x))\| + \Omega(h) \qquad (2\text{-}11)$$

x: دخل الشبكة، g: تابع مفكك الترميز، f: تابع المُرَمِّز

$\Omega(h)$: عقوبة الانتثار

تحتفظ الشبكة في أثناء التدريب بالعُقد المخفية النشطة، وتهمل العُقد غير النشطة. أي إن الشبكة لا تستخدم جميع العقد في الطبقة المخفية في وقت واحد، لذلك يَتِمُّ استخراج أهم الميزات من خلال تنشيط العُقد وإلغاء تنشيطها في الطبقات المخفية.

3. شبكة الترميز الآلي المكدسة (Stacked Autoencoder)

يَتِمُّ بناء الشبكة من خلال تكديس مجموعة من شبكات الترميز الآلي غير المكتملة. تُعتبر كُلّ شبكة طبقةً مخفيةً، مما يساعد في تمثيل البيانات ذات الأبعاد العالية في بُعد أقل، بمعنى إن كل طبقة مخفية تضغط البيانات على نحوٍ أكبر من الطبقة السابقة.

2-3-3- كشف الشذوذ القائم على الترميز الآلي

أصبح تقليل الأبعاد (Dimensionality Reduction) وتعلُّم الميزات ضمن مجموعات البيانات، باستخدام الشبكات العصبونية أمراً شائعاً في الآونة الأخيرة في سياق التَعلُّم العميق [31]. إن شبكة الترميز الآلي أحد أهم هذه الشبكات، إذ تتميز بقدرتها على تقليل الأبعاد غير الخطية، وتعلّم الأنماط المعقدة ضمن البيانات.

يعتمد كشف الشذوذ باستخدام شبكة الترميز الآلي على تعلُّم التمثيلات الطبيعية للبيانات، إذ يَتِمُّ بدايةً تدريب الشبكة على البيانات الطبيعية فقط لتعلُّم الأنماط والعلاقات المعقدة، تُصبح الشبكة بعد عملية التدريب قادرة على إعادة بناء البيانات الطبيعية على نحوٍ جيد للغاية، بينما تفشل في القيام بذلك مع البيانات الشاذة، تُعتبر نقاط البيانات التي لها خطأ إعادة بناء أعلى من حد معين نقاط شاذة.

يوضح الترميز الآتي استخدام شبكة الترميز الآلي لكشف الحالات الشاذة في مجموعات البيانات باستخدام عتبة تصنيف ثابتة [32].

Pseudo Code of Autoencoder based Anomaly Detection Algorithm	
Input:	$x^{(i)}$ // data points $i = 1 \dots N$ T // Fixed threshold, selected based on experience
Output:	reconstruction error $\|x - \hat{x}\|$

```
∅ , Θ ⟵ train an autoencoder using the normal dataset X
for i =1 to N do
    // encoder f_∅ , decoder g_Θ
    reconstruction error (i)= ‖x^(i) − g_Θ (f_∅ (x^(i)))‖
    if reconstruction error ( i ) > T then
            x^(i) is an anomaly
    else
            x^(i) is not an anomaly
    end if
end for
```

من خلال الترميز الزائف أعلاه، تعتمد شبكة الترميز الآلي لكشف الشذوذ على نمذجة البيانات الطبيعية أولاً، ثم تحديد عتبة تصنيف ثابتة بناءً على التجربة لفصل الحالات الشاذة عن الطبيعية.

2-4- الذاكرة قصيرة طويلة المدى (Long Short-Term Memory)

يُساعد الاعتماد على البيانات المتسلسلة، في نمذجة الترابطات المثيرة للاهتمام والتنبؤ بحالات الشذوذ المستقبلية. سَاعَدت التطورات السريعة في الآونة الأخيرة للشبكات العصبونية العميقة في توفير أداة قوية للتعامل مع هذا النوع من البيانات [33]. إن شبكات الذاكرة قصيرة طويلة المدى LSTMs هي الحل الأكثر فعالية للتسلسلات الزمنية، إذ تَتَمَيَّز LSTMs عن الشبكات العصبونية التقليدية بامتلاكها ذاكرة تساعدها على تذكر الأنماط والاحتفاظ بالتبعيات الزمنية (Temporal Dependencies) لفترات طويلة من الزمن، ومن ثَمَّ فهم السياق الكامن وراء هذه التسلسلات.

تحتوي LSTM على ما يسمى حالة الخلية (Cell State) وهي تمثل ذاكرة الشبكة، ويَتُّم في كُلّ خطوة الاحتفاظ بالمعلومات الضرورية والتخلص من المعلومات غير ذات الصلة [34] عن طريق بوابة النسيان (Forget Gate)، وبوابة الإدخال (Input Gate)، وبوابة الإخراج (Output Gate).

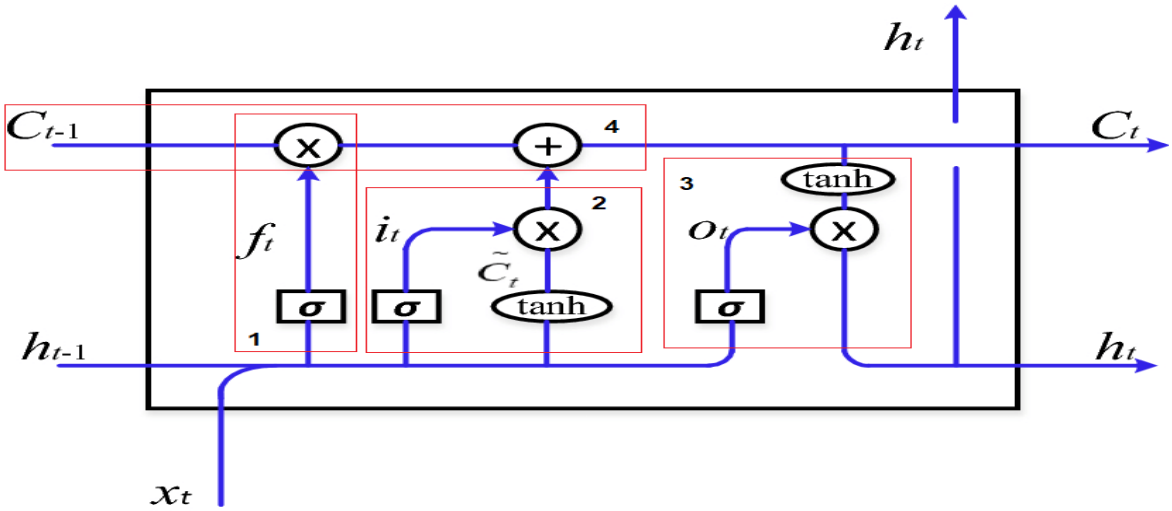
تحتوي المعلومات الموجودة ضمن الذاكرة (حالة الخلية) على ثلاث تبعيات، وهي كما يلي:

1. الحالة السابقة (المعلومات الموجودة بالذاكرة، في الخطوة الزمنية السابقة).

2. الحالة المخفية السابقة (خرج الخلية السابقة).
3. الحالة الحالية (المعلومات التي يتم إدخالها إلى الذاكرة، في الخطوة الزمنية الحالية).

2-4-1- مفاهيم الذاكرة طويلة المدى (LSTM Concepts)

يوضح الشكل الآتي بنية شبكة LSTM [35] التي تتكون من ثلاث بوابات.



الشكل 2-8 بنية الذاكرة قصيرة طويلة المدى

1. بوابة النسيان (Forget Gate)

يُمثل المربع الأول (1) بوابة النسيان: يَتِمُّ في هذه البوابة الإجابة عن السؤال الآتي: ما حالة الخلية السابقة التي يجب الاحتفاظ بها أو نسيانها؟

$$f_t = \sigma(w_f\,[h_{t-1}, x_t]) + b_f \qquad (2\text{-}12)$$

---

f_t : مُوَتِّر (Tensor) يستخدم كمرشح (Filter) للمعلومات الموجودة في حالة الخلية.

σ : تابع Sigmoid، x_t : حالة الدخل الجديد في اللحظة t.

h_{t-1} : الخرج السابق لحالة الخلية في الزمن $t-1$.

w_f: أوزان بوابة النسيان

يكون خرج البوابة إما 0 أو 1، حيث تُقابل القِيمَة 0 نسيان الحالة الداخلية (Internal State) السابقة على نحوٍ كامل، بينما تُقابل القِيمَة 1 تمرير الحالة من دون تغيير.

2. بوابة التحديث (الإدخال) (Update Gate)

يُمثل المربع الثاني (2) بوابة الإدخال: يَتِمُّ في هذه البوابة تحديد القِيَم المرشحة (Candidate) للدخل الحالي، للاحتفاظ بها في حالة الخلية الجديدة (الحالية).

$$\tilde{c}_t = \tanh(w_c\,[h_{t-1}, x_t]) + b_c \qquad (2\text{-}13)$$

$$i_t = \sigma(w_i\,[h_{t-1}, x_t]) + b_i \qquad (2\text{-}14)$$

يُستخدم التابع Tanh من أجل عملية تنظيم (Regulates) النموذج. إذ يَنتج عن التابع متجهة تحوي كل القِيَم (الحالات) التي يمكن إضافتها إلى حالة الخلية الجديدة، بينما يكون الهدف من استخدام تابع Sigmoid تحديد المعلومات الحالية التي يتم الاحتفاظ بها أو نسيانها.

3. بوابة الخرج (Output Gate)

يَتِمُّ في المربع الرابع (4) تحديث حالة الخلية السابقة c_{t-1} إلى حالة الخلية الجديدة c_t، من خلال ضرب الخلية السابقة بخرج بوابة النسيان، ومن ثم إضافة القِيَم المرشحة الجديدة الناتجة عن بوابة الإدخال.

$$c_t = f_t * c_{t-1} + i_t * \tilde{c}_t \qquad (2\text{-}15)$$

$i_t * \tilde{c}_t$ قيم مرشحة (خرج بوابة الإدخال)، f_t خرج بوابة النسيان

يُمثل المربع الثالث (3) بوابة الإخراج: يَتِمُّ في هذه البوابة الإجابة عن السؤال الآتي: ماذا سوف يكون خرج حالة الخلية الجديدة (الحالية) h_t ؟

$$O_t = \sigma(w_o\,[h_{t-1}, x_t] + b_o) \qquad (2\text{-}16)$$

$$h_t = O_t * \tan h(c_t) \qquad (2\text{-}17)$$

2-4-2- استخدام LSTM للتنبؤ بالشذوذ ضمن السلاسل الزمنية

يهدف استخدام الذاكرة طويلة المدى (LSTM) في مجال كشف الشذوذ إلى التنبؤ بحالة البيانات عند نقطة زمنية معينة [21]، من خلال دراسة التبعيات الزمنية لتسلسل الشذوذ ضمن سلاسل البيانات. تُمثل السلسلة الزمنية بالشكل الآتي:

$$x_t = \left\{x_t^{(1)}, x_t^{(2)}, \dots . x_t^{(k)}\right\} \qquad (2\text{-}18)$$

---

x_t: السلسلة الزمنية في الزمن t

k : عدد المتغيرات (الميزات)

$x_t^{(1)}$: قيمة الميزة الأولى في الزمن t

تستطيع شبكة LSTM التنبؤ بحالة الشذوذ ضمن السلاسل الزمنية المرصودة عند N نقطة زمنية، بالاعتماد على مفهوم النوافذ الزمنية المنزلقة (Sliding Window) بحجم m، حيث $m < N$. يتم تغذية الشبكة في نفس الوقت بعدد من السلاسل الزمنية المتعاقبة متعددة المتغيرات مساوية لحجم النافذة m.

تستخدم الشبكة المدخلات $m * k$، للتنبؤ بالقيمة التالية للميزة $x_*^{(K)}$ التي تشير إلى تصنيف السلسلة. إن دخل الشبكة من أجل النافذة الزمنية الأولى هي السلاسل الزمنية المتعاقبة $\{x_1, x_2, \dots . x_m\}$، عندئذٍ يمكن للشبكة التنبؤ بالقيمة $\hat{x}_{m+1}^{(K)}$. بينما يمكنها التنبؤ بالقيمة $\hat{x}_{m+2}^{(K)}$ بالاعتماد على تسلسل البيانات ضمن النافذة الزمنية الثانية $\{x_2, x_3, \dots . x_{m+1}\}$. يستمر انزلاق النافذة إلى نهاية مجموعة بيانات التدريب. تهدف الشبكة في أثناء عملية التدريب، إلى تصغير تابع الخسارة لخطأ التنبؤ لجميع النوافذ الزمنية، توضح المعادلة الآتية حساب خطأ التنبؤ.

$$e = \sum_{i=m+1}^{N} || \hat{x}_i^{(K)} - x_i^{(K)} || \qquad (2\text{-}19)$$

يمكن بعد حساب قيم الخطأ لجميع النوافذ الزمنية، تطبيق تابع الخسارة للشبكة على نحوٍ مشابه للمعادلة (2-10). تستطيع الشبكة بعد عملية التدريب، توقع القيمة $\hat{x}_{N+1}^{(k)}$ بناء على سلسلة الدخل $\{x_{N-m+1}, x_{N-m+2}, \dots . x_N\}$.

2-5- شبكة الترميز الآلي ذات الذاكرة طويلة المدى (LSTM Autoencoder)

يُمكن تنظيم شبكة LSTM Autoencoder بالاعتماد على بنية مشابهة لشبكة Autoencoder، تسمى Encoder–Decoder LSTM [36] ويكون فيها كل من المُرَمِّز (Encoder) ومفكك الترميز (Decoder) هو شبكة LSTM. يكون الهدف من استخدام LSTM ضمن المُرَمِّز ومفكك الترميز هو التقاط التبعيات الزمنية ضِمْنَ سلاسل البيانات.

تُساعد شبكة LSTM Autoencoder على تقليل أبعاد البيانات واختزالها في بُعد أصغر، مع الاحتفاظ بالمعلومات الرئيسية لهيكلية البيانات باستخدام خصائص شبكة الترميز الآلي، وتَعلُّم الأنماط المعقدة داخل الترتيب الزمني لتسلسل الإدخال باستخدام شبكة الذاكرة قصيرة طويلة المدى. كما تساعد في المحافظة على التبعيات الزمانية بين مكونات متجهة الخرج المتوقع.

2-5-1- كشف الشذوذ القائم على LSTM Autoencoder

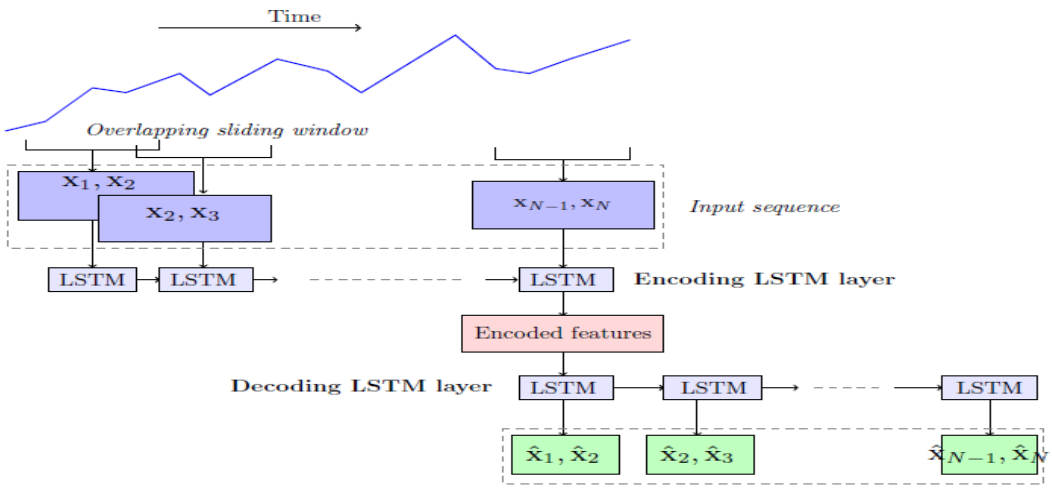
إن المبدأ الرئيسي لاستخدام شبكة LSTM–Autoencoder في مسائل اكتشاف الشذوذ، هو تدريبها على تسلسل البيانات الطبيعية فقط، مما يجعلها قادرة على إعادة بناء هذه التسلسلات على نحوٍ جيد، أما عند تغذيتها بتسلسل غير طبيعي (شاذ) فلا تكون قادرة على إعادة بنائه على نحوٍ جيد. إن تدريب الشبكة بهذه الطريقة له معنى عملي لأن البيانات الشاذة ليست متاحة دائماً، كما أنه من المستحيل تغطية جميع أنماط هذه البيانات.

بفرض أن $X = \{x_1, x_2, \ldots\ldots, x_N\}$ يشير إلى تسلسل زمني طبيعي يستخدم لتدريب الشبكة. وليكن $x_t = \left\{x_t^{(1)}, x_t^{(2)}, \ldots. x_t^{(k)}\right\}$ سلسلة زمنية متعددة المتغيرات في الوقت t. يمكن للشبكة باستخدام نافذة منزلقة بحجم m، قراءة التسلسل الزمني $x_i = x_t \ldots x_{t+m-1}$، ومن ثم يمرر إلى وحدة الذاكرة طويلة المدى (LSTM) لالتقاط التبعيات الزمنية ضمن التسلسل، يتم بعد ذلك ضغط خرج وحدة الذاكرة طويلة المدى باستخدام المُرَمِّز، لاستخراج الميزات الأكثر أهمية. تمرر السلاسل المضغوطة إلى وحدة مفكك الترميز لإعادة بنائها بالشكل الآتي: $\hat{x}_i = \hat{x}_t \ldots \hat{x}_{t+m-1}$، حيث إن $i = m + 1..N$

يتم حساب خطأ إعادة البناء $\{e_1, e_2, \ldots. e_n\}$ لجميع السلاسل الزمنية في التسلسل الطبيعي X، كما في المعادلة الآتية:

$$e_i = \left|\left|\hat{x}_i - x_i\right|\right|, i = m + 1..N \qquad (2\text{-}20)$$

يمكن فرض أن متجهات الخطأ تتبع توزيع غاوس متعدد المتغيرات [36]، ومن ثم استخدام تابع خسارة مثل likelihood لتقدير قيمة العتبة T. ومن ثَمَّ تكون جميع التسلسلات التي لها خطأ إعادة بناء أكبر من العتبة هي تسلسلات لحالات شاذة. يوضح **الشكل 2-9** عمل الشبكة LSTM Autoencoder باستخدام نافذة منزلقة بحجم 2.



الشكل 2-9 آلية عمل شبكة LSTM-Autoencoder

2-5-2- البارامترات الفائقة لشبكات التعلم العميقة

فيما يلي عرض للبارامترات الفائقة [37] المستخدمة في تدريب الشبكات العميقة السابقة:

- **تابع التنشيط (Activation Function)**

يُحدد آلية تحويل الأوزان الموزونة (Weights Weighted) للمدخلات إلى قِيمَة محددة تُمثل خرج العُقد. يُعدّ لاختيار تابع التنشيط تأثير كبير على قدرة الشبكة العصبونية وأدائها. يُوصى عادةً باستخدام تابع التنشيط نفسه في جميع الطبقات المخفية. توجد مجموعة واسعة من توابع التنشيط أهمها:

a. Logistic (Sigmoid): يحدد قِيمَة خرج العقد ضمن المجال $[0,1]$ ، والصيغة الرياضية للتابع هي بالشكل الآتي:

$$\text{sigmoid}(x) = 1.0/(1.0 + e^{-x}) \qquad (2\text{-}21)$$

b. Hyperbolic Tangent (Tanh): يحدد قِيمَة خرج العقد ضمن المجال $[-1,1]$ ، والصيغة الرياضية للتابع هي بالشكل الآتي:

$$\tanh(x) = (e^{x} - e^{-x})/(e^{x} + e^{-x}) \qquad (2\text{-}22)$$

c. Rectified Linear Activation (ReLU) : يحافظ على قِيَم الإدخال الموجبة، بينما يكون الخرج مساوياً للصفر من أجل قِيَم الإدخال السالبة. الصيغة الرياضية للتابع هي بالشكل الآتي:

$$\text{Relu}(x) = \max(0.0, x) \qquad (2\text{-}23)$$

d. Linear: لا يغير التنشيط الخطي المجاميع الموزونة للمدخلات، إذ تُمرر قيمة الأوزان مباشرةً.

$$\text{linear}(x) = x \qquad (2\text{-}24)$$

$$where\ x\colon \sum(weights * input + bais)$$

تعتبر توابع Sigmoid، Tanh، ReLU أكثر استخداماً من أجل الطبقات المخفية، بينما يستخدم Sigmoid وLinear من أجل طبقة الخرج.

- **معدل التَعلُّم (Learning Rate)**

يُشير إلى مقدار خطوة الانتشار الخلفي (Backpropagation) عند تحديث الأوزان، يَتُم ضبطه بقيم صغيرة جداً. إن القيمة الافتراضية هي 0.01.

- **حجم الدفعة (Batch Size)**

يؤدي تغذية الشبكات العصبونية بكل البيانات دفعة واحدة إلى نتائج عكسية. إحدى الممارسات الجيدة هي تزويدها بعينات صغيرة من البيانات الأصلية تسمى الدفعات، تُمثل الدفعة عدد العينات التي يَتُم تغذية الشبكة بها في كُلَ مرة. الحجم النموذجي هو 32 أو أعلى ومن مضاعفات العدد 2.

- **معدل التسريب (Dropout Rate)**

يفيد هذا البارامتر في تسريب بعض العقد ضمن الطبقة، التي تكون زائدة وغير مجدية، وتؤدي إلى ملاءمة زائدة (Overfitting) للبيانات. يمكن الاحتفاظ في أثناء التدريب بكل العقدة ذات احتمال p (احتمال الاحتفاظ) أو تسريبها باحتمال $1 - p$ (احتمالية التسريب /Dropout Rate).

على سبيل المثال من أجل $p = 0.5$ ، يَتِمُّ تسريب عشوائي (حذف مؤقت) لنصف عدد العقد في الطبقة خلال الدفعة الحالية، بينما تتغير مجموعة العقد المسربة من أجل الدفعات الأخرى، وتستمر هذه العملية حتى نهاية تدريب الشبكة.

- **حقبة (Epoch)**

تمثل مقدار الوقت الذي تحتاجه الشبكة من أجل أن تتدرب على مجموعة البيانات بأكملها[1].

- **العقد (Nodes)**

تُمَثل عدد العصبونات في طبقات الشبكة. يَتُم ضبط عدد العقد في النموذج المُقْتَرَح ضِمْنَ البحث الحالي، إلى النصف في كل طبقة تالية في المُرَمِّز، ومن ثمَّ مضاعفته رجوعاً في مفكك الترميز. على سبيل المثال، من أجل عدد عقد 32 وشبكة مكونة من ست طبقات مخفية، تكون العقد بالشكل الآتي [32,16,8,8,16,32].

[1] يجب التنبيه على أن مصطلح Epoch يختلف عن مصطلح التكرار (Iterations)، إذ يشير الأخير إلى عدد الدفعات اللازمة لإكمال مرحلة كاملة.

الفصل الثالث

مقاييس البحث وأدواتُهُ

يتضمن هذا الفصل شرحاً لأهم مقاييس الأداء المستخدمة في تقييم أداء أنظمة كشف الشذوذ، وبيان الحالة الأفضل لاستخدام هذه المقاييس كلّ على حِدة. بالإضافة إلى ذلك يعرض مجموعات البيانات البحثية المستخدمة ضمن الدراسة. من ثم يعرض الحزم والمكتبات المستخدمة في بناء النظام المقترح.

3-1- مقاييس الأداء (Performance Metrics)

يوجد مجموعة من المقاييس التي تُستخدم لتقييم خوارزميات التصنيف وفقاً لهدف التجربة المدروسة. مع أن اختيار المقاييس المناسبة يُعدّ مسألة مهمة في تفسير عمل الأنظمة عموماً، فإنه لم يَتِمُّ التوصل حتى الآن إلى إجماع كبير حول مقياس موحّد لتقييم جميع الحالات المحتملة لعمل الأنظمة.

يُعتَبر مقياس الدقة (Accuracy) المقياس الأكثر استخداماً والأكثر منطقية في تقييم أداء خوارزميات التصنيف وذلك حين تكون مجموعات البيانات متوازنة. فهو يمثل النسبة بين عدد العينات المصنفة على نحوٍ صحيح وعدد العينات الكليّة. ولكن بالمقابل لا يمكن اعتباره مقياساً جيداً في البيانات غير المتوازنة (كما في حالة اكتشاف الشذوذ) [38] لأنه يسبب ملاءمة زائدة (Overfitting) لجهة صف الأغلبية.

توجد مجموعة واسعة من المقاييس التي يمكن استخدامها لتقييم أداء الأنظمة عند التعامل مع بيانات غير متوازنة، ويمكن تقسيم هذه المقاييس إلى فئتين رئيستين هما:

1. **المقاييس الإحصائية.**
2. **المقاييس البيانية.**

فيما يلي عرض لما تَمّ استخدامه ضمن الدراسة في تقييم أداء نظام كشف الشذوذ المقترح، كونها الأكثر استخداماً عند التعامل مع مسائل كشف الشذوذ.

3-1-1- المقاييس الإحصائية (Statistical Metrics)

تُستخدَم هذه المقاييس عند توفر قيمة إحصائية، تدعى العتبة (Threshold) لمصفوفة الارتباك (Confusion Matrix). من أهم الأمثلة الاسترجاع (Recall) والدقة (Precision).

تُعدّ المقاييس الإحصائية هي الأكثر استخداماً في تقييم أنظمة كشف الشذوذ، تعتمد جميع هذه المقاييس على عناصر مصفوفة الارتباك.

1. مصفوفة الارتباك (Confusion Matric)

تُستخدَم مصفوفة الارتباك لوصف أداء نماذج التصنيف، وهي عبارة عن جدول يُصنّف عينات البيانات إلى تسميتها المتوقعة (إيجابية أو سلبية وفي حالة الدراسة الحالية طبيعية وشاذة)، لتقع كل عينة في نهاية المطاف ضمن إحدى الحالات الآتية:

1) الإيجابيات الصحيحة (True Positives TP) تدل على القيم الإيجابية (الشاذة) المتوقعة على نحوٍ صحيح.
2) السلبيات الصحيحة (True Negatives TN) تدل على القيم السلبية (الطبيعية) المتوقعة على نحوٍ صحيح.
3) الإيجابيات الخاطئة (False Positives FP) والسلبيات الخاطئة (False Negatives FN) عندما يتعارض الصف الحقيقي مع الصف المتوقع.

يمكن تلخيص الحالات السابقة ضمن مصفوفة 2*2 $M = \begin{pmatrix} TP & FN \\ FP & TN \end{pmatrix}$. يوضح **الشكل 3-1** مصفوفة الارتباك على نحوٍ أوضح.

		Predicted Class: Positive	Predicted Class: Negative	
Actual Class	Positive	True Positive (TP)	False Negative (FN) Type II Error	**Sensitivity** $\frac{TP}{(TP+FN)}$
	Negative	False Positive (FP) Type I Error	True Negative (TN)	**Specificity** $\frac{TN}{(TN+FP)}$
		Precision $\frac{TP}{(TP+FP)}$	**Negative Predictive Value** $\frac{TN}{(TN+FN)}$	**Accuracy** $\frac{TP+TN}{(TP+TN+FP+FN)}$

الشكل 3-1 مصفوفة الارتباك

يظهر بوضوح من خلال مصفوفة الارتباك، أن العينات الإيجابية هي مجموع الإيجابيات الصحيحة والسلبيات الخاطئة ($TP + FN = n^+$)، والعينات السلبية هي مجموع السلبيات الصحيحة والإيجابيات الخاطئة ($TN + FP = n^-$). يسعى أي مصنف للحصول على أكبر عدد من الإيجابيات

الصحيحة TP والسلبيات الصحيحة TN، وعدد أقل من الإيجابيات الخاطئة FP والسلبيات الخاطئة FN. يكون المصنف في حالته المثالية عندما تكون مصفوفة الارتباك بالشكل $M = \begin{pmatrix} n^+ & 0 \\ 0 & n^- \end{pmatrix}$.

لا يمكن في الحقيقة تحليل جميع عناصر مصفوفة الارتباك على نحوٍ منفصل، إذ يعتبر ذلك هدراً للوقت. قدّم الباحثون لتفادي تلك المشكلة مجموعة من المقاييس الإحصائية المفيدة والقادرة على وصف جودة التصنيف على الفور [39]، كالدقة والاسترجاع وغيرها.

2. الاسترجاع (Recall) والدقة (Precision)

يمكن تمثيل العينات الإيجابية والسلبية على أنها عينات ذات صلة أو غير ذات صلة بالبيانات الشاذة على التوالي. ومن ثَمَّ يُعبّر مقياس الاسترجاع (مقياس الدقة في صف العينات الإيجابية) عن نسبة العينات ذات الصلة التي تم استرجاعها على نحوٍ صحيح. بينما يُعرَّف مقياس الدقة على أنه نسبة العينات المسترجعة ذات الصلة. يوفر كُلّ من زوج دقة واسترجاع رؤية مفيدة في سلوك المصنف، كما يؤدي الجمع بين هذين المقياسين إلى إنشاء مقاييس تقييم ذات فعالية، وعلى وجه التحديد مقياس F1 والذي يمثل المتوسط التوافقي بين كل من الدقة والاسترجاع.

يُعرَّف مقياس الاسترجاع رياضياً [39]، بأنه نسبة عدد الإيجابيات الصحيحة (TP) على مجموع كُلّ من الإيجابيات الصحيحة (TP) والسلبيات الخاطئة (FN).

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \qquad (3\text{-}1)$$

يُعرَّف مقياس الدقة رياضياً [39]، بأنه نسبة عدد الإيجابيات الصحيحة (TP) على مجموع كُلّ من الإيجابيات الصحيحة (TP) والإيجابيات الخاطئة (TN).

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \qquad (3\text{-}2)$$

لتوضيح المقياسين السابقين ضمن سياق الشذوذ، نفرض وجود مجموعة بيانات تحتوي على 10 حالات شاذة، وإن نظام الكشف صنف 20 حالة على أنها شاذة، ومن بينها الحالات الشاذة الصحيحة. عندئذٍ تكون نسبة الاسترجاع 100% ونسبة الدقة 50%.

3. مقياس F1 Score

يُعدّ $F1$ في التحليل الإحصائي مقياساً لدقة الاختبار، فهو المتوسط التوافقي للدقة والاسترجاع. تُحسَب قيمة $F1$ بالاعتماد على مصفوفة الارتباك بالشكل الآتي:

$$\text{F1 score} = \frac{2 * \text{TP}}{2 * \text{TP} + \text{FP} + \text{FN}} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \quad (3\text{-}3)$$

تقع قيم المقياس $F1$ ضمن النطاق [0,1]، إذ تقابل القيمة 1 أفضل نتيجة، بينما 0 أسوأها. نحصل على $F1 = 0$ عندما $TP = 0$، أي أن جميع العينات الإيجابية صُنِّفت بشكل خاطئ. بينما نحصل على الحالة المثالية $F1 = 1$ عندما $FN, FP = 0$، أي إن جميع العينات صُنِّفت على نحوٍ صحيح.

نتيجةً لاختلاف أداء مقياس $F1$ عند مبادلة الصفوف (Classes Swapping)، فإننا نميز حالتين مختلفتين لمقياس $F1$، وذلك عندما يُهيمن صف الأغلبية على نحوٍ كامل ضمن المصنف. تختلف هاتان الحالاتان بناءً على ما يحتويه صف الأغلبية من عينات (هل هي سلبية أم إيجابية؟). تكون قيمة المقياس من أجل كل حالة وفق الآتي:

a) $if\ n^+ > n^-, then\ M = (n^+, 0\ , n^-, 0)\ and\ f1 = \frac{2n^+}{2n^+ + n^-}$

b) $if\ n^- > n^+\ then\ M = (0, n^+, 0, n^-), so\ that\ f1 = 0$

تَمّ إدخال مفهوم متوسط Macro عند حساب قيمة $F1$ للحد من مشكلة مبادلة الصفوف [40]، حيث يعطي المتوسط أوزاناً متساوية لِكلّا الصفين. ولذلك فإنه يزيد من أهمية صف الأقلية. يُعطى مقياس $F1\ macro$ بالصيغة الآتية:

$$\text{F1 score}_{\text{macro}} = 2 * \frac{\text{precision}_{\text{macro}} * \text{recall}_{\text{macro}}}{\text{precision}_{\text{macro}} + \text{recall}_{\text{macro}}} \quad (3\text{-}4)$$

$$recall_{macro} = \frac{recall^+ + recall^-}{2}, precision_{macro} = \frac{precision^+ + precision^-}{2}$$

4. معامل ارتباط ماثيوز (MCC: Matthews Correlation Coefficient)

يستخدم مقياس MCC للتغلب على مشكلة البيانات غير المتوازنة، فهو يعبر عن الارتباط بين القيم المتوقعة والحقيقية. تعتمد قيمة MCC على جميع عناصر مصفوفة الارتباك، ولذلك يحد من مشكلة مبادلة الصفوف. يعطى معامل ارتباط ماثيوز بالصيغة الرياضية الآتية.

$$\text{MCC} = \frac{\text{TP} * \text{TN} - \text{FP} * \text{FN}}{\sqrt{(\text{TP} + \text{FP}) * (\text{TP} + \text{FN}) * (\text{TN} + \text{FP}) * (\text{TN} + \text{FN})}} \quad (3\text{-}5)$$

تمثل القيمة 1 أفضل نتيجة، بينما 1− أسوؤها، أما القيمة 0 فهي للدلالة على عشوائية النموذج. يُعتَبر MCC المقياس الوحيد الذي يُستخدَم لمعرفة إن كان المصنف الثنائي قادراً على توقع معظم الحالات الإيجابية والسلبية بشكل صحيح [40].

يصبح معامل ارتباط ماثيوز غير محدد $MCC = 0$، عندما يوجد سطر أو عامود كامل في مصفوفة الارتباك مساوياً للصفر، وهذه الحالة مشابهة لحالة تحيّز النموذج لصف الأغلبية. يوجد مجموعة من الإجراءات الرياضية للتغلب على هذه المشكلة كإضافة قيمة صغيرة جداً ε إلى المعامل. أما عند وجود عنصر وحيد غير صفري في مصفوفة الارتباك، فهذا يعني أن جميع العينات في مجموعة البيانات تنتمي إلى صف واحد؛ إما جميع العينات مصنَّفة على نحوٍ صحيح ($TP \neq 0 \; or \; TN \neq 0$)، أو جميعها مصنَّفة على نحوٍ غير صحيح ($FP \neq 0 \; or \; FN \neq 0$)، يكون $MCC = 1$ من أجل الحالة الأولى، بينما من أجل الحالة الثانية $MCC = -1$.

5. معدل الإيجابيات الخاطئة (False Positive Rate)

يقيس معدل الإيجابيات الخاطئة (FPR) النسبة بين عدد الحالات السلبية التي صُنِّفت على أنها إيجابية (الإيجابيات الخاطئة FP) وإجمالي عدد الحالات السلبية بغض النظر عن تصنيفها.

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \qquad (3\text{-}6)$$

6. نسبة الفشل (Failure Rate)

قد يكون في بعض الحالات للمقاييس المستخدمة نفس القيم، نحتاج عندئذٍ إلى تفاضل بين هذه الحالات. اقترحت الدراسة لتحقق ذلك ما يسمى نسبة الفشل (Failure Rate)، وتمثل نسبة كُلّ من السلبيات الخاطئة (تصنيف الحالات الشاذة على أنها طبيعية) والإيجابيات الخاطئة (تصنيف الحالات الطبيعية على أنها شاذة). يجب أن تكون قيمة هذه النسبة أقل ما يمكن لتحقيق أفضل أداء لنظام كشف الشذوذ.

$$\text{Failure rate} = \frac{\mathrm{FP} + \mathrm{FN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} \qquad (3\text{-}7)$$

3−1−2− المقاييس البيانية (Graphic Metrics)

يوجد مجموعة من المقاييس التي يمكن الاعتماد عليها عند عدم القدرة على توفر عتبة مصفوفة الارتباك، تُعَدّ منحنيات الدقة والاسترجاع (PR: Precision−Recall Curves)، ومنحنيات خصائص المستقبل التشغيلية (ROC: Receiver Operating Characteristic) الأكثر شيوعاً.

1. منحنيات خصائص المستقبل التشغيلية (ROC)

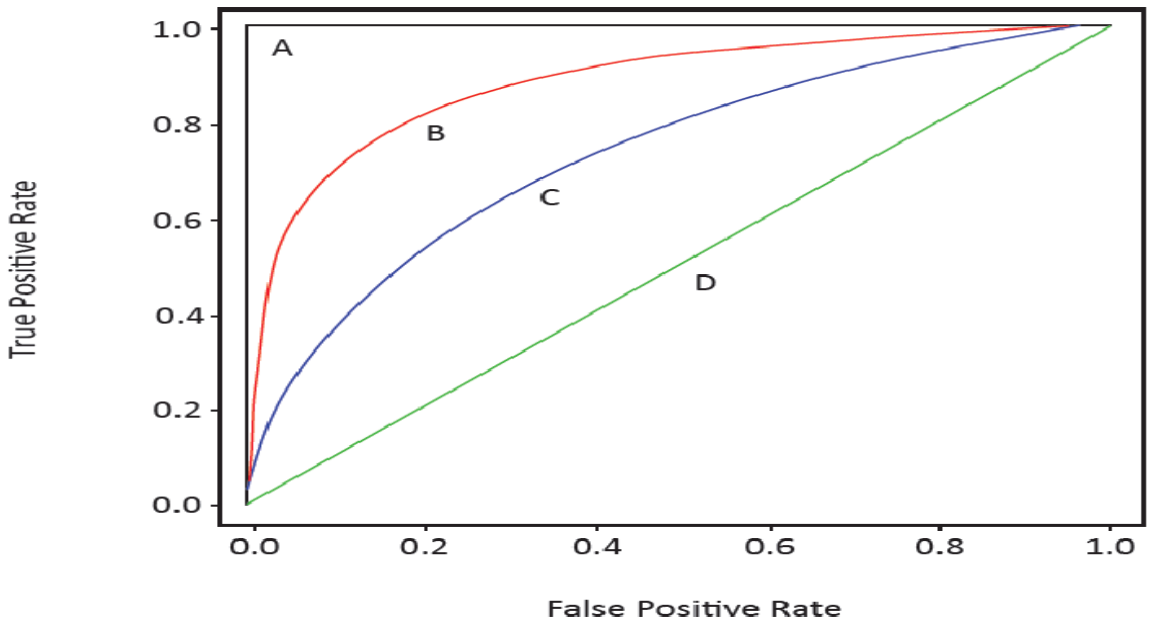
يُعبّر المنحني ROC عن العلاقة بين معدل الإيجابيات الصحيحة TPR (المحور العامودي)، ومعدل الإيجابيات الخاطئة FPR (المحور الأفقي) من أجل قيم مختلفة للعتبات [41].

تقيس منحنيات ROC درجة الفصل بين الصفوف بالاعتماد على مساحة السطح تحت المنحني (AUC: Area Under the Curve). تتراوح قيم AUC ضمن المجال [0,1]، يُعتبر النموذج أكثر دقة مع ازدياد قيمة AUC حيث يزداد الفصل والتمايز بين الصفوف. يكون المصنف في الحالة المثالية عندما $AUC = 1$ وفي أسوء حالاته عندما $AUC = 0$، أما عندما $AUC = 0.5$ يُعتبر المصنف عشوائياً.

تُمثل كُلّ نقطة من المنحني إحداثياتها TPR وFPR، قيمة عتبة T. لذلك يَتُّم رسم منحني ROC من خلال مجموعة النقاط المولدة من تغير قيمة T من الصفر إلى الواحد، إذ يبدأ منحني ROC من النقطة (0,0) وينتهي بالنقطة (1,1). يُعتبر النموذج ذا أداء جيد عندما يزداد المنحني على نحوٍ سريع من الصفر إلى الواحد، حيث يعني ذلك أن النموذج يُضحّي بقليل من الدقة مقابل الحصول على استرجاع عالٍ.

يُبيّن **الشكل 3-2** مجموعة من منحنيات ROC، حيث يدل المنحني D على أداء منخفض للنموذج لأنه يتخلى عن كثير من الدقة للحصول على استرجاع أعلى ($AUC = 0.5$). يدل المنحني A على أداء جيد للنموذج لأنه يحافظ على توازن كبير بين الاسترجاع والدقة ($AUC = 1$). يقع كُلّ من المنحنيين B وC بين الحالتين السابقتين، مع الإشارة إلى أن B أفضل من C لأن مساحة السطح تحت المنحني أكبر.

لا يُعَدّ المنحني ROC كافياً في البيانات غير المتوازنة كحالة البيانات المستخدمة في الدراسة، حيث لا ينخفض معدل الإيجابيات الكاذبة بشكل ملحوظ عندما تكون السلبيات الصحيحة TN كبيرة جداً –وذلك وفقاً للمعادلة الرياضية (3-6) لعدم وجود TN ضمن المقام–. لذلك لا يمكن الاعتماد فقط على منحني ROC في حالة البيانات غير المتوازنة حيث يمكن ببساطة الحصول على مُنحَنٍ جيد بتوقع كُلّ الحالات ضمن صف الأغلبية.



الشكل 3-2 حالات منحني ROC

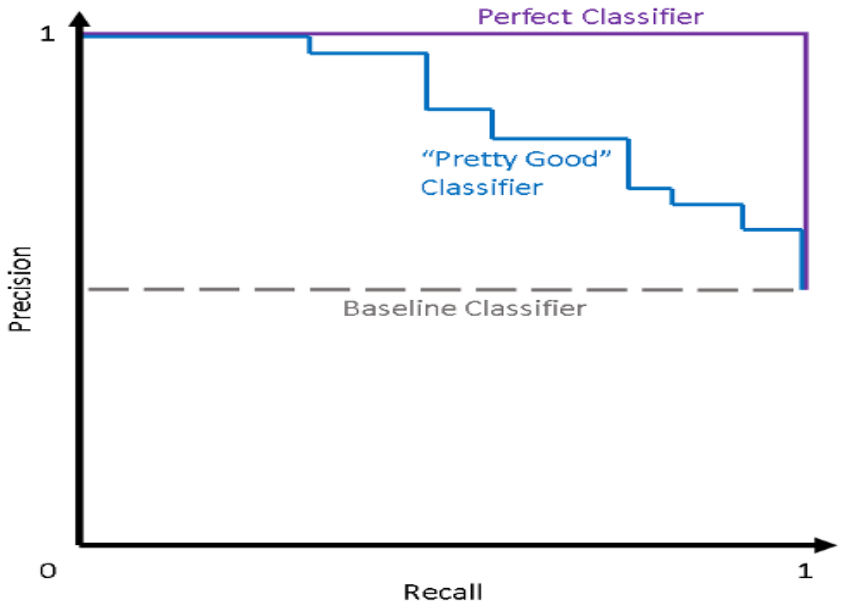
2. منحنيات الدقة والاسترجاع (PR)

يُوصَى عادةً بمنحنيات الدقة والاسترجاع عند التعامل مع مجموعات بيانات غير متوازنة، فقد توفر منحنيات ROC كما ذكرنا سابقاً رؤية مضللة ومنحازة لصف الأغلبية [42].

يوفر منحني PR رؤية بصرية لِكُلّ من الدقة (المحور العامودي) والاسترجاع (المحور الأفقي)، ومن أجل قيم عتبات مختلفة بدلاً من قيمة واحدة. تدل قيمة AUC من أجل منحني PR كما في منحني ROC.

بما أن المنحني PR يوضح العلاقة بين الدقة والاسترجاع فإنه لا يأخذ بيعن الاعتبار السلبيات الحقيقية TN وفق المعادلات الرياضية للدقة والاسترجاع (3-1) (3-2) لذا تكون هذه المنحنيات مفيدة عندما تمثل العينات الإيجابية صف الأقلية، أما إذا كانت العينات السلبية هي النادرة لا يُنصَح باستخدام هذه المنحنيات.

يقابل أفضل أداء للنموذج (Perfect Classifier) عند إحداثيات النقطة (1,1)، بينما تتوافق أسوء حالة للنموذج مع خط مستقيم أفقي (Baseline Classifier) بدقة تتناسب مع عدد العينات الإيجابية، يكون من أجل البيانات المتوازنة $L = 0.5$. يوضح **الشكل 3-3** الحالات المختلفة لمنحني الدقة والاسترجاع PR.



الشكل 3-3 حالات منحني PR

تختلف المقاييس المستخدمة لتقيم أداء المصنف المحدد، بناء على طبيعة النظام المدروس والغاية منه. مما يجعل من الصعب تحديد مقياس شامل لجميع الحالات. يَحظى كُلّ من F1 وMCC بمستوى انتشار أوسع في الأدبيات السابقة [43]، إذ يوفر هذين المقياسين تقديرات أكثر واقعية لأداء النماذج في العالم الحقيقي.

3-2- مجموعات البيانات البحثية (Research Datasets)

تَمَّ الاعتماد ضمن الدراسة على عدد من مجموعات البيانات الحقيقية، إذ تُمثل هذه المجموعات مجالات مختلفة في تطبيقات الكشف عن الشذوذ.

1. مجموعة بيانات الاحتيال الأوروبية (European Fraud Dataset)

تمثل مجموعة البيانات المقترحة، عدد من معاملات بطاقات ائتمان أوربية تمت على مدار يومين في أيلول عام 2013، وتُعِدّ من أكثر مجموعات البيانات الحقيقيّة المتاحة في الدراسات حتى الآن. تحتوي مجموعة البيانات على 284807 معاملة (سجل)، منها 492 معاملة احتيالية (حوالي 0.17٪) [44]، مما يجعل مجموعة البيانات هذه غير متوازنة (Unbalanced Dataset) إلى حد كبير.

تُمَثّل كل معاملة بـ 30 ميزة (Feature) جميعها رقمية. تَمَّ تحويل القيم الأصلية لـ 28 من هذه الميزات باستخدام تحليل المكونات الرئيسية (Principal Component Analysis)، وسُميت بأسماء من V1 وحتى V28، ولم يتم الكشف عن معلومات حول هذه الميزات لأسباب تتعلق بالسرية. كما لا يتوفر

أي معلومات عن مُعِّرف حامل البطاقة ID حيث يتم اعتبار كل معاملة مستقلة عن المعاملات الأخرى. تُعبّر ميزة الوقت (Time) عن الثواني المنقضية بين كل معاملة والمعاملة الأولى، وتحوي ميزة الكمية (Amount) مبلغَ المعاملة. يُعَدّ المتغير Class متغير الاستجابة ويأخذ القيمة 1 في حالة المعاملات الاحتيالية و0 على خلاف ذلك. يُلخص **الجدول 3-1** مجموعة بيانات الاحتيال الأوروبية.

الجدول 3-1 وصف بيانات الاحتيال الأوروبية

Element Type	No.	Remark
المتغيرات المستمرة (Continuous variables)	28	**V1 ~V28, Time, Amount**
الحالات الطبيعية (Normal)	284378	Class = 0
الحالات الشاذة (Abnormal)	492	Class = 1

2. مجموعة بيانات الاحتيال المجردة (Abstract Fraud Dataset)

تُعبر البيانات المجردة عن مجموعة من القيم والعمليات المحتملة من وجهة نظر محلل البيانات، وليس من وجهة نظر المستخدم. لذلك هي تصمم بهدف إجراء تصميم وتحليل الأنظمة. تحاكي مجموعة البيانات المقترحة [45] عدد من المعاملات المالية والميزات الهامة المكونة لها. تضم هذه المجموعة 3075 معاملة، منها 448 معاملة احتيالية (حوالي 14.6٪). تُمَثّل كل معاملة بـ 12 ميزة بعضها رقمية، والبعض الأخر فئوية (Categorical). توفر هذه الميزات معلومات عن تاريخ المعاملة، ومتوسط مبلغ المعاملة في اليوم الواحد، وعدد حالات الرفض في اليوم، ومبلغ المعاملة المفروضة، وهل هي معاملة غريبة (خارجية)؟، وهل البلد شديد الخطورة؟، ومتوسط مبالغ تَحُّمل التكاليف يومياً، ومتوسط مبالغ تَحمُّل التكاليف لمدة ستة أشهر، وعدد مرات دفع مبالغ التكاليف لمدة ستة أشهر. (يمثل مبالغ تحمل التكاليف، الرسوم التي يتم إرجاعها إلى حساب العميل بعد أن ينجح في الاعتراض على معاملة معينة). يلخص **الجدول 3-2** مجموعة البيانات المجردة المستخدمة.

الجدول 3-2 وصف بيانات الاحتيال المجردة

Element Type	No.	Remark
المتغيرات المستمرة (Continuous variables)	8	• Merchant_id • Transaction date • Average Amount • Transaction_amount • Total Number of declines • Daily_chargeback_avg_amt • 6_month_avg_chbk_amt • 6-month_chbk_freq
المتغيرات الفئوية (Categorical variables)	4	• Is declined • isForeignTransaction • isHighRiskCountry • isFradulent
الحالات الطبيعية (Normal)	2627	isFradulent = N
الحالات الشاذة (Abnormal)	448	IsFradulent = Y

3. مجموعة بيانات كسر الورق (Paper Break Dataset)

تُمَثل البيانات المستخدمة مجموعة بيانات حقيقية تتعلق بمشكلة كسر الورق. قُدِّمَتْ هذه المجموعة ضِمْنَ مسابقة البيانات المقامة في معهد أنظمة المهندسين الصناعيين (Institute of Industrial and Systems Engineers) لعام 2019. تَمَّ جَمْع المشاهدات من أحد معامل صناعة اللب والورق [46] على مدار شهر واحد باستخدام مجموعة متنوعة من أجهزة الاستشعار. تَقيس هذه المستشعرات المواد الخام (مثل كمية الألياف اللبيّة والمواد الكيميائية وغيرها)، ومتغيرات العملية (مثل نوع الشفرة وسرعة الدوران). تَتَضَّمن مجموعة البيانات قراءات 61 مستشعر عند 18398 نقطة زمنية ضِمْنَ فترات منتظمة (كل دقيقتين)، مع تحديد حالة النظام (طبيعي أو شاذ) عند كُلّ نقطة. ومع أن هذا العدد كان كبيراً من القياسات، كانت حالات الفشل تحدث فقط عند 124 نقطة زمنية (0.67٪ من إجمالي الملاحظات) في أثناء التشغيل مما يجعل من الصعب التنبؤ بالفشل قبل حدوثه؛ لكن أي تقليل لحالات الفشل بواسطة الاكتشاف المبكر، يوفّر قدراً كبيراً من تكاليف الانتاج. يُلّخص **الجدول 3-3** مجموعة بيانات كسر الورق.

الجدول 3-3 وصف بيانات كسر الورق

Type Element	No.	Remark
المتغيرات المستمرة (Continuous variables)	59	**X**1 ~**X**27, **X**29 ~**X**60
المتغيرات الفئوية (Categorical variables)	2	**X**28 (8 categories), **X**61 (2 categories)
الحالات الطبيعية (Normal)	18274	minute intervals=2
الحالات الشاذة (Abnormal)	124	Y=1

3-3- الاختبارات الإحصائية (Statistical Tests)

تتطلب المنهجية المتبعة لتحديد عتبة التصنيف ضمن نظام كشف الشذوذ المقترح، تحديد نوع التوزيع الذي تتبعه البيانات، وذلك لمعرفة نوع الاختبار اللازم لتحديد المجال الذي تقع ضمنه معظم العينات، سواء كانت هذه الاختبارات معلميه (Parametric Test) أو غير معلميه (Nonparametric).

تمَّ استخدم اختبار كولموغوروف سميرنوف (Kolmogorov–Smirnov test) لمعرفة نوع التوزيع الذي تأتي منه العينة، وعلى نظرية تشيبيشيف (Chebyshev's Theory)، أو القاعدة التجريبية (Empirical Rule) لتحديد الحدود الدنيا والعظمى للمجال الذي تقع ضمنه معظم العينات. إن القاعدة التجريبية هي طريقة معلميه، تستخدم مع التوزيع الطبيعي للبيانات، ونظرية تشيبيشيف هي طريقة غير معلميه، وتُطَبَّق من أجل مجموعة واسعة من التوزيعات.

3-3-1- اختبار كولموغوروف – سميرنوف (Kolmogorov–Smirnov Tests)

يستخدم اختبار كولموغوروف سميرنوف [47] لتحديد ما إذا كانت العينة تأتي من مجموعة بيانات ذات توزيع محدد. تَمَّ ترتيب التوزيعات المختبرة من الأكثر ملائمة للبيانات إلى الأقل، حسب قيمة مربع كاي (Chi–Square). إن فرضيات الاختبار هي:

1. الفرضية الصفرية H_0: إن البيانات تأتي من التوزيع المحدد.

$$H_0 : \hat{F}(x) = F(x) \;\; for\ all\ x\ from - \infty \text{ to } \infty$$

2. الفرضية البديلة H_1: إن عينة واحدة على الأقل، لا تطابق التوزيع المحدد.

$$H_1 : \hat{F}(x) \neq F(x)\ for\ at\ least\ one\ x$$

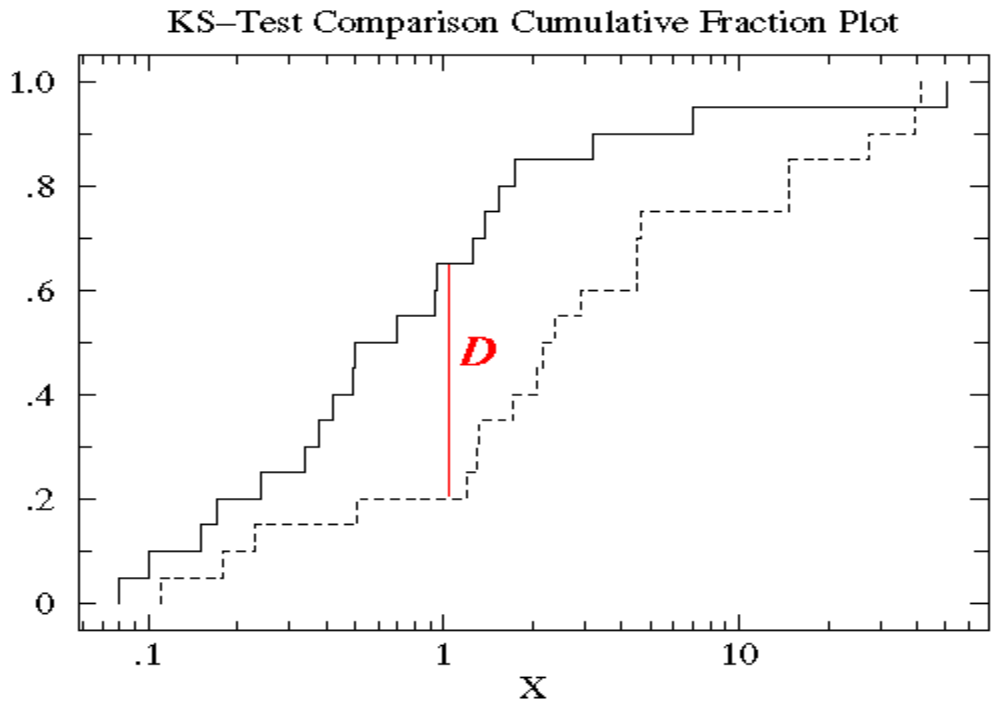
F: دالة التوزيع التراكمي النظري، $\hat{F}$: دالة التوزيع التراكمي التجريبي

يَتِمُّ التحقق من صحة فرضيات الاختبار بالاعتماد على حساب المسافة بين التوزيع التراكمي التجريبي (Empirical Cumulative)، والتوزيع التراكمي النظري (Theoretical Cumulative) للعينة. بفرض إن $x_1, \dots, x_m$ مجموعة من المشاهدات المستقلة بتوزيع تراكمي نظري F. فإن القيمة الإحصائية للاختبار (Test Statistic)، التي تمثل أعظم (Supremum) مسافة عامودية بين التوزيعين السابقين (**الشكل 3-4**)، تعطى بالقانون الآتي:

$$D_n = \sup_{x \in R} \left| \hat{F}(x) - F(x) \right| \qquad (3\text{-}8)$$

تعطي دالة التوزيع التراكمي التجريبي $\hat{F}(x)$ للعينة، وفق الصيغة الرياضية الآتية:

$$\hat{F}(x) = \frac{\#(i: x_i \le x)}{m} \qquad (3\text{-}9)$$



الشكل 3-4 التوزيع التراكمي النظري والتجريبي للبيانات

بعد حساب القيمة الإحصائية D، يتم الحصول على القيمة الحرجة (Critical Value) للاختبار، من جدول الكميات الإحصائية لاختبار كولموغوروف سميرنوف [48]، من أجل معامل ثقة (Significance Level) يساوي 0.05، وبناءً عليه يَتِمُّ رفض النظرية الصفرية إذا تحقق الشرط الآتي:

$$Reject\ H_0\ if\ D > \text{Critical Value}$$

3-3-2- نظرية تشيبيشيف (Chebyshev's Theory)

بفرض أن المتوسط والانحراف المعياري لمجموعة البيانات معلوم، ونريد معرفة نسبة البيانات التي تقع ضمن انحرافين معياريين أو أكثر عن المتوسط، عندئذ هناك احتمالان. إذا كانت البيانات تتبع التوزيع الطبيعي، يمكن عندئذٍ استخدام القاعدة التجريبية لتحديد الحدود العُلْيا والدنيا للمجال. أما إذا كان توزيع البيانات غير معروف، أو لا تتبع التوزيع الطبيعي، تُستخدم نظرية تشيبيشيف من أجل هذه الحالات.

تُقَدِّر نظرية تشيبيشيف الحد الأدنى لنسبة الملاحظات التي تقع ضمن عدد محدد من الانحرافات المعيارية عن المتوسط، وتُطبَّق على مجموعة واسعة من التوزيعات الاحتمالية. تَنصّ النظرية [49] على أنهُ يوجد على الأقل نسبة $1 - \frac{1}{k^2}$ من البيانات تَقَع ضِمْنَ k انحراف معياري عن المتوسط $\mu \pm k\sigma$، حيث $k > 1$.

3-3-3- القاعدة التجريبية (The Empirical Rule)

تنص القاعدة [50] على أنهُ إذا كان للبيانات توزع تكراري على شكل جرس (Bell-Shaped)، فعندئذٍ يوجد تقريباً:

- 68% من البيانات تقع ضمن انحراف معياري واحد عن المتوسط $[\bar{x} - \sigma, \bar{x} + \sigma]$.
- 95% من البيانات تقع ضمن انحرافين معياريين عن المتوسط $[\bar{x} - 2\sigma, \bar{x} + 2\sigma]$.
- 99% من البيانات تقع ضمن ثلاثة انحرافات معيارية عن المتوسط $[\bar{x} - 3\sigma, \bar{x} + 3\sigma]$

تُطبق القاعدة فقط على التوزيع الطبيعي، وإلا فإن هذه النسب يمكن أن تكون أكبر أو أصغر من تلك الواردة في القاعدة.

3-4- ضبط البارامترات الفائقة (Hyperparameter Tuning)

تُعَبِّر البارامترات الفائقة (Hyperparameters) عن مجموعة من الوسطاء الرياضية، التي يَتِمُّ ضبطها على نحوٍ مختلف عن البارامترات العادية، لن يقوم النموذج بتحديث قيم البارامترات الفائقة أثناء عملية التدريب كما في البارامترات العادية، لذلك هناك حاجة ضرورية إلى ضبطها بالشكل الأمثل قبل تدريب النموذج. إن اختيار أفضل القِيَم للبارامترات الفائقة يدوياً، عملية مملة وتسهلك الكثير من الوقت، لذلك لا بد من استخدام خوارزميات التحسين لضبط البارامترات الفائقة.

تَعني عملية ضبط (أو تحسين) البارامترات الفائقة، إيجاد مجموعة قِيَم البارامترات التي تحقق أفضل أداء لنموذج تَعلُّم الآلة. يوجد العديد من خوارزميات التحسين المستخدمة في مجال ضبط البارامترات الفائقة، مثل البحث الشبكي (Grid Search)، والبحث العشوائي (Random Search).

- **البحث الشبكي (Grid Search)**

إن البحث الشبكي [51] يُقِيم جميع التركيبات الممكنة للبارامترات الفائقة ضمن فضاء بحث محدد، إذ يعمل على عزل كل بارامتر على حِدة والبحث عن أفضل قِيمَة له، مع المحافظة على ثبات قيم البارامترات الفائقة الأخرى؛ لكن من أجل الحالات التي يكون فيها للبارامتر تأثير ضئيل على أداء النموذج، فإن ذلك يُعتَبر هدراً للوقت وزيادة في الكلفة الحسابية.

- **البحث العشوائي (Random Search)**

إن البحث العشوائي هو الخيار الأفضل عندما يكون فضاء البحث عالي الأبعاد، أي يحتوي على عدد كبير من التركيبات المختلفة للبارامترات الفائقة. تبحث الخوارزمية ضمن مجموعة عشوائية من هذه التركيبات لاختيار أفضل القيم للبارامترات الفائقة الخاصة بالنموذج المقترح، ولذلك فإن الوقت المستغرق للعثور على المجموعة الصحيحة يكون أقل مع عدد أقل من التكرارات.

يُعتَبر البحث العشوائي [52] أكثر فعالية من البحث الشبكي، ولديه قوة استكشافية محسنة من خلال التركيز على إيجاد القِيمَة المثلى للبارامتر الفائق، لذلك اعتمدت الدراسة الحالية على البحث العشوائي لضبط قِيَم البارامترات الفائقة لنظام كشف الشذوذ المقترح.

3-5- اختيار الميزات (Feature Selection)

تُعرَّف هندسة الميزات (Feature Engineering) بأنها عملية إنشاء مجموعة ميزات باستخدام خصائص البيانات التي تعزز أداء خوارزميات تَعلُّم الآلة. يُمكن أن تكون هذه الميزات ذات أبعاد عالية (High Dimensions) ويصعب تدريبها. يُعدّ تقليل الأبعاد (Dimensionality Reduction) أحد أكثر الطرق شيوعاً لتحويل (Mapping) الميزات من فضاء ذي أبعاد عالية إلى فضاء بِعَدَدٍ أقل من الأبعاد والتي لها معنى [53]. يُعتَبر كُلّ من استخراج الميزات (Feature Extraction) واختيار الميزات (Feature Selection) من أهم تقنيات تقليل الأبعاد [54]. تنشأ تقنية استخراج الميزات مجموعة ميزات جديدة باستخدام مجموعة من الميزات الأصلية وإسقاطها إلى فضاء بأبعاد أقل. من ناحية أخرى يهدف اختيار الميزات إلى تحديد مجموعة فرعية من الميزات وثيقة الصلة باستخدام مقياس معياري.

تُصنّف تقنيات اختيار الميزات على نطاق واسع إلى فئتين: خاضعة للإشراف (Supervised) وغير خاضعة للإشراف (Unsupervised). تندرج تحت هاتينِ الفئتين مجموعة من الطرائق أهمها التصفية (Filter)، والتغليف (Wrapper)، وتقنيات التضمين (Embedded Methods).

تقوم تقنيات التغليف على إنشاء عناقيد (Clusters) من المجموعات الفرعية للميزات، إذ تختار الميزات النهائية على نحوٍ تجريبي بناءً على أفضل دقة لخوارزمية تَعلُّم الآلة المدربة على المجموعات الفرعية [55]؛ لكن تقنيات التغليف باهظة الثمن من الناحية الحسابية وغير مجدية إذا كان هناك عدد كبير من الميزات. من ناحية أخرى تعتمد تقنيات التصفية على مقياس إحصائي لتحديد الميزات النهائية قبل عملية تدريب النموذج. إنَّ كل من معامل الارتباط (Correlation) ومربع كاي (Chi–Square) من طرائق التصفية [55]. تتميز تقنيات التصفية من تقنيات التغليف بأنها مستقلة عن خوارزمية التدريب ولذلك تَمنع تحيز الميزة مع النموذج المُدرب؛ لكن لا تراعي التفاعل بين الميزات. تجمع تقنيات التضمين كُلاً من ميزات طرائق التغليف والتصفية وذلك من خلال تحقيق تفاعل الميزات مع بعضها من جهة، والمحافظة على كلفة حسابية معقولة من جهة أخرى. تُعتبر أساليب التضمين تكرارية [56] بمعنى أنها تهتم في كل تكرار بتدريب النموذج واستخراج الميزات النهائية التي تسهم على نحوٍ أكبر في تدريب النموذج للتكرار المعين. تُعدّ الغابات العشوائية بما تقدمه من خاصية قياس أهمية الميزة (Feature Importance) من أهم الأمثلة على تقنيات التضمين.

إن الاعتماد على مفهوم أساليب التضمين لاختيار أهم الميزات في نماذج الشبكات العصبونية، يُعدّ أمراً مكلفاً للغاية، وذلك بسبب حاجة هذه الأساليب لتدريب النموذج أكثر من مرة لاختيار الميزات. درس الباحثون طرقاً مختلفة لاختيار الميزات في نماذج التَعلُّم العميق [57] [58] [59]، كاستخدام معدل التسريب المتغير (Variational Dropout) في طبقة الدخل كوسيلة لقياس أهمية الميزة [60]. يشير معدل التسرب الفردي لكل ميزة إلى مقدار السماح للنموذج بإزالة هذه الميزة، ولذلك فإن الميزات ذات معدل التسرب المنخفض تكون أكثر صلة من تلك ذات معدل التسرب المرتفع. يَتِمُّ استخدام هذه القيم لبناء ترتيب الميزات. كما تَمَّ استخدام مقياس الحجوم (Magnitude Measures) [61] لقياس مساهمة كُلّ ميزة في أوزان طبقة الخرج، ومن ثم ترتيب الميزات وفقاً لأكثر الميزات وزناً. أظهرت النتائج أن هذه الأساليب تحقق نتائج أفضل عند مقارنتها بطرق التصفية والتضمين.

اعتمدت الدراسة على خاصية أهمية الميزة المقدمة من الغابات العشوائية لقياس أهمية الميزة، في نماذج تعلم الآلة الكلاسيكية. أما بالنسبة لنماذج التَعلُّم العميق فإنه تَمَّ استخدام مقياس الحجوم لترتيب أهمية الميزات. سوف يَتِمُّ ذكر آلية تطبيق هذه الأساليب ضمن الدراسة الحالية في الفصل الخامس والسادس من هذه الأطروحة.

3-6- الحزم والمكتبات المستخدمة (Used Packages and Libraries)

تَمّ بناء نظام كشف الشذوذ المقترح في مجموعات البيانات السابقة باستخدام لغة بايثون **Python** وبالاعتماد على مجموعة من المكتبات البرمجية وأهمها:

- **Numpy:** هي اختصار لعبارة (Numerical Python Library) وتُستخدَم هذه الحزمة من أجل المصفوفات متعددة الأبعاد والعمليات الجبرية الخطية [62].
- **Pandas:** توفر هذه الحزمة أداة لتحليل ومعالجة البيانات. تَمّ استخدامها لقراءة مجموعة البيانات وتحميلها [63].
- **Scikitlearn:** تُستخَدم هذه الحزمة من أجل الأساليب الإحصائية وتَعلُّم الآلة [64].
- **Keras:** توفر هذه الحزمة واجهات برمجية متناسقة وبسيطة من أجل التخاطب مع المستخدم النهائي وليس الآلة ، وتحتوي على مجموعة من النماذج (Models) مثل الشبكات العصبونية وأشجار القرار وتوابع التنشيط ، كما تتميز بقابليتها للتوسع أي القدرة على إضافة نماذج جديدة. تكون المهمة الأساسية للمكتبة جعل التطبيق أكثر استجابة مع إمكانية إعطاء المستخدم المزيد من القدرة على التحكم به [65].
- **TensorFlow** : تُطبّق هذه الحزمة في العديد من المجالات كحساب المشتقات والمصفوفات الضخمة بالإضافة إلى استخدامها في توزيع العمليات الحاسوبية على وحدات المعالجة المركزية CPU، وكذلك على شبكة موزعة مكونة من مجموعة أجهزة بعيدة تتضمّنَ هذه المكتبة. يُستخدم TensorFlow على نحوٍ أساسي في تعلم الآلة في الوقت الحالي [66].

الفصل الرابع

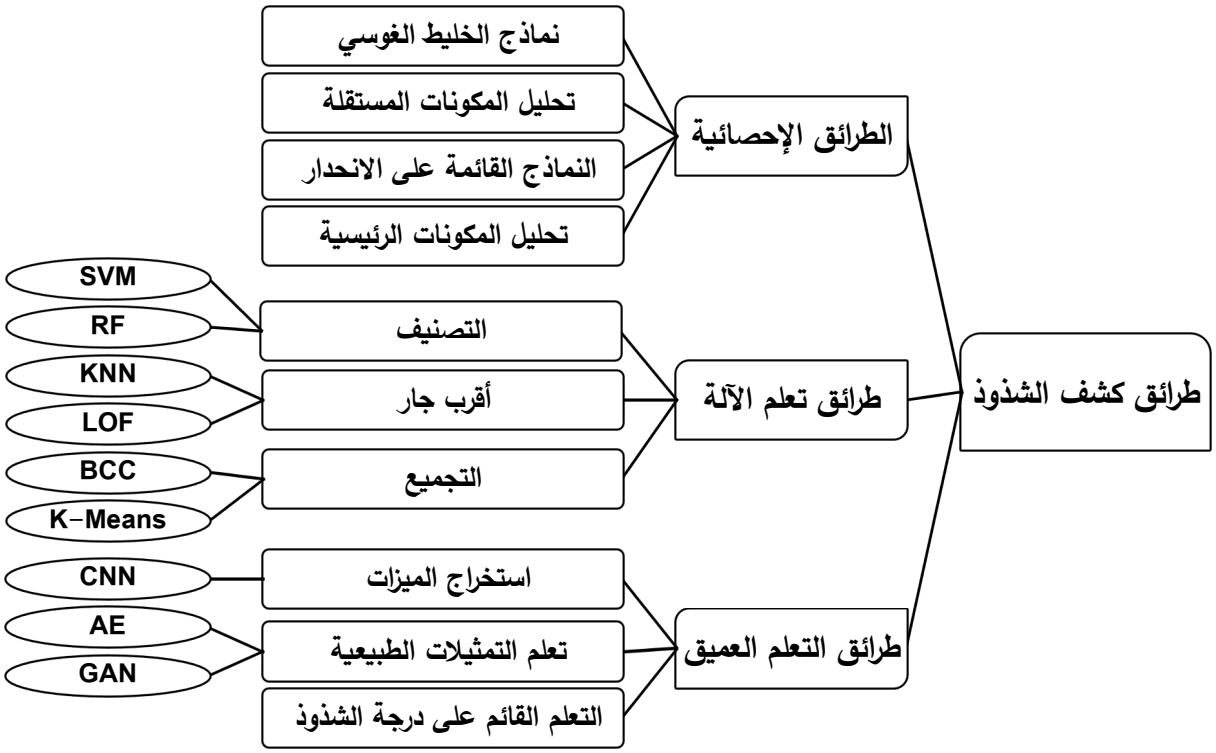
الدراسة المرجعية

اشتملت الدراسات المرجعية على العديد من طرائق كشف الشذوذ في البيانات وخوارزمياته. اعتمدت الدراسة للوصول إلى أحدث الاتجاهات التكنولوجية في أنظمة كشف الشُّذُوذ على تصنيف أدبيات الدراسات السابقة حسب تقنيات كشف الشذوذ (ADT: Anomaly Detection Techniques).

يُعدّ تصنيف الدراسات بواسطة طرائق الكشف مفيداً في:

1. التعرف على التقنيات المناسبة لمعالجة المشكلة المطروحة.
2. تحديد سبب اختيار طرائق معينة أو نجاحها من خلال مقارنتها بطرائق أخرى.
3. تسليط الضوء على التحديات الموجودة في أنظمة كشف الشذوذ الحالية.

يوجد العديد من الطرائق المستخدمة في مجال كشف الشذوذ وفق أدبيات الدراسات السابقة، وَيُبَيِّن المخطط الموضّح في **الشكل 4-1** طرائق كشف الشذوذ وتصنيفاتها.



الشكل 4-1 تصنيف طرائق كشف الشذوذ. المصدر: الدراسة الحالية

نبين فيما يلي طرائق كشف الشذوذ المختلفة لكل نوع من الطرائق المبينة في المخطط السابق:

4-1- الطرائق الإحصائية (Statistical Methods)

تعتمد أغلب الطرائق الإحصائية في اكتشاف الشذوذ على مبدأ الكثافة الاحتمالية للبيانات، وهو أن البيانات الطبيعية سوف تقع في مناطق احتمالية عالية، بينما تقع البيانات الشاذة في مناطق احتمالية منخفضة [2] [67]. يَتِمّ تَوَقُّع التوزيع الاحتمالي (Probability Distribution) لبيانات التدريب أولاً (يفترض أن تكون في أغلبها بيانات طبيعية)، ومن ثم يَتِمُّ تحديد الحالات الشاذة بناءً على قيمة درجة الشذوذ، التي تُعبر عن بُعد العينة عن مناطق الكثافة الاحتمالية، إذ تُعتَبر جميع النقاط التي لها درجة أكبر من حد مُعيّن نقاطاً شاذة.

يوجد عدد كبير من التقنيات والأساليب التي تندرج تحت طرائق الكشف الإحصائية، لكن أكثرها استخداماً هي: نماذج الخليط الغاوسي (Gaussian Mixture Models)، تحليل المكونات المستقلة (Independent Component Analysis)، النماذج القائمة على الانحدار (Regression Based-Models)، تحليل المكونات الرئيسية (Principal Component Analysis)

4-1-1- نماذج الخليط الغوسي (Gaussian Mixture Models)

تَفرُض نماذج الخليط الغوسي أن البيانات يَتُم إنشاؤها من خليط موزون (Weighted Mixture) لتوزيع غاوس (Gaussian distributions). تعتمد نماذج الخليط لاكتشاف الشذوذ على حساب المسافة بين مثيل البيانات (Data Instance) ومتوسط مجموعة العينات، إذ تُعتَبر جميع مثيلات البيانات التي لها مسافة أكبر من حد مُعيّن هي حالات شاذة. تَمَّ تطوير العديد من أنظمة كشف الشذوذ بالاعتماد على نماذج الخليط الغاوسي (GMM)، وتطبيقها في مجالات الشذوذ المختلفة مثل كشف الاختراقات الشبكية [68].

يوجد عدة قيود تَحدّ من فعالية نماذج الخليط الغوسي في اكتشاف الشذوذ من أهمها:

1. تحاول نماذج الخليط ملائمة جميع البيانات، بما فيها الحالات الشاذة أثناء عملية التدريب.
2. يجب معرفة عدد توزيعات غاوس ضمن البيانات مسبقاً.

4-1-2- تحليل المكونات المستقلة (Independent Component Analysis)

يسمح تحليل المكونات المستقلة بتحديد المتغيرات الكامنة (Latent Variables) في البيانات المرصودة متعددة المتغيرات (Multivariate). تفرض هذه الأساليب أن البيانات المرصودة عبارة عن مزيج خطي غير معروف من المتغيرات الكامنة غير الغاوسية والمستقلة على نحوٍ متبادل.

استُخدِم تحليل المكونات المستقلة في اكتشاف الشذوذ في العديد من المجالات، كاكتشاف التغيرات في محركات الديزل، من خلال دراسة إشارات الانبعاث الصوتي [69] [67]. بالإضافة إلى تحديد مشاكل الملاحة الجوية مثل انحرافات المسار وحالة المدرج [70].

4-1-3- النماذج القائمة على الانحدار (Regression Model-Based)

تُعدّ النماذج القائمة على الانحدار [2] هي نماذج معلميه (Parametric)، وتمّ استخدامها على نحوٍ واسع في بيانات السلاسل الزمنية (Time Series). تستند هذه الطرائق لاكتشاف الشذوذ على خطوتين. يَتِمُّ في الخطوة الأولى إنشاء نماذج الانحدار بالاعتماد على بيانات التدريب، وفي الخطوة الثانية اختبار النموذج على متواليات الاختبار لحساب القيم المتوقعة. يمثل الفرق بين القيم الحقيقية والقيم المتوقعة مقدار الشذوذ، إذ تُعتَبر جميع النقاط التي لها درجة أكبر من حد معين نقاطاً شاذة.

دُمِجَت هذه النماذج مع العديد من طرائق الكشف التقليدية للتنبؤ بالشذوذ ضمن السلاسل الزمنية، ومنها شعاع الانحدار الذاتي (Vector Auto-Regressive) [71] [72]، الانحدار الذاتي والمتوسط المتحرك (Auto-Regressive Moving Average) [73] [74].

4-1-4- تحليل المكونات الرئيسية (Principal Component Analysis)

يُعتبر التعامل مع البيانات ذات الأبعاد العالية أمراً صعباً للغاية، لذلك نلجأ إلى الأساليب التي تُستخدم لتقليل الأبعاد (عدد المتغيرات) في البيانات. يُعدّ تحليل المكونات الرئيسية من الأساليب التي تساعد على إسقاط البيانات في فضاء ذي بُعد أقل، مع المحافظة على المكونات التي يكون التباين (Variance) بينها أعظم (Maximized) ما يُمكن.

يَعتمد تحليل المكونات الرئيسية في اكتشاف الشذوذ على إنشاء مصفوفة التباين للبيانات الطبيعية، ومن ثم حساب المتجهات الذاتية (Eigenvectors) للمصفوفة. تُعبّر المتجهة الذاتية عن خواص المصفوفة، وتستخدم في اختزالها وإعادة بنائها. يتم حساب المسافة بين البيانات الأصلية والبيانات التي تم إعادة بنائها باستخدام المتجهات الذاتية، حيث يكون للبيانات الشاذة فرق أكبر من البيانات الطبيعية. استُخدِمَت هذه الطريقة لاكتشاف الشذوذ في العديد من المجالات، والتي يكون العلاقة بين بياناتها خطية حصراً. فعلى سبيل المثال دراسة سلاسل DNA لتشخيص مرض السرطان [20].

إن أفضل المقاربات لاكتشاف الشذوذ بالاعتماد على الطرائق الإحصائية، كانت باستخدام تحليل المكونات الرئيسية. أُجريَت دارسة لاكتشاف الاختراقات ضمن الشبكة [75] باستخدام الطرائق الإحصائية، وأظهرت النتائج تفوق تحليل المكونات الرئيسية على الطرائق الإحصائية الأخرى. إن تقنيات الكشف

القائمة على تحليل المكونات الرئيسية لا تحتاج لوضع أي افتراض حول توزيع البيانات، بالإضافة إلى تقليل أبعاد البيانات من دون فقدان أي معلومات مهمة، وانخفاض التعقيد الحسابي مقارنة بالطرائق الإحصائية الأخرى.

نجد من خلال أدبيات الدراسات السابقة وجود قصور واضح في طرائق كشف الشذوذ الإحصائية، فهي لا تتكيف مع أنماط البيانات الشاذة الجديدة من جهة، ومن جهة أخرى فإنها تضع مجموعة من القيود والفرضيات متعلقة بتوزيع علاقات البيانات ونوعها. بالمقابل يبدو في العديد من المواقف العملية أنه من الصعب الاحتفاظ بهذه الفرضيات. لذلك كان لا بد من التوجه إلى استخدام أساليب أكثر مرونة مثل طرائق تَعلُّم الآلة والتَعلُّم العميق.

4-2- طرائق تعلم الآلة (Machine Learning Methods)

تختلف طرائق تَعلُّم الآلة في اكتشاف الشذوذ، بالاعتماد على تسميات (Labels) بيانات الدخل المتوفرة هل هي مسماة أو غير مسماة (Labeled/Unlabeled) ؟، ونوع الخرج المراد هل هو تسمية أو درجة شذوذ (Score/Label)؟ تندرج طرائق تَعلُّم الآلة في كشف الشذوذ، إلى ثلاث فئات رئيسية وهي التصنيف (Classification)، أقرب جار (Nearest Neighbor)، التجميع (Clustering).

تتطلب تقنيات التصنيف تسميات حقيقية لجميع بيانات التدريب الطبيعية والشاذة. تضمنت الأدبيات السابقة الكثير من خوارزميات التصنيف [76] [77] [78] ، كالشبكات العصبونية، آلة شعاع الدعم (SVM)، الغابات العشوائية، **راجع الفصل الثاني من هذه الأطروحة للتذكير بهذه الخوارزميات.** بينما لا تتطلب تقنيات أقرب جار والتجميع تسميات حقيقية لبيانات التدريب، إذ يكون الافتراض الأساسي لهذه الطرائق أن نسبة صغيرة فقط من البيانات تنتمي إلى صف الحالات الشاذة. يوجد عدد من الخوارزميات التي تندرج تحت هذه الفئات مثل طريقة K-Means والمعامل الخارجي المحلي (LOF: Local Outlier Factor) [79] [76].

فيما يلي أهم مقاربات كشف الشذوذ القائمة على أحد طرائق تَعلُّم الآلة وفق أدبيات الدراسات السابقة، ثم مقاربات كشف الشذوذ الهجينة التي تجمع بين اثنين أو أكثر من طرائق تَعلُّم الآلة.

4-2-1- تقنيات كشف الشذوذ القائمة على التصنيف

تُعالج طرائق التصنيف مشكلة كشف الشذوذ كمشكلة تصنيف ثنائي. تهدف هذه الطرائق لبناء نموذج قادر على تصنيف البيانات إلى صفين رئيسيين، هما صف الحالات الشاذة وصف الحالات الطبيعية.

تُشير الدراسات السابقة [80] إلى وجود حوالي 49 طريقة تصنيف في اكتشاف الحالات الشاذة، تتفوق فيها كل من الشبكات العصبونية، والغابات العشوائية، وآلة شعاع الدعم .

تمَّ مقارنة ثماني خوارزميات تعلم آلة [81] في مسائل كشف الشذوذ ضمن البيانات. أظهرت النتائج تفوق كل من خوارزميات آلة شعاع الدعم (SVM) والشبكات العصبونية والغابات العشوائية، وفقاً لثلاث مقاييس أداء وهي الاسترجاع (Recall)، الدقة (Accuracy)، مساحة السطح تحت منحني الدقة والاسترجاع (AUCPR). لكن من جهة أخرى، نوّه الباحثون بضرورة إجراء ضبط البارامترات الفائقة واختيار الميزات لتحقيق نتائج أفضل لهذه الخوارزميات، فضلاً عن عدم قدرتها على التعامل مع البيئات الديناميكية (تكيّف الأنماط الشاذة مع الأنماط الطبيعية).

استُخدِمت خوارزمية الغابات العشوائية بغرض كشف الاحتيال المالي [82] ضمن أحد الشركات المالية الصينية. اعتمدت الدراسة على بناء نموذجين من الغابات العشوائية يختلفان عن بعضهما بآلية اختيار الميزات (Features) ضمن العقد (Nodes). تعتمد الآلية الأولى على حساب المسافة ما بين نقاط البيانات وصفي البيانات (الطبيعية والشاذة)، بينما تعتمد الآلية الثانية على حساب قيمة شائبة جيني (Gini Impurity) لكل ميزة واختيار تلك التي تُحقِّق أقل قيمة. أظهرت النتائج تفوق الآلية الثانية من حيث الاسترجاع (Recall) والدقة (Precision)، إذ بلغت قيمتهما 95% و89% على التوالي. بالمقابل نوهت الدراسة بضرورة إجراء ضبط البارامترات الفائقة، إذ يمكن أن تكون دقة هذه النماذج مضللة بعض الشيء.

استُخدِمَت خوارزميات الانحدار اللوجستي (Logistic Regression) والغابات العشوائية وأشجار القرار (Decision tree) لاكتشاف الحالات الشاذة ضمن البيانات [83]. اختبرت الدراسة مدى فعالية هذه الخوارزميات باستخدام جميع ميزات مجموعة البيانات، وعند اختيار مجموعات جزئية من الميزات مكونة من (5–10 ميزات)، أظهرت النتائج تفوق الغابات العشوائية بدقة (Accuracy) حوالي 90% عند استخدام جميع الميزات. لم تذكر الدراسة الطريقة التي تَمّ اختيار الميزات بها من جهة، ومن جهة أخرى لا يمكن تبني هذه النتائج على نحوٍ كبير بسبب اعتمادها على مقياس الدقة.

استُخدِمَت أداة اختيار الميزات (Features Selector) لتحديد الميزات الأكثر أهمية ضمن مجموعة بيانات شاذة متمثلة بالاحتيال المالي (البيانات الأوروبية)، إذ تَمَّ اختيار 27 ميزة لهذه التجربة. ليَتُّم في المرحلة التالية تطبيق مجموعة من خوارزميات تَعلُّم الآلة وهي الانحدار اللوجستي والغابات العشوائية ومصنف بايز (Naive Bayes) كطرائق لكشف الشذوذ (الاحتيال) ضمن مجموعة البيانات

المستخدمة [84]. أظهرت نتائج الدراسة تفوق الغابات العشوائية بنسبة استرجاع (Recall) حوالي 81%. لكن بالمقابل، لم تتَطَرَّق الدراسة لضبط البارامترات الفائقة الخاصة بالنماذج المقترحة، فضلاً عن عدم قدرتها على التعامل مع الحالات الاحتيالية الجديدة.

تَمّ تطبيق البحث الشبكي (Grid Search) لضبط البارامترات الفائقة الخاصة بخوارزميتي آلة شعاع الدعم (SVM) والغابات العشوائية من أجل بناء نماذج لاكتشاف الشذوذ ضمن عدة مجموعات بيانات غير متوازنة [85]. أظهرت نتائج الدراسة تفوّق آلة شعاع الدعم على الغابات العشوائية من أجل جميع مجموعات البيانات المستخدمة. إذ تمَّ تقييم النتائج باستخدام مقياس MCC، وبلغت قيمته في خوارزمية SVM حوالي 81% من أجل مجموعة البيانات الأكبر. إن أحد قيود هذه الدراسة أنها تتعامل فقط مع حالات الاحتيال المصنفة مسبقاً، بالإضافة إلى عدم تحديد الميزات الأكثر أهمية.

4-2-2- تقنيات كشف الشذوذ القائمة على أقرب جار

تُعالج طرائق أقرب جار مشكلة كشف الشذوذ، من خلال حساب التشابه بين نقاط البيانات، بالاعتماد على مقياس المسافة (Distance) أو مقياس الكثافة (Density). يكون للنقاط الشاذة إما مسافة أبعد أو كثافة أقل من النقاط الطبيعية.

دُمجَت خوارزميتا (K-Nearest Neighbor) والجينية (Genetic Algorithm) لتحديد الميزات الأكثر أهمية ضمن مجموعة بيانات شاذة تمثل هجمات DoS/DDoS [86]. أظهرت نتائج الدراسة أن النموذج المقترح أكثر قدرة على اكتشاف الحالات الشاذة المعروفة مقارنة بالحالات الشاذة غير المعروفة، مع وجود اختلاف بمجموعة الميزات المختارة لكل من الحالات الشاذة المعروفة وغير المعروفة.

تم مقارنة خوارزميات KNN والانحدار اللوجستي ومصنف بايز، في اكتشاف الحالات الشاذة ضمن البيانات [87]. أظهرت نتائج الدراسة تفوق خوارزمية KNN على باقي الخوارزميات المقترحة، إذ بلغت الدقة (Accuracy) لها 97%. بالمقابل فإن خوارزمية KNN غير قادرة على اكتشاف الشذوذ وقت حدوثه.

استخدمت خوارزمية المعامل الخارجي المحلي (Local Outlier Factor) بالاعتماد على تقنيات التنقيّب في النصوص (Text Mining) لاكتشاف الظروف الشاذة ضمن تقارير حوادث المصانع الكيميائية في كوريا الجنوبية [88]. أظهرت نتائج الدراسة قدرة النموذج المقترح على تحديد الحوادث الشاذة، من خلال تحديد الكلمات المفتاحية للشذوذ ومقارنتها بالكلمات المفتاحية للحوادث الطبيعية.

4-2-3- تقنيات كشف الشذوذ القائمة على التجميع

تُعالج طرائق التجميع مشكلة كشف الشذوذ، من خلال تجميع نقاط البيانات الطبيعية ضمن عناقيد (Cluster)، بينما لا تنتمي النقاط الشاذة إلى تلك العناقيد.

أُسْتُخْدِمَتْ Bayesian Co-Clustering [89] لكشف الاحتيال في شركات تأمين الرعاية الصحية. برزت هذه الطريقة كأداة قوية يمكن من خلالها تحليل البيانات الثنائية، تساعد هذه الطريقة في معرفة نوع وطبيعية العلاقة بين المكونات وتجميعهم في عنقود مشترك، على عكس طرائق التجميع التقليدية. حقق النموذج المقترح أداء أفضل وقدرة على التنبؤ بالسلوك المستقبلي لمقدمي الخدمات والمستفيدين وفقاً لخصائصهم. لكن بالمقابل يحتاج النموذج للوصول إلى جميع البيانات الخاصة بالمشكلة المدروسة وهذا غير مُمكن في حالة البيانات الطبيّة بسبب قضايا السرية.

تَمَّ استخدام خوارزمية K-Means لاكتشاف جميع أنواع الحالات الشاذة، باستخدام تقنية اختزال الميزات (Feature Reduction) القائمة على حساب درجة الارتباط (Correlation) [90]. أظهرت نتائج الدراسة تفوق الطريقة المقترحة على K-Means الأساسية من حيث دقة وزمن الكشف. لكن بالمقابل تعاني خوارزمية K-Means من ضعف تصنيف الحالات الطبيعية.

استُخدِمَت تقنية تحسين عناصر السرب (Particle Swarm Optimization)، لتطوير خوارزمية K-means في كشف الحالات الشاذة [91]. تبحث عناصر السرب عن العناقيد الأكثر كثافة، وتسند لها أوزان أعلى. تَمَّ اختبار الطريقة على بيانات Yahoo، وأظهرت قدرتها على تحسين دقة الكشف وزمنه.

4-2-4- النماذج الهجينة الكلاسيكية (Classic Hybrid Model)

توجهت مؤخراً بعض الأبحاث لبناء أنظمة كشف الشذوذ باستخدام أساليب هجينة بين اثنين أو أكثر من طرائق الكشف. تَمَّ مقارنة خوارزميتي أقرب جار (KNN) وآلة شعاع الدعم (SVM) [77] في كشف الشذوذ كمرحلة أولى، ثم بناء نموذج كشف هجين بين هاتين الخوارزميتين في المرحلة الثانية. أظهرت النتائج تفوق SVM على KNN بدقة (Accuracy) 81.6%. بينما كان للنموذج الهجين المقترح أداء أفضل من الخوارزميتين كُلٌّ على حِدى، حيث بلغت دقته 82.5%.

دُمجت خوارزميتي غابة العزل (Isolation Forest) مع المعامل الخارجي المحلي، لبناء نظام كشف شذوذ قادر على التقاط حالات الشذوذ العامة (Global) والمحلية (Local) [92]. يَتُّم في البداية تطبيق غابة العزل لتحديد جميع حالات الشذوذ العامة بأقل تعقيد زمني، من ثم يَتِمُّ في المرحلة الثانية

تطبيق المعامل الخارجي المحلي لاكتشاف الحالات الشاذة المتبقية. أظهرت نتائج الدراسة تفوّق المنهجية المقترحة من حيث دقة الكشف والتخفيف من تعقيد الوقت.

دُمجت خوارزميتي (K–means) مع أشجار القرار لبناء نظام كشف الشذوذ [93]. يَتِمُّ في المرحلة الأولى تجميع نقاط البيانات ضمن عناقيد باستخدام K–means، ثم في المرحلة الثانية بناء الشجرة بالاعتماد على النقاط الموجودة في العناقيد، تؤشر جميع العناقيد الموجودة في الأوراق على حالات شاذة.

استُخدِمَت الغابات العشوائية مؤخراً لتصنيف الحالات الشاذة ضمن بيانات غير موسومة (Unlabeled). اعتمدت الدراسة [94] في بناء نموذج كشف الشذوذ على مجموعتي بيانات تدريب مسماة واختبار غير مسماة. يتم في المرحلة الأولى تدريب النموذج من خلال استخدام انحدار الغابات العشوائية، ليتم اختباره فيما بعد بواسطة مصنفات الغابة العشوائية. أظهرت النتائج قدرة النموذج على اكتشاف 8000 حالة شاذة من أصل 21000 حالة ضمن مجموعة البيانات المستخدمة. لم تعتمد الدراسة على أي نوع من مقاييس الأداء ولم تذكر أيضاً قيم البارامترات الفائقة التي تَمَّ استخدامها.

يعرض **الجدول 4–1** مقارنة لأهم تقنيات كشف الشذوذ القائمة على تَعلُّم الآلة، والمستخدمة في أدبيات الدراسات السابقة.

الجدول 4–1 تقنيات كشف الشذوذ القائمة على تَعلُّم الآلة

التقنيات المستخدمة	نتائج الدراسة	المقاييس	المرجع
SVM, RF, NN, Capsule Network	تفوق شبكة Capsule Network؛ لكنها تستهلك وقتاً أطول	Accuracy = 99.21% Recall =95.50%	[95]
RF, LR, SVM, KNN, DT	تفوق تقنيات التصنيف؛ لكنها تتطلب التسمية المسبقة للحالات الشاذة	أعلى دقة للغابات العشوائية Precision = 95%	[96]
RF, NN	الغابات العشوائية أقل تأثيراً بالضجيج؛ لكنها تتطلب المزيد من وقت التدريب	Accuracy = 90%	[97]
SVM, KNN, LR	اكتشاف الشذوذ في الوقت الحقيقي	SVM=91%, LR=74%, KNN=72%	[98]

توفر طرائق تَعلُّم الآلة المستخدمة في كشف الشذوذ، الإجابة عن أحد الفرضيات المتعلقة بالبيانات المدروسة، ما الحالات الشاذة؟ ما الحالات الطبيعية؟ ما التوزيع المحتمل لكل منهما؟ لذلك فإن طريقة الكشف الأمثل هي التي تكون غير متحيزة لحالة معينة أو توزيع معين، بالإضافة إلى تكيفها مع جميع أنواع البيانات والأبعاد العالية. يصعب على طرائق تَعلُّم الآلة (التصنيف، أقرب جار، التجميع) تحقيق

جميع ما سبق، وهذا تَمَّ ملاحظته من خلال الدراسات السابقة. مما يؤكد على ضرورة التوجه نحو طرائق التَعلُّم العميق.

4-3- طرائق التَعلُّم العميق (Deep Learning Methods)

تُصنَّف طرائق كشف الشذوذ القائمة على التَعلُّم العميق إلى ثلاث مجموعات رئيسية وهي اِسْتِخْرَاج الميزات (Features Extraction)، والتَّعَلُّم القائم على درجة الشُّذُوذ (Anomaly Score Learning)، وتَعَلُّم التَمْثيلِات الطبيعية (Learning Representations of Normality). توجهت الأبحاث والدراسات الأخيرة إلى الاعتماد على طرائق تَعَلُّم التَمْثيلِات الطبيعية [99] لكفاءتها في معالجة معظم التحديات التي تواجه مسائل كشف الشذوذ.

1. طرائق استخراج الميزات

تهدف طرائق استخراج الميزات إلى تقليص عدد الميزات في البيانات عالية الأبعاد أو غير القابلة للفصل خطياً، وتفرض هذه الطرائق أن تمثيلات الميزات المستخرجة تحافظ على المعلومات التي تساعد في فصل البيانات الطبيعية والشاذة. تتمثل أحد الاتجاهات البحثية القائمة على هذه الطرائق في استخدام نماذج التعلم العميق المدربة مسبقاً على نحوٍ مباشر، مثل AlexNet، VGG، ResNet لاستخراج الميزات وكشف الشذوذ في البيانات المعقدة عالية الأبعاد مثل بيانات الصور والفيديو [101] [100].

2. طرائق التَّعَلُّم القائم على درجة الشُّذُوذ

تركز طرائق التَّعَلُّم القائم على درجة الشُّذُوذ على تحسين أساليب قياس الانحرافات للنقاط الشاذة، وذلك من خلال دمج مقاييس الشذوذ الحالية ونماذج الشبكات العصبونية من جهة، وابتكار توابع خسارة (Loss Function) جديدة من جهة أخرى. تتضمن هذه الطرائق أربع فئات وهي نماذج الترتيب (Ranking Models) [102]، والنماذج المشتقة مسبقاً (Prior-Driven Models) [103]، والنماذج الاحتمالية (Likelihood Models) [104]، ونماذج الصف الواحد (One Class Models) [105].

3. طرائق تَعَلُّم التَمْثيلِات الطبيعية

تُعدّ طرائق تَعَلُّم التمثيلات الطبيعية الأكثر شيوعاً في مجال كشف الشذوذ، إذ تركز على تَعَلُّم أنماط البيانات الطبيعية، ومن ثم تحدد الأنماط الشاذة التي تسلك سلوكاً مغايراً للأنماط الطبيعية، مما يساهم في تعويض نقص العينات الشاذة في أثناء التدريب. تستخدم هذه طرائق مثل شبكات الخصومة التوليدية (Generative Adversarial Networks) [106] [107] [108]، وشبكة الذاكرة قصيرة طويلة المدى [109]، لاكتشاف الشذوذ في البيانات المتسلسلة (Sequential Data) مثل الصوت

والسلاسل الزمنية والنصوص. بينما تلعب شبكة الترميز الآلي (Autoencoder) [110] [111] دوراً هاماً في البيانات غير المتسلسلة مثل الصور والبيانات القائمة على الأحداث.

فيما يلي عرض لأهم وأحدث الأبحاث التي استخدمت طرائق تَعلُّم التمثيلات الطبيعية، في اكتشاف الشذوذ ضمن البيانات المتسلسلة وغير المتسلسلة.

4-3-1- طرائق تَعَلُّم التَمثيلِات الطبيعية (Learning Representations of Normality)

1. الشذوذ في البيانات غير المتسلسلة (Non-Sequential Data)

يُطلَق على البيانات عندما لا يكون هناك ارتباطات بين عينات المجموعة، مصطلح البيانات غير المتسلسلة. فعلى سبيل المثال مجموعة من الأحداث المتعلقة بظاهرة معينة، من دون وجود علاقة زمانية أو مكانية بين أحداثها.

استُخدِمَت شبكة عصبونية عميقة مكونة من طبقتين مخفيتين فقط، لاكتشاف الحالات الشاذة في مجموعة بيانات حقيقية [112]، واعتمدت على تقنيات إعادة تكوين العينات (Resampling Methods) لتحقيق التوازن بين صفي البيانات. تم تطبيق النموذج المقترح في اكتشاف الاحتيال المالي ضمن بطاقات الائتمان، وأظهرت نتائج الدراسة تفوق الشبكة المقترحة على طرائق تَعلُّم الآلة الكلاسيكية، لكن بالمقابل لا يمكنها اكتشاف الأنماط غير الخطية، كما في شبكة الترميز الآلي (Autoencoder).

تَمَّت مقارنة مجموعة من خوارزميات التعلم العميق كشبكة الترميز الآلي والشبكة العصبونية الالتفافية (Convolutional Neural Networks)، بمجموعة من طرائق تَعلُّم الآلة الكلاسيكية (آلة شعاع الدعم، الغابات العشوائية، KNN) [113]، لاكتشاف الشذوذ ضمن ثلاث مجموعات متمثلة بالاحتيال المالي. أظهرت نتائج الدراسة تفوق شبكة CNN على باقي النماذج المقترحة، لكن من جهة أخرى، نبّه الباحثون على أن شبكة الترميز الآلي تم تدريبها ضمن الدراسة بالاعتماد على النهج الخاضع للإشراف، بمعنى أن بيانات التدريب تتضمن حالات طبيعية وشاذة (احتيالية). ومع أن نتائج CNN تبدو جيدة، فإنها لا تعمل على نحوٍ جيد في البيئات الديناميكية (تكيُّف أنماط الشذوذ). لذلك فإن تدريب شبكة الترميز الآلي وفق النهج شبه الخاضع للإشراف، هو الحل الأمثل لمشكلة تكيُّف الحالات الشاذة.

تَمَّت مقارنة شبكة الترميز الآلي بآلة بولتزمان المقيدة (Restricted Boltzmann Machine)، لاكتشاف الحالات الشاذة ضمن عدة مجموعات [114]. أكدت نتائج الدراسة تفوق شبكة الترميز الآلي على آلة بولتزمان المقيدة، ومن أجل جميع مجموعات البيانات المستخدمة. لكن بالمقابل، فإن عتبة التصنيف والبارامترات الفائقة تَمَّ اختيارها على نحوٍ تجريبي.

تمت مقارنة شبكة الترميز الآلي بمجموعة من طرائق تَعلُّم الآلة الكلاسيكية (آلة شعاع الدعم، أشجار القرار، الغابات العشوائية) [115] لاكتشاف الشذوذ في البيانات. أظهرت النتائج تفوق شبكة الترميز الآلي، وفق مقياس الاسترجاع (Recall)، إذ بلغت قيمته 81%، وذلك عند تطبيقه على بيانات خاصة بالاحتيال المالي.

استُخدِمَت شبكة الترميز الآلي لاكتشاف حالات الانهيار ضمن جهاز عملاق [116]. أُعتُمد ضمن الدراسة على جهاز يسمى D.A.V.I.D.E، تم استضافته في بولونيا، يتكون من 45 عقدة. أظهرت النتائج قدرة النموذج على اكتشاف حالات الانهيار في الوقت الحقيقي بنسبة 87%. لكن بالمقابل، تم اختيار عتبة التصنيف للنموذج على نحوٍ تجريبي.

بهدف تحسين أداء شبكة الترميز الآلي في اكتشاف الحالات الشاذة، استُخدِمَت تقنية البحث الشبكي (Grid Search) لضبط البارامترات الفائقة [117]. تَمَّ تقييم 50 نموذج مدرب لشبكة الترميز الآلي، بالاعتماد على متوسط الخطأ التربيعي (Mean Squared Error)، وتختلف هذه النماذج بعضها عن بعض بتكوينات البارامترات الفائقة المحتملة. اعتُمد على النموذج الذي يحقق أقل قيمة لمتوسط الخطأ التربيعي، واشتقاقه لكشف الشذوذ في البيانات الشبكية، إذ استطاع النموذج كشف 222 عنواناً شاذاً. بالمقابل إن البحث الشبكي قد يتسبب في زيادة التعقيد الزمني للنموذج، من خلال اختباره لجميع التكوينات المحتملة وذات التأثير الضئيل على الأداء.

استُخدِمَت شبكة الترميز الآلي لبناء نموذج قادر على اكتشاف الحالات الشاذة ضمن تدفقات البيانات المستمرة [118]، واعتُمد على برنامج HyperNOMAD لضبط البارامترات الفائقة. تَمَّ تطبيق النموذج المقترح لاكتشاف الحالات غير المكتملة (الشاذة) ضمن بيانات القياس المرسلة من مركبة الفضاء Curiosity، وأظهرت النتائج فعالية النموذج المقترح في كشف الشذوذ، إذ بلغت قيمة مقياس F1 حوالي 87%. لكن بالمقابل، يفتقر HyperNOMAD إلى استراتيجية بحث عامة (Global).

تَمَّ تقييم شبكة الترميز الآلي في كشف الحالات الشاذة وفق منهجيتين [119]. تعتمد المنهجية الأولى على إزالة بعض الميزات من مجموعة البيانات قبل تمريرها إلى الشبكة باستخدام معامل الارتباط، أما في المنهجية الثانية يتم تمرير جميع الميزات إلى الشبكة. تم اشتقاق النموذج المقترح وتطبيقه لاكتشاف حالات الانهيار في آلات التصنيع، وأظهرت النتائج تفوق المنهجية الثانية وبالنسبة لجميع مقاييس الأداء.

استُخدِمَت خصائص شبكة الترميز الآلي لتحسين أداء أنظمة كشف الشذوذ [120]، وذلك بإزالة الميزات الزائدة التي لا تملك ارتباطات قوية. يُمرر خرج طبقة المرمز (Encoder) ضمن الشبكة، إلى

مجموعة من طرائق تَعلُّم الآلة الكلاسيكية (الانحدار اللوجستي، KNN، شبكة عصبونية متعددة الطبقات) لاكتشاف الحالات الشاذة. كما تَمَّ استخدام تقنية تقليص العينات (Under–Sampling) لتوازن صفي البيانات. أظهرت نتائج الدراسة عند تطبيقها على بيانات شاذة متمثلة بالاحتيال زيادة دقة الكشف من 6% إلى 10%. لكن بالمقابل إن استخدام تقنيات تقليص العينات يؤدي إلى فقدان بعض من الخصائص المهمة في عملية الكشف.

2. الشذوذ في البيانات المتسلسلة (Sequential Data)

يُطلق على البيانات عندما يكون هناك ارتباطات بين عينات المجموعة، مصطلح البيانات المتسلسلة [21]. بمعنى أنه لا يَعْتَمِد كُلّ متغير فقط على قيمه السابقة، بل يَعْتَمِد أيضاً على بعض المتغيرات الأخرى ضمن السلسلة، كالسلاسل الزمنية.

يوجد نوعان للبيانات المتسلسلة وهي السلاسل أحادية المتغير (Univariate) والسلاسل متعددة المتغيرات (Multivariate)، ويختلفان بعدد متغيرات التابع (Dependent Variable) الموجودة ضمن السلسلة.

قَدَّمَت أدبيات الدراسات السابقة العديد من الطرائق والخوارزميات لمعالجة مسائل التصنيف ضِمْنَ السلاسل الزمنية أحادية المتغير (Univariate Time Series). اعْتُمِدت منهجية هجينة لتحسين دقة مصنفات السلاسل الزمنية باستخدام نماذج ماركوف المخفية (Hidden Markov Models) [121]. كما تمَّت مقارنة ثلاث منهجيات من خوارزميات أشجار القرار الشائعة، وهي الغابات العشوائية، AdaBoost،Multi Boost [122] في اكتشاف حالات عدم انتظام ضربات القلب ضِمْنَ السلاسل البيولوجية الزمنية(Biomedical Time–Series) ، وأشارت النتائج إلى تفوق AdaBoost على المصنفات الأخرى. أُسْتُخْدِمَت مؤخراً الشبكات العصبونية الالتفافية في مسائل تصنيف السلاسل الزمنية أحادية المتغير، بهدف دمج كل من مهام التصنيف واستخراج الميزات (Feature Extraction) [123] في إطار عمل واحد.

من جهة أخرى، حظيت السلاسل الزمنية متعددة المتغيرات في الآونة الأخيرة باهتمام كبير لدى العديد من الباحثين. إذ تمَّ معالجة التحديات التي تواجُها [124] ومن أهمها: 1) تدفقات البيانات عالية الأبعاد، 2) الحالات الشاذة الطَّارئة على عمل النظام، وذلك من خلال بناء نظام مراقبة تدفق بيانات حقيقية. حَقَّقَت خوارزميات التَعلُّم العميق نتائج بارزة في مجال تصنيف السلاسل الزمنية متعددة المتغيرات.

تَفَوَّقَت الشبكات العصبونية العميقة على الأساليب القائمة على الميزات [125] في تَعلُّم ميزات السلاسل الزمنية، تمَّ تطوير شبكة عصبونية التفافية متعددة القنوات (Multi–Channels) لتصنيف السلاسل الزمنية ضِمْنَ مجموعتين من بيانات العالم الحقيقي، إذ تَتَعلّم الشبكة الميزات من سلاسل زمنية أحادية المتغير في كل قناة، ومن ثم يَتِمُّ جمع المعلومات من جميع القنوات لتمثيل الميزات المهمة في الطبقة النهائية. أظْهَرَتْ النتائج التجريبية قدرة التَعلُّم العميق على تَعلُّم الميزات الأكثر أهمية، مما يُساعد على تحسين أداء التصنيف. بالمقابل لم تستخدم الدراسة تقنيات ضبط البارامترات الفائقة، بالإضافة لتحديد عَتَبة التصنيف على نحوٍ يدوي.

تَمَّت مقارنة أربعة نماذج مختلفة للتَعلُّم العميق [126] وهي: الشبكات العصبونية الصنعية (Artificial Neural Networks)، الوحدة المتكررة ذات البوابات (Gated Recurrent Units)، والشبكات العصبونية التكرارية (Recurrent Neural Networks)، والذاكرة قصيرة طويلة المدى (LSTM) في مسائل كشف الشذوذ القائم على التسلسل. أظْهَرَتْ النتائج تفوق LSTM على النماذج الأخرى، وتَوَصَّلَت الدراسة إلى تحديد الطوبولوجيا المناسبة لكل نموذج باستخدام ضبط البارامترات الفائقة. **بالمقابل لم تَتَطرّق الدراسة إلى موضوع تحديد عَتَبة التصنيف على نحوٍ ديناميكي.**

استُخدِمَت الذاكرة قصيرة طويلة المدى (LSTM) لبناء نموذج كشف الشذوذ ضِمْنَ طلبات المستهلك في إدارة سلسلة التوريد [127]. حَقَّقَت الشبكة تفوقاً على خوارزمية آلة شعاع الدعم في دقة الكشف، كما اعتَمَدت الدارسة على طريقة توقع الكميات (Quantiles Estimation) لتحديد قِيمَة العَتَبة. ومع وجود تفوقٍ للنموذج المُقْتَرَح في كشف الحالات الشاذة، فإنهُ من المُمَكِّن تطويره من خلال التحكم بتدفق البيانات واختزالها قدر الإمكان، من خلال بناء نموذج هجين بين LSTM وأحد الشبكات العصبونية العميقة مثل شبكة الترميز الآلي والشبكة الالتفافية.

بهدف تحسين اكتشاف الشذوذ ضمن التسلسلات المرتبطة بالزمن، تم استخدام الذاكرة قصيرة طويلة المدى (LSTM) مع مفهوم آلة الانتباه (AM: Attention Machine) [18]. تعمل AM على حساب تأثير التسلسلات الزمنية السابقة على التسلسل الأخير، وإعطاء أوزان للتسلسلات الأكثر أهمية، ثم تُمرر هذه الأوزان كدخل لشبكة الذاكرة طويلة المدى. تم اشتقاق النموذج المقترح وتطبيقه لاكتشاف الحالات الشاذة (الهجمات) ضمن بيانات حركة الشبكة، وأظهرت النتائج قدرة النموذج على اكتشاف 96% من الهجمات (Recall =96%). لكن بالمقابل إنَّ النموذج غير قادر على التعامل مع حالات الشذوذ الديناميكية من جهة، وعلى تحديد عتبة التصنيف من جهة أخرى.

بهدف حل المشاكل المتعلقة بندرة البيانات الشاذة ومعالجة الضجيج. استُخدِمَت شبكات الخصومة التوليدية (Generative Adversarial Networks) لكشف الشذوذ ضمن السلاسل الزمنية متعددة المتغيرات [128]. يتم بناء المميز (Discriminator) والمولد (Generator) كشبكات عصبونية متكررة قصيرة طويلة المدى (LSTM–RNN)، حيث يستخدم المميز لكشف التسلسلات الزمنية الشاذة الناتجة عن المولد. تم اشتقاق النموذج المقترح لاكتشاف الهجمات الإلكترونية، وأظهرت النتائج فعالية جيدة للنموذج في كشف الحالات الشاذة. لكن بالمقابل نوّه الباحثون بضرورة اختيار الميزات الأكثر أهمية لتحسين أداء النموذج، بالإضافة إلى أن المولد بعد مرحلة معينه من التدريب، يصبح قادراً على خداع المميز.

4-3-2- النماذج الهجينة العميقة (Deep Hybrid Model)

توجهت الدراسات في مجال اكتشاف الشذوذ لاستخدام طرائق هجينة [129] [130]، من أجل تحسن أداء عمل أنظمة كشف الشذوذ. تعتمد النماذج الهجينة على الجمع بين اثنين أو أكثر من طرائق كشف الشذوذ القائمة على التَعلُّم العميق.

1. الشذوذ في البيانات غير المتسلسلة (Non–Sequential Data)

بهدف الاستفادة من خصائص كل من شبكة الترميز الآلي والشبكة العصبونية الالتفافية، تم دمج الشبكتين معاً لكشف الشذوذ [131]، استطاع النموذج المقترح (CNN–AE) تقليل زمن التدريب بالمقارنة مع شبكة الترميز الآلي التقليدية. تم اشتقاق النموذج وتطبيقه لاكتشاف الشذوذ (الاختراقات) ضمن البيانات الشبكية، وأظهرت النتائج تفوّق النموذج على شبكة الترميز الآلي على نحوٍ طفيف من حيث الدقة وزمن التدريب. لكن بالمقابل فإن تحويل دخل الشبكة الالتفافية من ثلاثية البعد (3D) إلى ثنائية البعد (2D)، يفقد البيانات بعض من خصائصها الإحصائية، وهذا هو السبب الرئيسي في زيادة الدقة.

استُخدم مفهوم نقل التَعَلُّم (Transfer Learning) لتطوير أداء عمل أنظمة كشف الشذوذ [132]. تَمَّ الاعتماد على نموذج Google Net [133] للاستفادة من البيانات المدربة مسبقاً، وتمريرها إلى شبكة عصبونية التفافية (CNN). استطاع النموذج المقترح عند تطبيقه على بيانات شبكية، تحسين دقة الكشف بمقدار 4%. لكن بالمقابل فإن نموذج Google Net تم تدريبه لمهام محددة كاكتشاف البرامج الضارة على الشبكة، ويحتاج إلى المزيد من التدريب لتعميمه على مجالات أوسع.

استُخدِمَت الشبكة العصبونية الالتفافية المدربة مسبقاً على مجموعة ImageNet لنقل التَعَلُّم إلى شبكة عصبونية متعددة الطبقات، بهدف تصنيف الحالات الشاذة (المرضية) ضمن مجموعة من صور

الأشعة السينية [134]. تم اشتقاق النموذج وتطبيقه في تشخيص مرض كوفيد-19. تضمنت عينة الدراسة 1431 صورة للرئتين بالأشعة السينية، حيث تم تأكيد وجود مرض كوفيد-19 ضمن 70 صورة فقط. أظهرت نتائج الدراسة قدرة النموذج المقترح على اكتشاف 96% من حالات مرض كوفيد-19 (Recall=96%)، بينما بلغت نسبة الصور التي صُنِّفت على نحوٍ خاطئ على أنها مرض كوفيد-19 حوالي 4% (FNR=4%)، وذلك عند تحديد قيمة ثابتة 0.15 لعتبة التصنيف.

2. الشذوذ في البيانات المتسلسلة (Sequential Data)

تمَّ بناء عدة نماذج هجينة باستخدام شبكات عصبونية عميقة لتصنيف السلاسل الزمنية متعددة المتغيرات، ومن أهمها شبكة الذاكرة قصيرة طويلة المدى (LSTM) والشبكة الالتفافية (CNN) وشبكة الترميز الآلي [135] [136] [137].

أُسْتُخْدِمَت الشبكة (CNN-LSTM) لبناء نموذج اكتشاف الأنماط غير الطبيعية [6] في حركة بيانات السلاسل الزمنية عبر الويب. إذ تُستَخدم الشبكة الالتفافية لتقليل أبعاد الميزات المكانية (Spatial Features)، بينما يكون الهدف من LSTM نمذجة معلومات الوقت. حَقَّقَ النموذج المُقْتَرَح أداء غير مسبوق للكشف عن الحالات الشاذة حتى مع البيانات المتشابهة جداً. ومع تفوق هذه الطريقة، مالت دقتها للانخفاض عند اكتشاف القيم الشاذة التي يَتِمُّ إنشاؤها عند حدود نوافذ البيانات، لأن الطريقة المقترحة تعالج البيانات مسبقاً باستخدام النوافذ الزمنية المنزلقة.

اِستَطاعَ النموذج (LSTM-CNN) التفوق على جميع النماذج الأخرى [33] في التعامل مع السلاسل الزمنية. إذ لا يحتاج للكثير من عمليات المعالجة المسبقة للبيانات، وكان ذا كفاءة عالية في وقت الاختبار. تمَّ اختبار النموذج على أكثر من 30 مجموعة بيانات متنوعة ومن ضِمْنَها بيانات صناعية. لكن على الجانب الآخر، **لم يَتِمُّ ضبط البارامترات الفائقة، بالإضافة إلى عدم تحديد العَتَبة للنموذج على نحوٍ ديناميكي.**

بهدف تحسين التنبؤ بالحالات الشاذة ضمن سلاسل البيانات الزمنية. دمجت شبكة الترميز الآلي مع الذاكرة قصيرة طويلة المدى على الترتيب [138]. يمرر خرج المرمز ضمن شبكة الترميز الآلي إلى وحدة الذاكرة طويلة المدى. استطاع النموذج المقترح (AE-LSTM) اختزال الميزات من البيانات عالية البعد، والتنبؤ بالأحداث الشاذة على نحوٍ أسرع وفي الوقت الحقيقي. تم اشتقاق النموذج المقترح وتطبيقه لاختبارات الطيران للتحقق من وظائف الصحة والسلامة للطائرات، وأظهرت النتائج عند اختبار النموذج على بيئة خاصة بشركة الطيران تفوقه من حيث زمن الكشف بنسبة 36%.

تمَّ الاعتماد على خصائص كل من شبكتي Autoencoder و LSTM لبناء نموذج هجين لكشف الشذوذ القائم على التسلسل ضِمْنَ مجموعتي بيانات حقيقية وصناعية [19]. أظْهَرَتْ النتائج أن لدمج الشبكتين السابقتين تأثيراً كبيراً في زيادة دقة الكشف مقارنة باستخدام كُلّ شبكة على حِدة. حيث يتميز النموذج (LSTM–Autoencoder) بقدرته على التعامل مع البيانات عالية الأبعاد من جهة، ومن جهة تذكر الأنماط المعقدة لفترات أطول. بالمقابل لم تَعْتَمِد الدراسة على أي منهجية لتحديد العَتَبَة بشكل ديناميكي.

يستعرض الجدول الآتي مقارنة بين تقنيات كشف الشذوذ القائمة على التَعلُّم العميق وتقنيات كشف الشذوذ القائمة على طرائق تَعلُّم الآلة، إذ يؤكد على تفوق تقنيات كشف الشذوذ العميقة.

الجدول 4–2 مقارنة بين طرائق الكشف العميقة والكلاسيكية

التقنيات المستخدمة	نتائج الدراسة	المقاييس	المرجع
SVM, KNN, deep NN	تفوق الشبكة العصبونية العميقة؛ لكن لا تتكيف مع حالات الشذوذ الجديدة	Accuracy = 99% Precision =81%	[139]
NN, MLP, CNN	تفوق MLP؛ لكن جميع التقنيات المقترحة هي تعلم بإشراف	Precision = 95%	[140]
CNN, LSTM	تفوق شبكة LSTM؛ لكنها تتطلب استخدام تقنيات إعادة تكوين العينات	F1 = 84.85%	[34]
SVM, RF, LR, LSTM	تفوق شبكة LSTM؛ لكن يجب ألا تتجاوز عدد الدورات حداً معيناً	Loss Rate = 0.21	[141]
LSTM, SVM, MLP, NB	تفوق شبكة LSTM، لكن لم تستخدم تقنيات ضبط البارامترات الفائقة	Precision = 85% Recall = 88%	[142]

تمَّ ملاحظة التفوّق الكبير من خلال أدبيات الدراسات السابقة للشبكات العصبونية العميقة في مجال اكتشاف الشذوذ ضمن البيانات على باقي الطرائق، وبرز في العديد منها قدرة شبكة الترميز الآلي على إيجاد الحالات الشاذة في كل من بيانات العالم الحقيقي والمحاكاة [114] [115] [143] [144]. كما تم توضيح الحالات التي تتفوق بها الشبكة على طرائق الكشف الأخرى [99]، وأظهر المسح المرجعي للأبحاث السابقة التوجه لدمج شبكة الذاكرة قصيرة طويلة المدى (LSTM) مع شبكة الترميز الآلي بهدف التقاط التبعيات الزمنية لتسلسل الشذوذ ضِمْنَ سلاسل البيانات [138] [19].

لكن في الوقت نفسهُ تمَّت ملاحظة القصور الحاصل فيما يتعلق ببناء أنظمة كشف الشذوذ، ولعلَّ أهمها دراسة الميزات الأكثر أهمية في اكتشاف الشُّذُوذ، اختيار قِيَم البارامترات الفائقة الأفضل وبخاصَّةٍ مع ازدياد عددها؛ إضافةً إلى دراسة توزيع البيانات وتَحْدِيدِ عَتَبَةِ التصنيف على نحوٍ ديناميكي، وأخيراً تنوع الحالات الشاذة. اِستَوجَبَ كل ذلك المزيد من البحث لبناء نظام ديناميكي للكشف عن الحالات الشاذة، يكون قادراً على اختزال الميزات عالية الأبعاد، والتقاط جميع الحالات الشاذة. بالإضافة إلى تحديد عَتَبة التصنيف الأمثل على نحوٍ ديناميكي، دون وضع فرضيات حول توزع البيانات وطبيعتها. لتَحَقيق ذلك كان لا بدّ من الاعتماد على النماذج الهجينة بين شبكات التَعلُّم العميق، وإيجاد أفضل قِيَم البارامترات الفائقة لها بهدف تحسين أدائها.

الفصل الخامس

تحليل أنظمة كشف الشذوذ

يَتَضَمَّن هذا الفصل الْمَنْهَجِيَّة التي اِتَّبَعَتْهَا هذه الدراسة لِتَحْلِيلِ عمل الْأَنْظِمَة الْكِلَاَسِيكِيَّة لكشف الشذوذ المعمول بها حالياً، بِهَدَف تحديد كفاءة هذه الْأَنْظِمَة من حيث زمن التدريب ونسبة الكشف. وَقَدْ تَوَصَّلَتْ نتائج التَّحْلِيل إلى تَحديد السيناريو الأفضل في بناء هذه الأنظمة وبخاصَّةٍ فيما يَتَعَلَّق بترتيب إجراءات ضبط البارامترات الفائقة واختيار الميزات الأكثر أهمية.

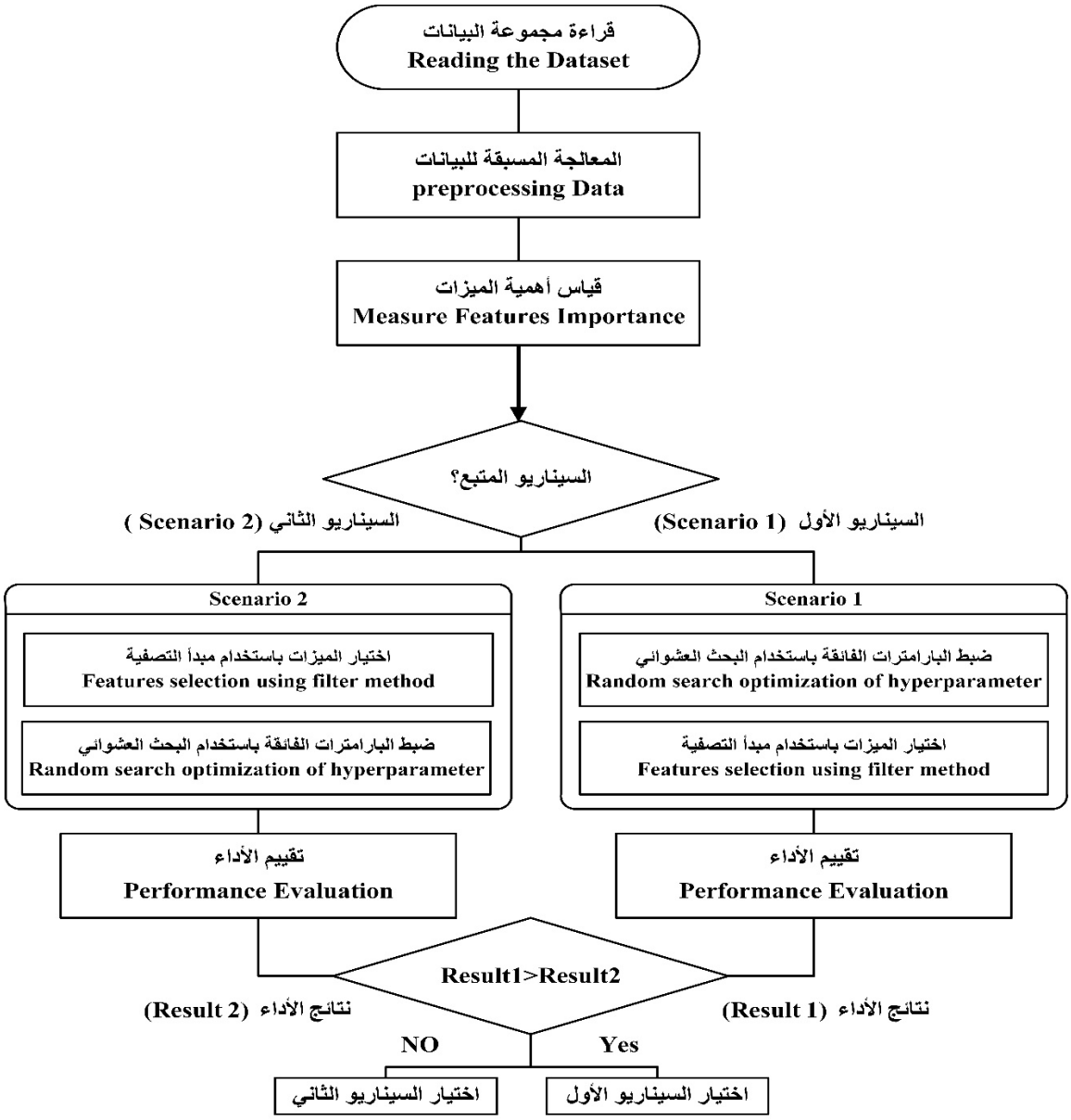
اعتمدت الدراسة لإجراء عملية التحليل على خوارزميتين من أكثر خوارزميات تَعَلُّم الآلة انتشاراً في مجال كشف الشذوذ، وفقاً لما تضمنتهُ الأدبيات السابقة المتعلقة بمجال الدراسة، وهما خوارزميتي الغابات العشوائية (RF) وآلة شعاع الدعم (SVM). بالإضافة إلى استخدام مجموعتي الاحتيال الأوروبية والمجردة لاختبار السيناريوهات المقترحة.

5-1- منهجية التحليل (Analysis Methodology)

يتأثر أداء عمل أنظمة كشف الشذوذ القائمة على تَعَلُّم الآلة بعامّةٍ بمجموعة من العوامل. لكنها تتأثر على نحوٍ كبير بترتيب إجراءات ضبط البارامترات الفائقة، واختيار الميزات الأكثر أهمية ضمن مجموعات البيانات، إذ يؤدي اختيار مجموعة من قِيَم البارامترات الفائقة إلى اختلاف مجموعة الميزات المحددة والعكس صحيح، وينعكس ذلك بدوره على عمل هذه الأنظمة من حيث دقة الكشف والزمن اللازم لتطوير هذه الأنظمة. يوضح **الشكل 5-1** خطوات منهجية التحليل المتبعة ضمن الدراسة الحالية.

1. المعالجة المسبقة (Preprocessing)

بدايةً وقبل البدء ببناء هذه الأنظمة، يجب إجراء المعالجة المسبقة (Preprocessing) لمجموعات البيانات المستخدمة، مثل ملء القيم المفقودة (Missing Values)، وترميز البيانات الفئوية (Categorical Data Encoding)، وتَقيِيس البيانات (Data Standardization) وما إلى ذلك. يَتِمُّ قبل تَقيِيس البيانات، تقسيمها إلى مجموعة تدريب (Training Set) ومجموعة اختبار (Testing Set)، إذ تَمَّ تَقيِيس بيانات التدريب أولاً، ثم تَقيِيس بيانات الاختبار باستخدام المتوسط والانحراف المعياري لبيانات التدريب بعد تَقيِيسها، مما يُبقي بيانات الاختبار غير معروفة في أثناء النمذجة. مع العِلم أن تقسيم مجموعات البيانات المستخدمة يَتِمُّ بنسبة **70%** لبيانات التدريب و**30%** لبيانات الاختبار.



الشكل 5-1 منهجية التحليل المقترحة. المصدر: الدراسة الحالية

بعد الحصول على مجموعة بيانات التدريب، يَتِمُّ تقسيمها باستخدام التحقق من الصحة المتقاطع (CV: Cross Validation)، بهدف ضبط البارامترات الفائقة من جهة، وتقليل تحيّز المصنفات لبعض العينات في بيانات التدريب من جهة أخرى [145].

تحتوي طريقة CV على بارامتر واحد هو K، يشير إلى عدد مجموعات التقسيم، يُطلق عادةً على هذه الطريقة K-Fold cross validation. ومن ثَمَّ منح كل عينة من بيانات التدريب الفرصة لاستخدامها

في تدريب النموذج $k-1$ مرة، ومرة واحدة في اختبار النموذج. يَتُّم حساب متوسط خطأ جميع تجارب k لتقييم كفاءة النموذج. وفق الصيغة الرياضية الآتية.

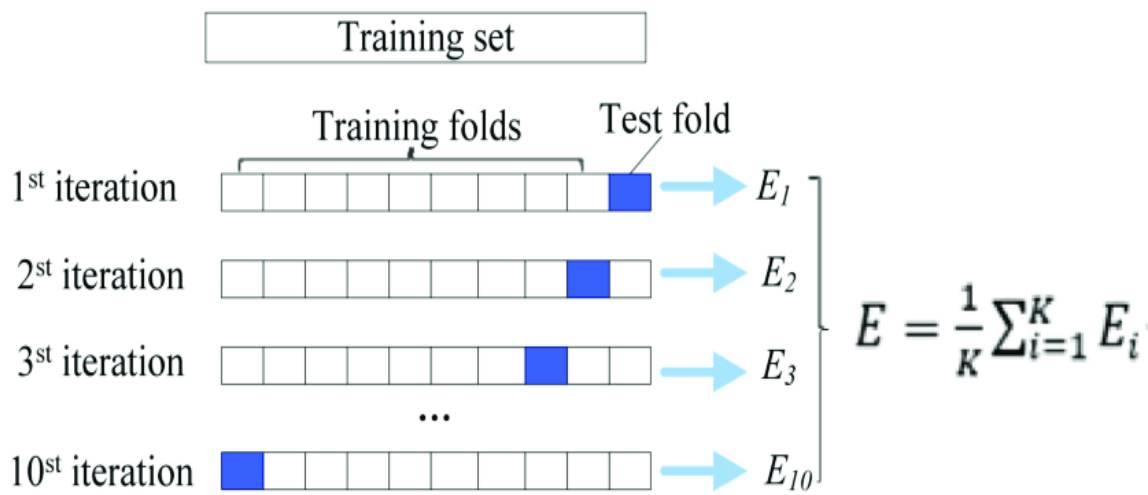
$$E = \frac{1}{K}\sum_{i=1}^{K} E_i \qquad (5\text{-}1)$$

k: عدد مجموعات التقطيع

E_i: خطأ النموذج من أجل المجموعة i

يجب اختيار قيمة k بعناية، فقد يؤدي اختيار قيمة عشوائية إلى تصور خاطئ لكفاءة النموذج. يُوصَى عادة باختيار $k = 10$.

يوضح **الشكل 5-2** كيفية تقسيم البيانات باستخدام طريقة التحقق من الصحة المتقاطع



الشكل 5-2 استخدام 10-Fold cross validation في تدريب المصنفات

بالنسبة لبيانات الاحتيال المجردة فقد تمَّ ترميز الميزات الفئوية الموضحة في **الجدول 3-2** ضمن الفصل الثالث من هذه الأطروحة، باستخدام مفهوم ترميز التسمية (Label Encoding) [146]، إذ يَتِمُّ تحويل كل تسمية إلى قيمة عدد صحيح (0,1). بالإضافة لحذف ميزة تاريخ المعاملة لأن قِيَمها مفقودة.

2. اختيار السيناريو المستخدم لبناء النظام

كما أُشير سابقاً، إنَّ الهدف من إجراء التحليل هو تحديد السيناريو الأنسب لبناء أنظمة كشف الشذوذ، فيما يتعلق بترتيب إجراءات ضبط البارامترات الفائقة واختيار الميزات الأكثر أهمية لتحقيق أفضل

أداء من حيث الزمن ونسبة الكشف. اعتمدت الدراسة الحالية للوصول إلى ذلك على سيناريوهين يختلفان بترتيب تلك الإجراءات.

يكون ترتيب الإجراءات ضمن **السيناريو الأول** على الشكل الآتي:

1) ضبط البارامترات الفائقة للخوارزميات المستخدمة.

2) اختيار الميزات الأكثر أهمية التي تحقق أفضل أداء لهذه الخوارزميات، باستخدام البارامترات الفائقة المحددة من الخطوة الأولى.

بينما يكون ترتيب الإجراءات ضمن **السيناريو الثاني** على الشكل الآتي:

1) اختيار الميزات الأكثر أهمية.

2) ضبط البارامترات الفائقة للخوارزميات، بالاعتماد على الميزات المحددة من الخطوة الأولى.

3. اختيار الميزات (Features Selection)

تعتمد الدراسة الحالية لاختيار الميزات في أثناء تحليل الأنظمة الكلاسيكية لكشف الشذوذ على الغابات العشوائية، إذ تتمتع بخاصية قياس الأهمية النسبية (Relative Importance) [56] لكل ميزة في التصنيف. يَتُّم قياس أهمية الميزة من خلال النظر إلى عدد العقد النقية في نهاية جميع الأشجار التي تستخدم هذه الميزة (يحدث الانقسام عندها باتجاه واحد). بمعنى آخر، تكون العقد الشائبة (Impurity Nodes) في بداية الشجرة، بينما تحدث الملاحظات (Observations) التي تُسبب نقصاً في شوائب العُقد في نهاية الشجرة. بتقليم الأشجار أسفل العقد النقية يمكننا إنشاء مجموعة فرعية من أهم الميزات. يمكن من خلال النظر إلى الأهمية النسبية للميزة اختيار الميزات التي من المحتمل حذفها، لأنها لا تُسهم بشكل كافٍ (أو أحياناً لا تساهم على الإطلاق) في عملية التصنيف.

يُبَيِّن **الجدول 5-1** ترتيب أهمية الميزات لمجموعة بيانات الاحتيال الأوروبية، التي توصلت إليها الدراسة الحالية بناءً على الأهمية النسبية لكل ميزة، علماً أنهُ تم تَقيِيس الأهمية النسبية لجميع الميزات ليصبح مجموعها يساوي الواحد.

يظهر بوضوح من خلال الجدول أن الميزات (V14,V4,V12 and V10) لها أهمية نسبية أكبر من باقي الميزات، ولذلك تُسهم في زيادة دقة المصنف، على عكس الميزات (V24,V28 and Time) التي لها دور أقل في تحسين دقة المصنف.

الجدول 5-1 الأهمية النسبية لميزات مجموعة بيانات الاحتيال الأوروبية

Rank	Feature	Score	Rank	Feature	Score	Rank	Feature	Score
1	V14	0.184	**11**	V9	0.022	**21**	V15	0.009
2	V4	0.113	**12**	V21	0.020	**22**	V1	0.007
3	V12	0.109	**13**	V19	0.017	**23**	V13	0.007
4	V10	0.101	**14**	V27	0.012	**24**	V6	0.007
5	V17	0.088	**15**	V5	0.012	**25**	V22	0.006
6	V3	0.058	**16**	V18	0.012	**26**	V23	0.006
7	V11	0.046	**17**	Amount	0.012	**27**	V25	0.006
8	V16	0.044	**18**	V8	0.011	**28**	V24	0.005
9	V2	0.036	**19**	V26	0.009	**29**	V28	0.005
10	V7	0.023	**20**	V20	0.009	**30**	Time	0.005

يُبَيِّن **الجدول 5-2** ترتيب أهمية الميزات لمجموعة بيانات الاحتيال المجردة، التي توصلت إليها هذه الدراسة بناء على الأهمية النسبية لكل ميزة.

الجدول 5-2 الأهمية النسبية لميزات مجموعة بيانات الاحتيال المجردة

Rank	Feature	Score
1	Total Number of declines/days	0.217
2	Transaction amount	0.192
3	Is Foreign Transaction?	0.168
4	Is High Risk Country?	0.132
5	Average Amount of Transaction/day	0.078
6	6_month_ chargeback _ frequency	0.078
7	6_month_avg_ chargeback _amt	0.064
8	Daily chargeback average amount	0.061
9	Is declined?	0.011
10	Transaction Date	0.0

تظهر النتائج المبينة في الجدول السابق أن أهم الميزات التي حصلنا عليها هي عدد حالات الرفض خلال اليوم الواحد بالمرتبة الأولى يليها كُلّ من كمية المناقلة، وهل المناقلة أجنبية أو لا؟ وهل هي من بلد مصنف على أنه ضمن البلدان ذات الخطورة العالية؟ في المراتب 2 و3 و4 على الترتيب. هذه النتائج منطقية لو نظرنا إليها بِتَمَعُّن، وهذا إن دل على شيء فإنما يدل على قدرة الخوارزمية على تحديد الميزات الأهم فعلياً وترتيبها ترتيباً مقبولاً حسب درجة أهميتها وعلاقتها بكشف الشذوذ المطلوب.

في المقابل يظهر أيضاً بوضوح من خلال الجدول أن ميزة **هل المعاملة مرفوضة؟** (Is declined?) ليس لها أهمية كبيرة في زيادة دقة المصنف، ولذلك ساهمت الخوارزمية في معرفة الميزات التي من الأفضل حذفها لضعف أهميتها وارتباطها بكشف الشذوذ قبل تدريب المصنف.

بعد قياس الأهمية النسبية لميزات مجموعات البيانات المستخدمة، يَتِمُّ اختيار الميزات الأكثر أهمية التي تُسهم في زيادة دقة المصنف، من خلال الاعتماد على مبدأ التصفية (Filter) باستخدام مقاييس إحصائية كالدقة والاسترجاع. لذلك تمّ تدريب المصنف من خلال زيادة عدد الميزات بدءاً من الميزة ذات الأهمية الأكبر (وفقاً لترتيب أهمية الميزات)، وصولاً إلى الميزة التي لا يحدث بعدها أي تحسين في دقة المصنف.

4. ضبط البارامترات الفائقة (Hyperparameters Tuning)

تعتمد هذه الدراسة لضبط قِيَم البارامترات الفائقة لمصنفات الغابات العشوائية (RF) وآلة شعاع الدعم (SVM) على تقنية البحث العشوائي (Random Search). تَمَّ تدريب تلك الخوارزميات باستخدام عدد من التكوينات المرشحة (Candidate Combinations) للبارامترات الفائقة الخاصة بها، إذ وصل عددها من أجل خوارزمية SVM إلى **1200** تكوينة مرشحة، وفي خوارزمية الغابة العشوائية إلى **302400** تكوينة مرشحة. لذلك من أجل الوصول إلى التكوينات الأمثل لهذه الخوارزميات بأقل زمن ممكن وأكثر دقة، كان لا بد من ضبط البارامترات الفائقة باستخدام تقنيات تحسين البارامترات الفائقة، وتحديداً البحث العشوائي (وفق ما تم الإشارة إليه في الفصل الثالث من هذه الأطروحة)

يوضح **الجدول 5-3** مجال القِيَم للبارامترات الفائقة الخاصة بخوارزمية الغابات العشوائية ضِمن الدراسة الحالية، ومن أجل مجموعتي البيانات المستخدمة.

الجدول 5−3 مجال القيم لبارامترات الغابة العشوائية

Hyperparameters	Type		Range		Range
Maximum Depth of Tree	Integer	European Dataset	[40,200]	Abstract Dataset	[10,60]
Min of Samples to Split	Integer		[2,10]		[1,7]
Number of Trees	Integer		[100,1000]		[10,100]
Number of Features	Real		[1,28]		[1,10]
Min of Samples to be at leaf	Integer		[1,10]		[1,5]
Bootstrap	Bool		True, False		True, False

يوضح **الجدول 5−4** مجال القِيَم للبارامترات الفائقة الخاصة بخوارزمية آلة شعاع الدعم في هذه الدراسة، ومن أجل مجموعتي البيانات المستخدمة.

الجدول 5−4 مجال القيم لبارامترات آلة شعاع الدعم

Hyperparameters	Type		Range		Range
Regularization	Real	European Dataset	[0.001,3000]	Abstract Dataset	[0.001,1000]
Gamma	Real		[1e−7,1e−2]		[1e−5,1e−2]
kernel	Categorical		• Sigmoid • Linear • rbf		• Sigmoid • Linear • rbf

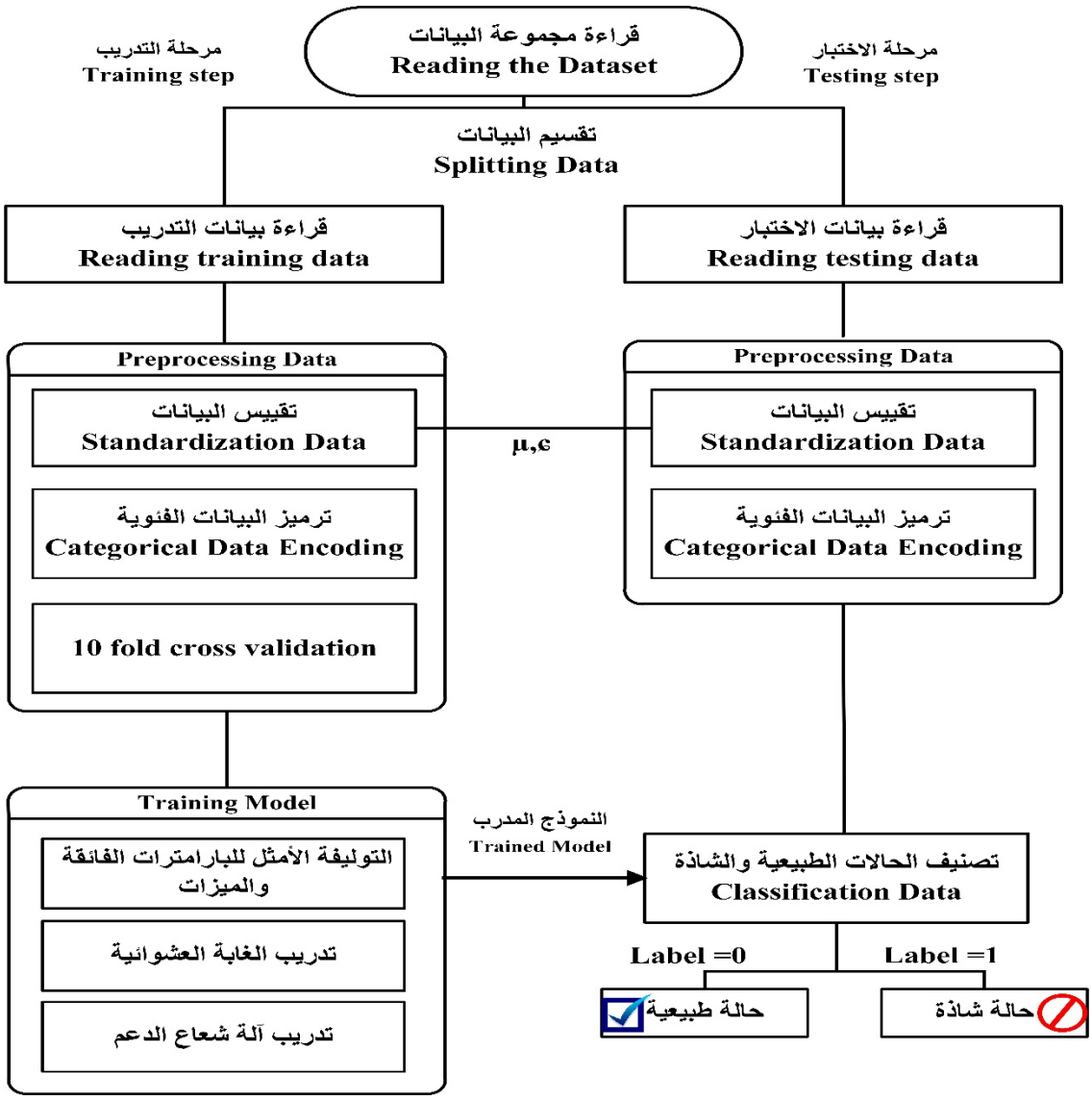
يَتِمُّ اختيار تكوينات البارامترات الفائقة التي تحقق أفضل أداء للمصنفين السابقين، بالاعتماد على مقياس $f1_{macro}$ ، إذ يسعى البحث العشوائي إلى إيجاد التكونية التي تُعظِّم قيمة المقياس المذكور.

5. تقييم الأداء (Performance Evaluation)

يَتِمُّ اختبار النظام باستخدام المقاييس المشار إليها في الفصل الثالث، لتحديد السيناريو الأفضل لبنائه من حيث زمن البناء ودقة الكشف. سيتم عرض نتائج تحليل الأنظمة في الفصل السابع: النتائج والمناقشة.

5-2- بناء نظام الكشف (Detection System Creation)

يوضح **الشكل 5-3** مراحل بناء النظام الموضحة أعلاه بدءاً من المعالجة المسبقة للبيانات وصولاً إلى تدريب النظام باستخدام التوليفة الأمثل من قِيَم البارامترات الفائقة والميزات الأكثر أهمية التي تَمَّ الحصول عليها من منهجية التحليل المقترحة في هذه الدراسة. إن استخدام التوليفة الناتجة تساعد النظام في جعله أكثر فعالية من حيث كشف الحالات الشاذة وتقليص الزمن اللازم لتطويره، وهذا ما ستؤكده نتائج الدراسة الحالية في الفصل السابع من هذه الأطروحة.



الشكل 5-3 خطوات بناء نظام كشف الشذوذ بالاعتماد على نتائج التحليل. المصدر: الدراسة الحالية

الفصل السادس

نظام كشف الشذوذ المقترح

يتضمن الفصل الحالي شرحاً عن نظام كشف الشذوذ المقترح AEDT–ADS وهو اختصار لـ : **A**uto–**E**ncoder with a **D**ynamic **T**hreshold – **A**nomaly **D**etection **S**ystem. كما هو واضح من التسمية فهو نظام كشف شذوذ يعتمد على شبكة AEDT المقترحة في هذه الدراسة، والتي تتمتع بقدرتها على تحديد عَتَبَة التصنيف ديناميكياً. سُميّت الشبكة المقترحة والمعدلة من شبكة الترميز الآلي، شبكة الترميز الآلي مع عَتَبَة ديناميكية (Autoencoder with a Dynamic Threshold).

يَتَمَتَّع النظام المقترح AEDT–ADS، بقدرتهِ على تقليص أبعاد بيانات الدخل، واكتشاف الميزات غير المرتبطة خطياً وتحديد قِيَم البارامترات الفائقة آلياً من جهة. ومن جهة أخرى فإنه يستخدم عَتَبَة تصنيف ديناميكية لفصل البيانات الطبيعية عن البيانات الشاذة.

بالإضافة لما سبق يُمكن إضافة وحدة الذاكرة قصيرة طويلة المدى (LSTM) إلى بنية النظام، بهدف تَمْكِينِ النظام من تذكر الحالات السياقية للبيانات الشاذة. يُرمَّز النظام عندئذٍ بـ AEDTM–ADS (**AEDT** LST**M** – **A**nomaly **D**etection **S**ystem)، إذ يُمكن تفعيل وحدة الذاكرة أو إلغاءها حسب مقتضيات طبيعة الحالة المدروسة.

تَمَّ اختبار النظام المقترح بحالتيه مع ذاكرة ومن دونها على مجموعتي بيانات حقيقية وهما، مجموعة الاحتيال الأوروبية، ومجموعة كسر الورق. إن السبب الرئيسي لاختيار هاتين المجموعتين هو احتواؤهما على عدد كبير من الميزات (متعددة الأبعاد) من جهة، ومن جهة أخرى على أنواع شذوذ مختلفة (شذوذ نقطة، وشذوذ سياق).

6–1– شبكة الترميز الآلي مع عتبة ديناميكية (Overall Procedure of AEDT)

تَمَّ تعديل المنهجية الأساسية لشبكة الترميز الآلي التقليدية (AE) بحيث تصبح قادرة على تحديد عَتَبَة التصنيف على نحوٍ ديناميكي. تتضمن شبكة الترميز الآلي مع عَتَبَة ديناميكية (AEDT) مراحل إضافية تُعزّز من آلية الاكتشاف وتحدد العَتَبَة على نحوٍ ديناميكي. كما تَمّ اختيار أهم الميزات وضبط البارامترات الفائقة للشبكة، للاستفادة من كُلّ ذلك في جعل النظام أداة متكاملة وفعالة في اكتشاف الشذوذ.

يوضح الترميز الآتي إجرائية شبكة الترميز الآلي مع عتبة ديناميكية (AEDT) المقترحة في هذه الدراسة. تَتَعلَّم الشبكة في أثناء التدريب التمثيلات الطبيعية للبيانات لِتُعيد إنتاجها في طبقة الخرج، ثم تقوم بحساب المتبقي (Residual) أو ما يسمى خطأ إعادة البناء للبيانات الطبيعية التي لم يَتُّم تَعلّيمها للنموذج باستخدام متوسط الخطأ التربيعي (MSE). تأتي بعد ذلك المرحلة الهامة والإضافية وهي حساب عَتَبَة التصنيف ديناميكياً، والتي يمكن أن تتغير مع مرور الوقت نتيجة لتباين طبيعة بيانات الدخل.

Pseudo Code of AEDT for Calculate Dynamic Threshold

Input	X_n: normal data that is used in the training model Y_n: normal data that is not learned by the trained model
Output	T: Dynamic threshold
Parameters	$\emptyset$: encoder, Θ : decoder. e : reconstruction error $e \sim$: distribution of error e μ : mean of reconstruction error σ : standard deviation of reconstruction error k: integer number ($k > 1$)

Step 1: Train AEDT:

$\emptyset$, $\Theta \leftarrow$ train an AEDT using the normal dataset X_n
for i =1 to Y_n do // encoder function $f_\emptyset$, decoder function g_Θ
$e\ (i) = \left\| x^{(i)} - g_\Theta\ (f_\emptyset\left(x^{(i)}\right)) \right\|$ // reconstruction error of normal data
end for
// PS: do not use normal training data to calculate DT to avoid model overfitting

Step 2: Calculate Dynamic Threshold:

$e \sim \leftarrow$ get reconstruction error distribution for only normal points that are not learned by the trained model using Kolmogorov-Smirnov Test
if $e \sim$ is normal distribution
[μ ± kσ] ⟵ based on Empirical Rule
else
[μ ± kσ] ⟵ based on Chebyshev's Theory
end if
$T \leftarrow$ Threshold selection within [μ ± kσ] based on the target of system

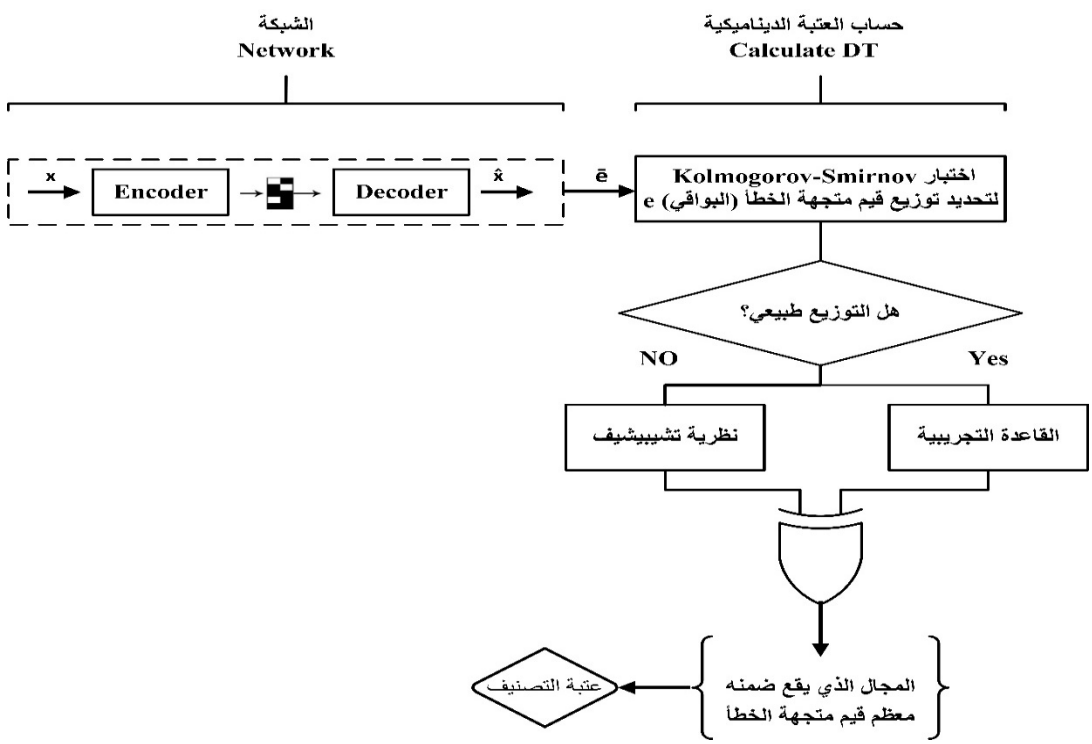
تعتمد مرحلة حساب عتبة التصنيف (DT) على تحديد نوع التوزيع (Distribution) لقِيَم متجهة الخطأ $\vec{e}$ أولاً، وتَمَّ الاعتماد على اختبار كولموغوروف سميرنوف (Kolmogorov–Smirnov test)، لاختبار مدى ملائمة بيانات المتجهة لأحد التوزيعات المحتملة. يَتمُّ بعد ذلك بناءً على نوع التوزيع المحدد، اختيار الإجراء اللازم لإيجاد المجال الذي تقع ضِمنَهُ معظم قِيَم متجهة الخطأ. تستخدم AEDT القاعدة

التجريبية (Empirical Rule) من أجل التوزيع الطبيعي، أما فيما عدا ذلك فإنها تستخدم نظرية تشيبيشيف (Chebyshev's Theory).

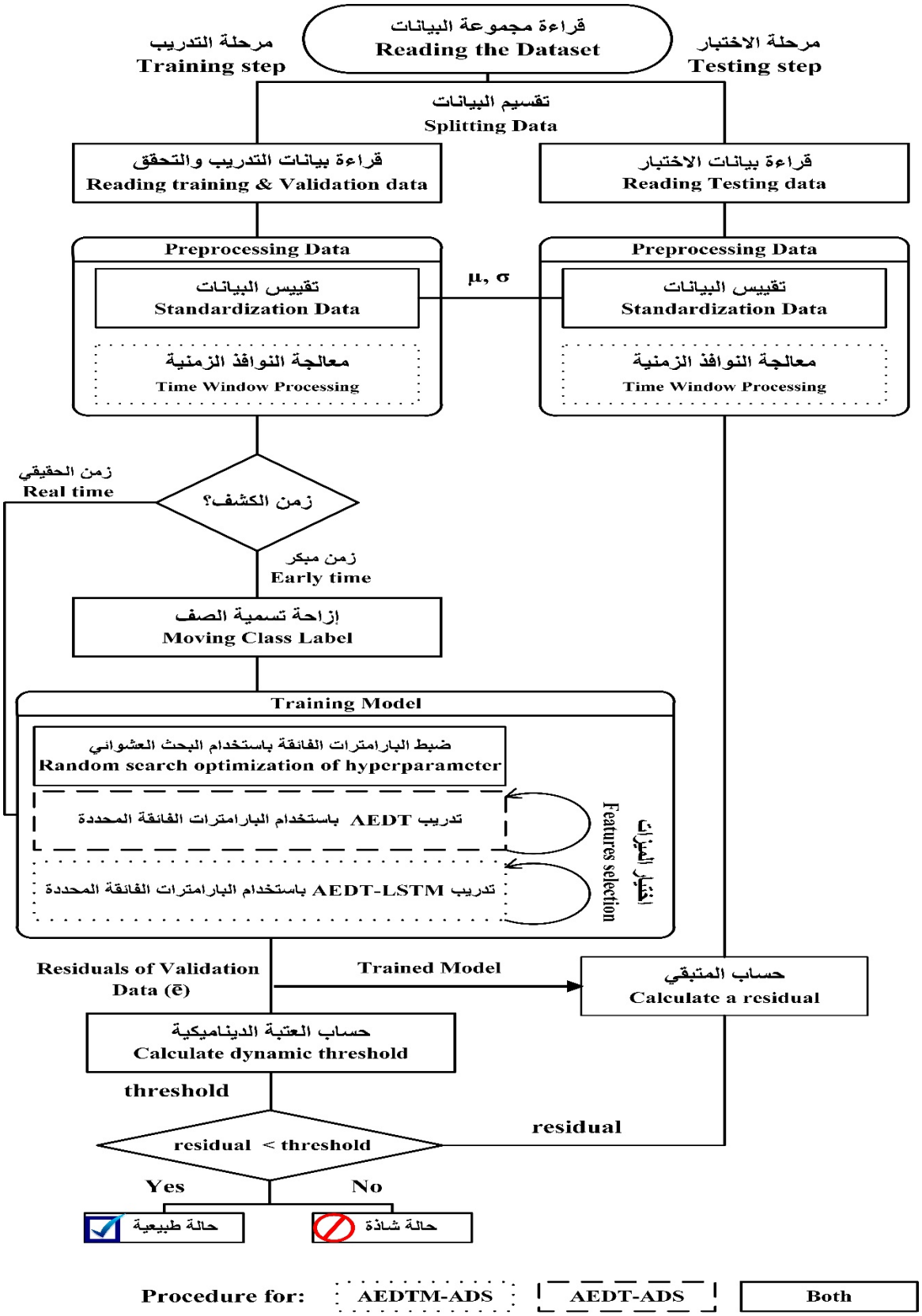
يُعرَّف المجال بالشكل الآتي $[\mu \pm k\sigma]$، حيث μ متوسط متجهة الخطأ، σ الانحراف المعياري للمتجهة، أما k فَعَددٌ صحيح أكبر من الواحد $(k > 1)$. تختلف نسبة قِيَم الخطأ التي تقع ضمن المجال المذكور حسب نوع النظرية (تشيبيشيف أو القاعدة التجريبية)، لكن من أجل $k = 3$ فإن معظم القِيَم تقع ضمن المجال.

تختار AEDT عَتَبَة تصنيف من ضمن المجال المحدد، لذلك فإن جميع قِيَم العتبات التي تقع ضمن المجال تكون مقبولة؛ لكن تختلف القيمة الافتراضية للعَتَبَة المختارة بناءً على هدف النظام. يمكن تعيين القيمة الافتراضية على الحد الأدنى للمجال (المتوسط) في حال كان الهدف الحصول على أكبر قيمة للاسترجاع (High Recall)، أو على الحد الأعلى للمجال في حال كان الهدف تحقيق توازن بين قيمتي الدقة والاسترجاع، بالإضافة إلى تقليل الإنذارات الكاذبة (Less FPR).

تستطيع بذلك شبكة AEDT المقترحة، اختيار عَتَبَة التصنيف المتغيرة بناء على طبيعة بيانات الدخل بشكل ديناميكي، ومن دون الحاجة إلى تغيير هذه القيمة على نحوٍ تجريبي، كما في شبكة الترميز الآلي التقليدية (AE). يُمكن توضيح الإجرائية المقترحة على نحوٍ أبسط من خلال **الشكل 6-1**.



الشكل 6-1 إجرائية شبكة AEDT المقترحة. المصدر: الدراسة الحالية



الشكل 6-2 نظام كشف الشذوذ المقترح. المصدر: الدراسة الحالية

6-2- النظام المقترح (Proposed System)

يوضح **الشكل 6-2** جميع الإجراءات المتبعة لبناء نظام كشف الشذوذ المقترح، بحالتيه مع ذاكرة (AEDTM-ADS) ومن دونها (AEDT-ADS). تتشابه الإجراءات المتبعة في كلتا الحالتين بمعظمها؛ لكن تتطلب عملية إضافة وحدة الذاكرة (LSTM) إلى النظام بعض الإجراءات الإضافية، وبخاصّةٍ في المعالجة المسبقة للبيانات. تَنقسم مراحل بناء النظام المقترح، كما في جميع أنظمة كشف الشذوذ الأخرى إلى مرحلة التدريب (التطوير)، ومرحلة الاختبار.

تتضمن مرحلة التدريب معظم الإجراءات، بدءاً من المعالجة المسبقة لِكُلّ من بيانات التدريب والتحقق، ومن ثم تحديد الزمن اللازم للكشف (زمن حقيقي، زمن مبكر) بناءً على ما تتطلبه الحالة الحالية للنظام، وصولاً إلى تدريب خوارزمية الكشف المقترحة (AEDT أو LSTM-AEDT). بينما تحتوي مرحلة الاختبار على إجرائيتين رئيسيتين هما: المعالجة المسبقة للبيانات، وحساب المتبقي (خطأ إعادة البناء) لبيانات الاختبار. إذ يَتِمُّ استخدام قِيَم متجهة الخطأ للبيانات الطبيعية في مجموعة التحقق من الصحة لحساب عتبة التصنيف ديناميكياً، بعد ذلك تَتُّم مقارنة العتبة مع قيم متجهة الخطأ للدخل الحالي، لتصنيف الحالات المقابلة لتلك القيم إلى طبيعية وشاذة.

بدايةً وقبل البدء ببناء نظام كشف الشذوذ المقترح، يجب تقسيم مجموعات البيانات المستخدمة إلى بيانات تدريب (Training)، واختبار (Testing)، وتحقق من الصحة (Validation). بما أن النظام المقترح، يقوم بنمذجة خصائص البيانات الطبيعية فقط في أثناء عملية التدريب، فسيتم وضع جميع العينات الشاذة ضِمْنَ بيانات الاختبار مع **20%** من البيانات الطبيعية (مجموعة الاختبار: **20%** من البيانات الطبيعية + كُلّ البيانات الشاذة)، بينما تحتوي بيانات التدريب على **80%** المتبقية من البيانات الطبيعية. تُقسم مجموعة التدريب في المرحلة الثانية، إلى مجموعة التدريب الفعلية ومجموعة التحقق من الصحة، وتكون نسبتهما **80%** و**20%** على الترتيب.

فيما يلي مراحل بناء نظام كشف الشذوذ المقترح ضمن الدراسة الحالية.

1. مرحلة التدريب (Training Step)

1. المعالجة المسبقة للبيانات (Preprocessing Data)

I. تَقيِيس البيانات (Standardization Data)

يَتِمُّ في المرحلة الأولى من المعالجة المسبقة للبيانات، تَقيِيس كُلّ من بيانات التدريب والتحقق. تُقيَّس جميع قيم الميزات لمجموعة البيانات المستخدمة، بالاعتماد على المتوسط والانحراف المعياري للميزة المحددة، كما يلي.

$$s_i = \frac{f_i - \text{mean}(f_i)}{\text{std}(f_i)}, i = 1 \dots . n \qquad (6\text{-}1)$$

s_i: قيم الميزة i بعد تَقييسها، f_i: القيم الحقيقية للميزة i.

$mean(f_i)$، $std(f_i)$: المتوسط والانحراف المعياري للقيم الحقيقية

تهدف عملية التَقييس لتوحيد (Scale) قيم الميزات، بمتوسط = 0 وانحراف معياري = 1، مما يعطي عادةً أداء أفضل للخوارزمية.

II. معالجة النوافذ الزمنية (Time Window Processing)

يتطلب النظام عند إضافة وحدة الذاكرة، استخدام مفهوم النوافذ الزمنية حتى يَتَمكَّن من التقاط التبعيات الزمنية خلال فترة معينة. ولذلك فإن هذه الإجرائية خاصة بالحالة AEDTM–ADS.

يَتضّمْنَ مثيل النافذة (Window Instance) من أجل حجم نافذة m، النقاط الزمنية المقابلة لآخر m قراءة وصولاً للوقت الحالي t. يَتُم تصنيف مثيل النافذة، بالاعتماد على تصنيف آخر نقطة زمنية في النافذة (c_t).

يُستَخدم مثيل النافذة في تدريب النموذج، بالإضافة إلى معالجة مشكلة البيانات غير المتوازنة (Imbalanced Data)، من خلال إنشاء مثيل النافذة عند جميع النقاط الزمنية المقابلة لحالة الشذوذ $(c_t = 1)$، وبعض النقاط الزمنية المقابلة للحالة الطبيعية $(c_t = 0)$، مما يُقْلَص الفرق بين صفوف البيانات. يَتِمُّ تمثيل مثيلات النافذة وتسميات الحالات المقابلة بالشكل الآتي:

$$(w, c) = \begin{bmatrix} w_{1,1} & w_{1,2} & \dots & w_{1,p} & c1 \\ w_{2,1} & w_{2,2} & \dots & w_{2,p} & c2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ w_{n,1} & w_{n,2} & \dots & w_{n,p} & cn \end{bmatrix} \qquad (6\text{-}2)$$

n: رقم النافذة الزمنية، p: ترتيب الميزة

$w_{n,p}$: تسلسل بطول m لقيم الميزة p

cn: تسمية مثيل النافذة n

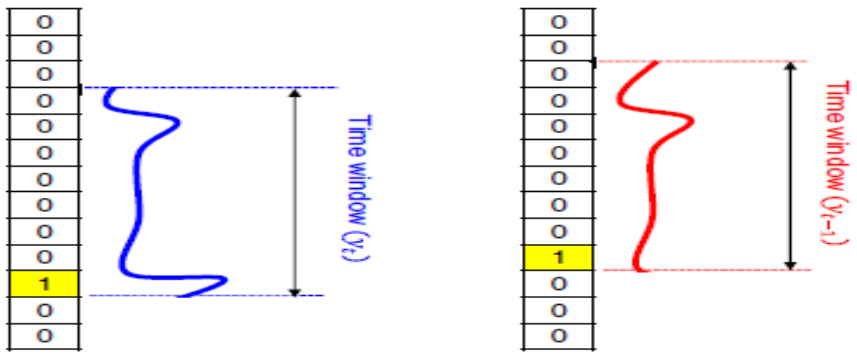
يَتِمُّ استخدام مجموعة بيانات التدريب والتحقق من الصحة بعد معالجتها باستخدام النوافذ الزمنية في تدريب النظام المقترح (AEDTM–ADS).

2. زمن الكشف (Detection Time)

تتطلب بعض التطبيقات من النظام، أن يقوم بالكشف عن الشذوذ ضمن تسلسلات البيانات قبل حدوثها بوقت مناسب. ومن ثَمَّ يقتضي ذلك معالجة إضافية للبيانات، تَتَمَثَّل أحد الأساليب لتحقيق ذلك بإزاحة تصنيف النقطة الزمنية المقابلة لحالة الشذوذ إلى الأعلى بمقدار s، بحيث تكون المصنفات قادرة على التنبؤ بحالة النظام الحالية (c_t) قبل s وحدة زمنية.

$$c_t \leftarrow c_{t+s}, \text{where } s = 1,2, \ldots \quad (6\text{-}3)$$

يوضح **الشكل 6-3** عملية إزاحة تسمية الصف إلى الأعلى بمقدار سطر واحد.



الشكل 6-3 الكشف المبكر بإزاحة نقطة البيانات إلى الأعلى بمقدار 1

3. تدريب النموذج (Training Model)

يتضمن تدريب النموذج مجموعة من الإجراءات الهامة هي، ضبط البارامترات الفائقة وقياس أهمية الميزات في عملية التدريب، ومن ثم تدريب خوارزمية الكشف (AEDT أو LSTM-AEDT) باستخدام قِيَم البارامترات الفائقة والميزات الأكثر أهمية المحددة.

I. ضبط البارامترات الفائقة (Hyperparameters Tuning)

تعتمد الدراسة الحالية لضبط قِيَم البارامترات الفائقة لخوارزميات الكشف المقترحة على تقنية البحث العشوائي. تَمَّ تدريب الخوارزميات باستخدام عدد من التكوينات المرشحة للبارامترات الفائقة الخاصة بالشبكات العصبونية، والمشار إليها في الفصل الثاني من هذه الأطروحة، حيث وصل عددها من أجل خوارزمية AEDT إلى **48,000** تكوينة مرشحة، وفي خوارزمية LSTM-AEDT إلى **36,000** تكوينة مرشحة.

يوضح **الجدول 6-1** مجال القِيَم للبارامترات الفائقة لخوارزمية AEDT ضمن هذه الدراسة، ولِكُلّ من مجموعتي البيانات المستخدمة.

الجدول 6-1 مجال قيم البارامترات الفائقة لخوارزمية AEDT

Hyperparameters	Type		Range		Range
Activation Function	Categorical	European Dataset	Sigmoid, Tanh, Relu, Linear	Paper Break Dataset	Sigmoid, Tanh, Relu, Linea
Learning Rate	Real		$[1e-4, 1e-1]$		$[1e-4, 1e-1]$
Batch Size	Integer		[30,256]		[32,256]
Dropout Rate	Real		[0,1]		[0,1]
Epoch	Integer		[50,100]		[50,250]
Nodes	Integer		[8,20]		[8,32]

يوضح **الجدول 6-2** مجال القِيَم للبارامترات الفائقة لخوارزمية LSTM-AEDT ضمن الدراسة الحالية، ولِكُلّ من مجموعتي البيانات المستخدمة.

الجدول 6-2 مجال قيم البارامترات الفائقة لخوارزمية LSTM-AEDT

Hyperparameters	Type		Range		Range
Activation Function	Categorical	European Dataset	Sigmoid, Tanh, Relu	Paper Break Dataset	Sigmoid, Tanh, Relu
Learning Rate	Real		$[1e-4, 1e-1]$		$[1e-4, 1e-1]$
Batch Size	Integer		[30,256]		[32,256]
Dropout Rate	Real		[0,1]		[0,1]
Epoch	Integer		[25,75]		[50,250]
Nodes	Integer		[10,100]		[8,32]

II. أهمية الميزات (Features Importance)

تعتمد الدراسة لقياس أهمية الميزات، على مقياس الحجم (Magnitude Measure) [61]، إذ يَتِمُّ قياس مقدار مساهمة عصبونات الدخل في أوزان عصبونات الخرج بعد عملية التدريب.

يَتِمُّ في المرحلة الأولى حساب مساهمة أحد عصبونات الدخل في وزن أحد عصبونات الطبقة المخفية، وفق القانون الآتي:

$$P_{ij} = \frac{|w_{ij}|}{\sum_{p=1}^{ni} |w_{pj}|} \qquad (6\text{-}4)$$

w_{ij}: الوزن بين عصبون الدخل الحالي i والعصبون المخفي j

w_{pj}: الوزن بين كل عصبون دخل p والعصبون المخفي j

بينما يَتِمُّ في المرحلة الثانية وبالآلية نفسها حساب مساهمة أحد عصبونات الطبقة المخفية في وزن أحد عصبونات طبقة الخرج.

$$P_{jk} = \frac{|w_{jk}|}{\sum_{r=1}^{nh} |w_{rk}|} \qquad (6\text{-}5)$$

في نهاية المطاف، يكون مقدار مساهمة عصبون دخل في وزن عصبون خرج بالشكل الآتي:

$$Q_{ik} = \sum_{r=1}^{nh} (P_{ir} * P_{rk}) \qquad (6\text{-}6)$$

P_{ir}: مساهمة عصبون الدخل i في العصبون المخفي r

P_{rk}: مساهمة العصبون المخفي r في عصبون الخرج k

تتكرر المراحل السابقة من أجل كل عصبونات الشبكة، للحصول على مصفوفة حجوم أوزان مساهمة كل عصبون دخل في عصبونات طبقة الخرج.

III. تدريب الخوارزمية المقترحة

يَهدُف تدريب خوارزميات الكشف المقترحة على نمذجة خصائص البيانات الطبيعية، من خلال تغذية دخلها بالبيانات الطبيعية فقط في أثناء عملية التدريب. كما يعتمد تدريبها على البارامترات الفائقة المحددة، إذ تَنْتَقي الخوارزمية خلال التدريب، قِيَم البارامترات التي تُسهِم في تقليص خسارة الشبكة، والذي يمثل متوسط الخطأ التربيعي كالآتي:

$$l = \frac{1}{n} \sum_{i=1}^{n} (x_i - \hat{x}_i)^2 \qquad (6\text{-}7)$$

---

x: شعاع الدخل، $\hat{x}$: شعاع الخرج المتوقع

n: حجم بيانات الدخل

3. حساب العَتَبَة الديناميكية (Calculate Dynamic Threshold)

تَمرّ عملية حساب عَتَبَة التنصيف T ديناميكياً بمرحلتين رئيسيتن، كما في **الشكل 6-1**. يَتِمُّ في المرحلة الأولى، تحديد نوع التوزيع لقِيَم متجهة الخطأ $\vec{e}$ للبيانات الطبيعية ضمن بيانات التحقق من الصحة باستخدام اختبار كولموغوروف سميرنوف، إذ يَتِمُّ الاختبار على مجموعة واسعة من التوزيعات المحتملة. بينما يَتِمُّ في المرحلة الثانية تطبيق أحد النظريتين القاعدة التجريبية أو نظرية تشيبيشيف، وذلك لتحديد المجال الذي يقع ضمنه معظم قِيَم المتجهة. **راجع الفصل الثالث للتذكير بنص النظريتين.**

- **مرحلة الاختبار (Testing Step)**

1. المعالجة المسبقة للبيانات

تَتِمُّ المعالجة المسبقة لبيانات الاختبار بالآلية نفسها المتبعة في بيانات التدريب؛ لكن تَقيِيس بيانات الاختبار باستخدام المتوسط (μ) والانحراف المعياري (σ) لبيانات التدريب بعد تَقيِيسها، مما يُبقِّي بيانات الاختبار غير معروفة أثناء النمذجة.

2. حساب البواقي (Calculate Residuals)

يعتمد حساب البواقي (خطأ إعادة البناء) للبيانات بعد تمريرها إلى النموذج المدرب، على متوسط الخطأ التربيعي (MSE)، فتكون قيمة الخطأ للشعاع الدخل الحالي i بالشكل الآتي:

$$e_i = \frac{1}{n}(x_i - \hat{x}_i)^2 \qquad (6\text{-}8)$$

---

x_i: شعاع الدخل ، $\hat{x}_i$: شعاع الخرج المتوقع

n: بُعد البيانات (عدد الميزات)

- **كشف الشذوذ (Anomaly Detection)**

يَتِمُّ في المرحلة الأخيرة من النظام تصنيف حالة الدخل c (طبيعية أو شاذة)، من خلال مقارنة قيمة الخطأ e لشعاع الدخل الحالي بقيمة العَتَبَة الديناميكية T كالآتي:

$$c \rightarrow \text{normal} \ \text{ if } e \leq T \qquad (6\text{-}9)$$

$$c \rightarrow \text{anomaly if } e > T \qquad (6\text{-}10)$$

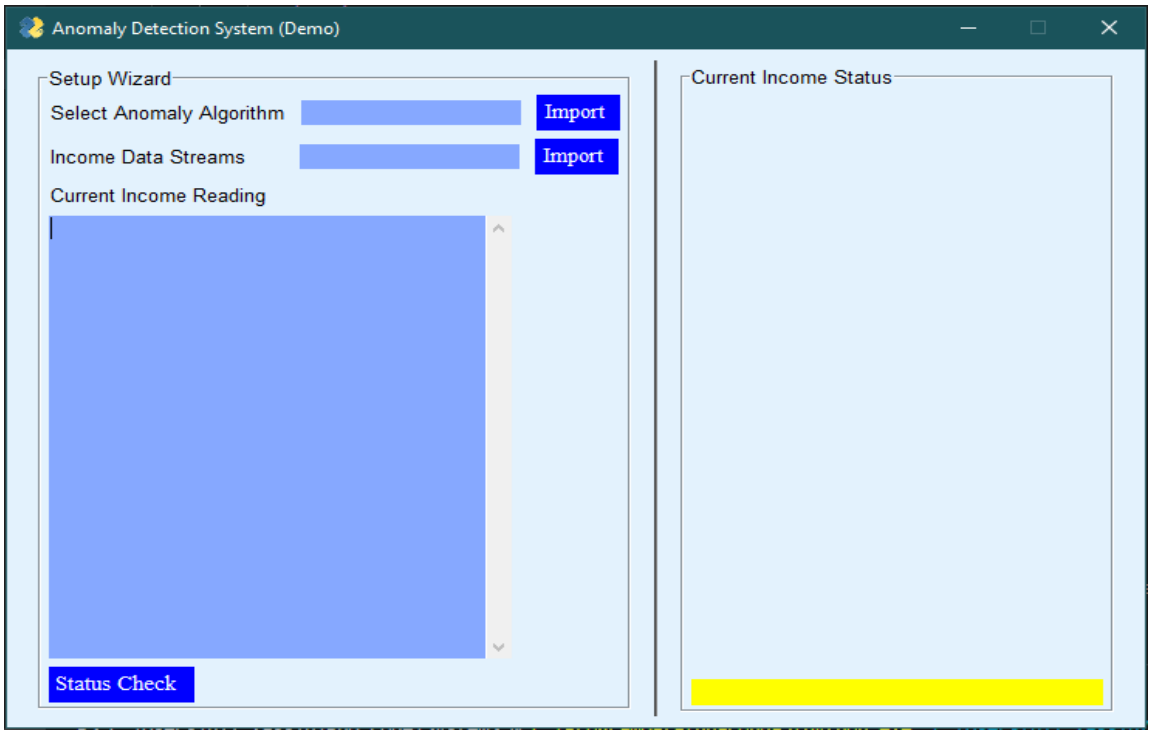
يظهر بوضوح من خلال المعادلتين (6-9) و (6-10) ، أنه يتم تصنيف جميع الحالات التي لها خطأ أكبر من العَتَبَة على أنها حالات شاذة. أما فيما عدا ذلك، فتُصنف على أنها حالات طبيعية.

6-3- واجهة النظام (System GUI)

تَمَّ تطوير واجهة تخاطبية مبسطة للنظام، باستخدام لغة بايثون (Python). تهدف الواجهة إلى تبيان إمكانية استثمار النظام المقترح مباشرةً في أي تطبيق من تطبيقات العالم الحقيقي بعد ملاءَمَته ليناسب البيانات المدخلة. وفيما يلي عرض لواجهة النظام المقترح.

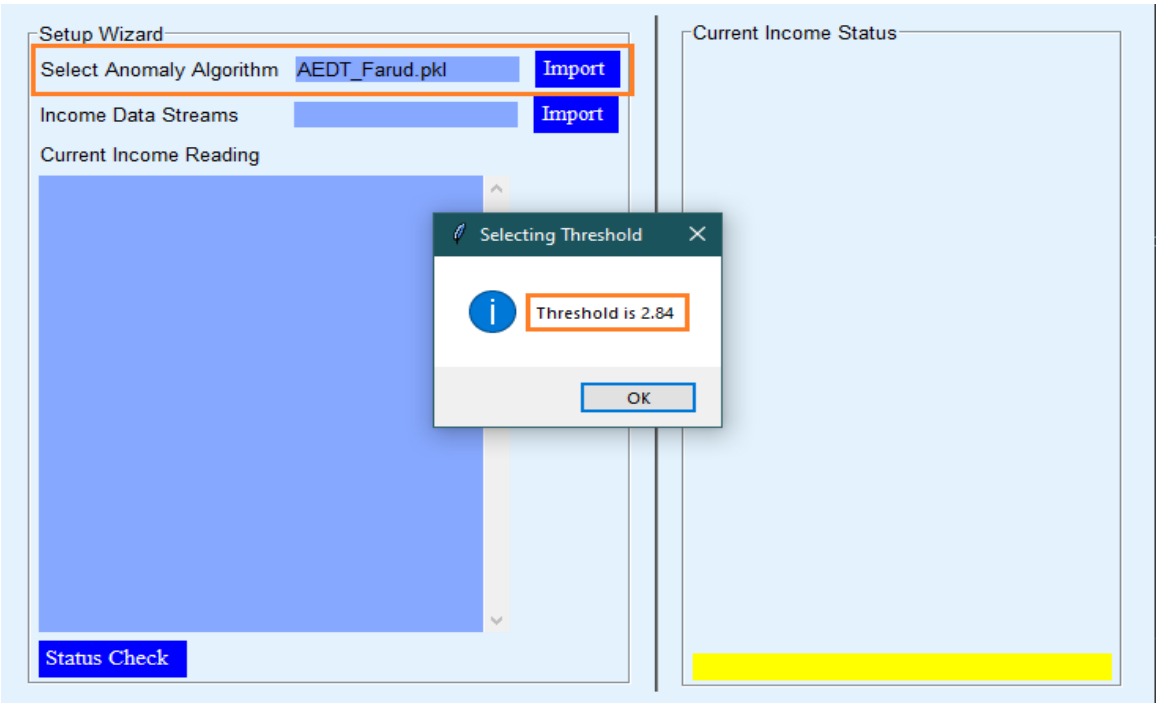
- **واجهة النظام الرئيسية**

تتكون الواجهة الرئيسية من قسمين هما: إعدادات النظام (Setup Wizard)، وحالة الدخل الحالي (Current Income Status).



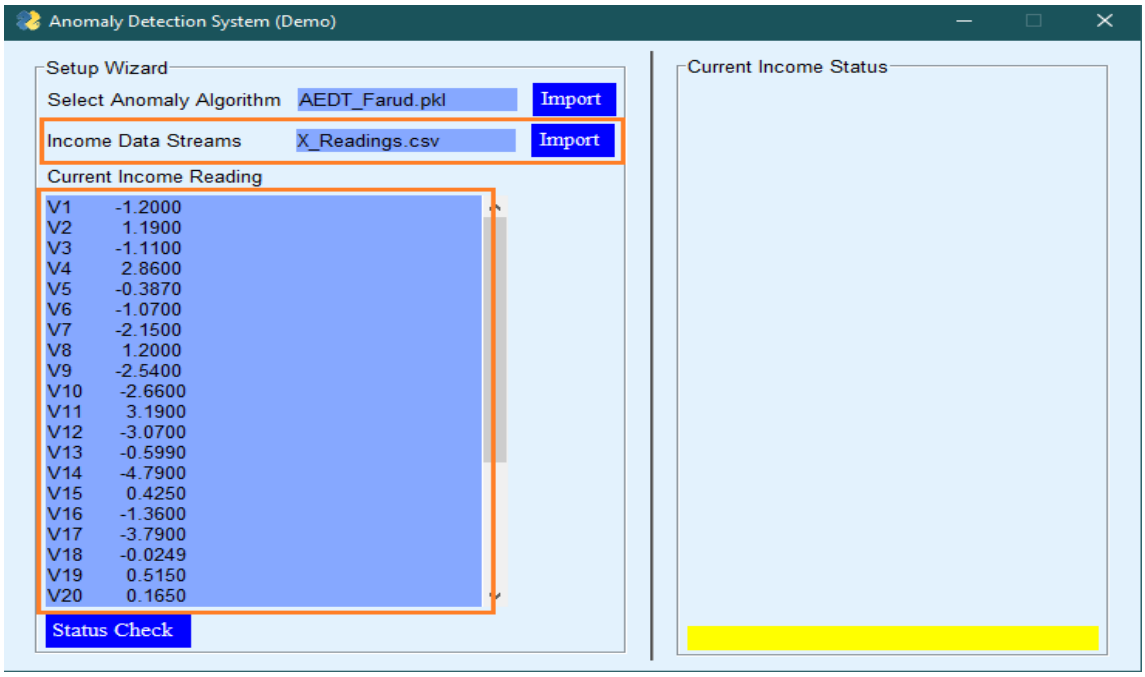
الشكل 6-4 الواجهة الرئيسية لنظام كشف الشذوذ المقترح

بدايةً يتم ضبط الإعدادات من خلال تحديد نوع خوارزمية الكشف (LSTM-AEDT أو AEDT)، ليعيد النظام بعد ذلك قيمة عَتَبَة التصنيف ديناميكياً.

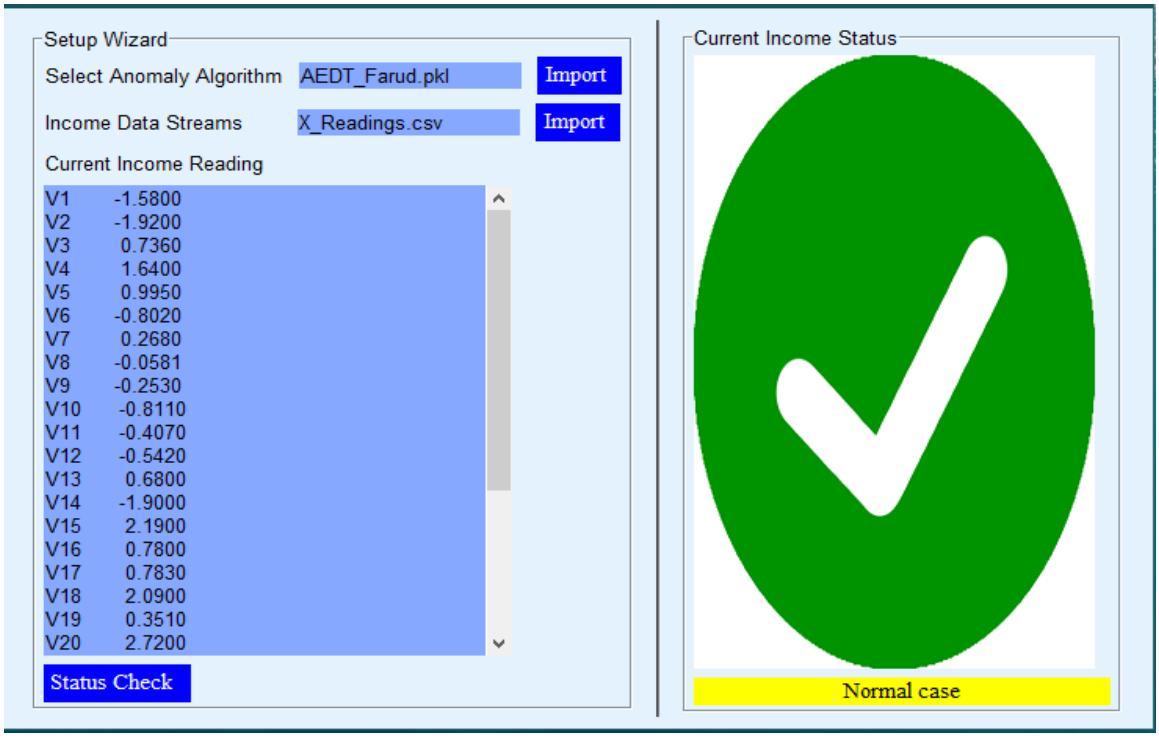


الشكل 6-5 ضبط إعدادات النظام- تحديد خوارزمية الكشف

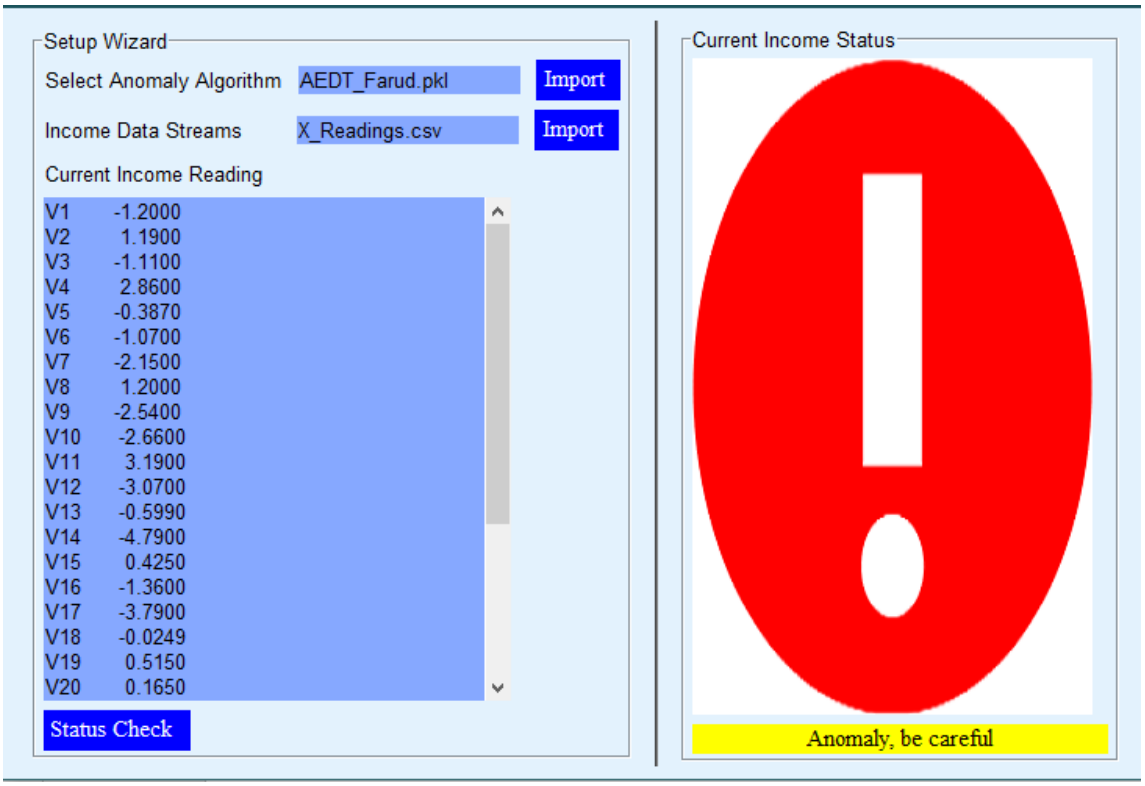
يَتُم في المرحلة الثانية استيراد تدفقات البيانات الحالية، من أجل تحديد الحالات المراد فحصها ومن ثم تحديد حالة الدخل الحالية (شذوذ وطبيعية).



الشكل 6-6 ضبط إعدادات النظام- استيراد تدفقات البيانات الحالية



الشكل 6-7 تحديد حالة الدخل الحالي- حالة طبيعية



الشكل 6-8 تحديد حالة الدخل الحالي- حالة شاذة

إن نتائج اختبار النظام المقترح على الحالتين الموضحتين ضمن **الشكل 6-7** و**الشكل 6-8** هي نتائج صحيحة ومتطابقة، مما يؤكد فعالية عمل النظام.

الفصل السابع

النتائج والمناقشة

يتضمن الفصل الحالي عرض النتائج وتقييم الأداء لجميع التجارب التي أجرتها الدراسة، والمشار إليها في الفصلين السابقين الخامس والسادس. بدءاً من تحليل الأنظمة الكلاسيكية لكشف الشُّذُوذ، وصولاً إلى اختبار نظام كشف الشُّذُوذ الْمُقْتَرَح بحالتيه (AEDT–ADS، AEDTM–ADS).

7–1– تحليل أنظمة كشف الشُّذُوذ الكلاسيكية

ستُعرَضُ نَتَائِجُ تحليل أداء الأنظمة الكلاسيكية لكشف الشُّذُوذ وفق منهجية التحليل الْمُقْتَرَحة في **الشكل 5–1** ضمن الفصل الخامس من هذه الأطروحة، باستخدام خوارزميتي الغابات العشوائية (RF) وآلة شعاع الدعم (SVM).

7–1–1– تحليل أداء خوارزمية الغابات العشوائية في اكتشاف الشُّذُوذ

فيما يلي نتائج أداء خوارزمية الغابات العشوائية (RF) في اكتشاف الشُّذُوذ وفق السيناريوهين الْمُقْتَرَحين، وبالاعتماد على مجموعتي البيانات المستخدمة (الاحتيال الأوروبية، الاحتيال المجردة).

- **مجموعة الاحتيال الأوروبية**

I. السيناريو الأول (Scenario 1)

1. ضبط البارامترات الفائقة (Hyperparameters Tuning)

يُبَيِّن **الجدول 7–1** نتائج ضبط البارامترات الفائقة باستخدام تقنية البحث العشوائي، بينما يظهر أداء الخوارزمية في **الجدول 7–2** باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المستخدمة.

الجدول 7–1 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الأول (البيانات الأوروبية)

البارامترات الفائقة	القيمة
الحد الأعظمي لعمق الشجرة	150
الحد الأدنى للعينات المطلوبة للتقسيم	10
عدد الأشجار	100
العدد الأعظمي للعينات	$RoundUp(\sqrt{\#features\ of\ data})$
الحد الأدنى للعينات ضمن الأوراق	5
Bootstrap	False

الجدول 7−1 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات الأوروبية – السيناريو الأول

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.87	0.85	0.86	0.85	0.84	0.46	0.046

يوضح الجدول السابق أداء نموذج الغابات العشوائية في المرحلة الأولى من السيناريو الأول، إذ وصلت قيمة MCC إلى **85%**، وقيمة AUCPR **إلى 84%**، مع معدل إيجابيات خاطئة **46%** ($FPR = 0.46$). بالتالي فإن للغابة أداء جيد في اكتشاف الحالات الشاذة.

2. اختيار الميزات (Features Selection)

يُبَيِّن **الجدول 7−3** أداء الخوارزمية عند تدريبها باستخدام مبدأ التصفية (Filter) للميزات، وفقاً لترتيب أهميتها النسبية (Relative Importance) في **الجدول 5−1** ضمن الفصل الخامس، إذ تَمَّ تدريبها من خلال زيادة عدد الميزات، بدءاً من الميزة الأكثر أهمية وصولاً إلى الميزة التي لا يحدث بعدها أي تحسين في أداء الخوارزمية. مع العِلم أن الخوارزمية تَعتَمِدُ في هذه المرحلة على قيم البارامترات الفائقة المحددة من الخطوة السابقة.

الجدول 7−2 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الأول

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.27	0.74	0.39	0.44	0.88	0.53	0.364
2	0.61	0.76	0.67	0.68	0.67	0.72	0.117
3	0.82	0.83	0.83	0.83	0.51	0.82	0.055
4	0.82	0.83	0.82	0.82	0.52	0.84	0.056
5	**0.87**	**0.88**	**0.87**	**0.87**	**0.51**	**0.86**	**0.041**
6	0.87	0.86	0.86	0.86	0.48	0.86	0.043
7	0.86	0.85	0.86	0.85	0.46	0.86	0.046

يظهر بوضوح من خلال الجدول السابق، أن نموذج الغابات العشوائية، يُحقِّق أفضل نتيجة له في المرحلة الثانية من السيناريو الأول، عند استخدام توليفة من قيم البارامترات الفائقة المحددة من المرحلة الأولى وأهم **5** ميزات وهي: (V14, V4, V10, V12, V17) وفقاً لترتيب أهميتها، حيث تصل قيمة AUCPR إلى **86%** وقيمة MCC إلى **87%**، وبزيادة **2%** عن قيم المرحلة الأولى للسيناريو الأول. وتقابل تلك القيم أقل قيمة لنسبة الفشل ($Failure\ rate\ = 0.041$)، مع قيم عالية أيضاً لباقي

المقاييس التي تعبر عن اكتشاف الشُّذُوذ. لكن بالمقابل يزداد معدل الإيجابيات الخاطئة من **46%** إلى **51%**. لذلك إن النموذج مع تصنيفه لمعظم الحالات الشاذة (الاحتيالية) على نحوٍ صحيح عند اتباعه لخطوات السيناريو الأول، يصل معدل الإيجابيات الخاطئة إلى **51%** وهذا مؤشر غير جيد في أنظمة كشف الاحتيال المالي بسبب أمور تتعلق بسياسة الشركات المالية. كما بلغ الزمن اللازم لتدريب (بناء) النظام في هذا السيناريو **31.23** دقيقة.

II. السيناريو الثاني (Scenario 2)

1. اختيار الميزات

يُبَيِّن **الجدول 7–4** أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم الميزات.

الجدول 7–3 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.46	0.52	0.49	0.49	0.55	0.52	0.172
2	0.86	0.65	0.74	0.75	0.22	0.73	0.071
3	0.92	0.80	0.86	0.86	0.25	0.84	0.042
4	0.93	0.83	0.86	0.86	0.22	0.85	0.041
5	0.94	0.79	0.86	0.86	0.20	0.85	0.041
6	**0.96**	**0.80**	**0.87**	**0.88**	**0.16**	**0.85**	**0.037**
7	0.95	0.78	0.85	0.86	0.16	0.85	0.042

أظهرت نتائج المرحلة الحالية المبينة في الجدول السابق، أن أفضل أداء لنموذج الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم الميزات، يكون عند اختيار أهم **6** ميزات ضمن البيانات المستخدمة وفقاً لترتيبها في **الجدول 5–1** وهي: (V14, V4, V10, V12, V17,V3)، إذ بلغت قيمة AUCPR **85%** وقيمة MCC **88%**، مع قيم عالية أيضاً لباقي المقاييس، وبمعدل إيجابيات خاطئة مقبول **16%**، وذلك عندما تكون قيمة نسبة الفشل $Failure\ rate = 0.037$ أقل ما يمكن.

2. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 5–7** نتائج ضبط البارامترات الفائقة لخوارزمية الغابات العشوائية باستخدام تقنية البحث العشوائي، مع العِلم أن البحث العشوائي ضمن السيناريو الثاني، يعتمد في أثناء عملية ضبط البارامترات الفائقة على أهم الميزات المحددة من الخطوة السابقة. بينما يُبَيِّن **الجدول 7–6** أداء الخوارزمية

باستخدام توليفة من أفضل قيم البارامترات الفائقة المحددة في المرحلة الحالية وأهم الميزات المحددة من المرحلة السابقة.

الجدول 7−4 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الثاني (البيانات الأوروبية)

البارامترات الفائقة	Value
الحد الأعظمي لعمق الشجرة	150
الحد الأدنى للعينات المطلوبة للتقسيم	2
عدد الأشجار	250
العدد الأعظمي للعينات	$RoundUp(\sqrt{\#\ selected\ features})$
الحد الأدنى للعينات ضمن الأوراق	1
Bootstrap	True

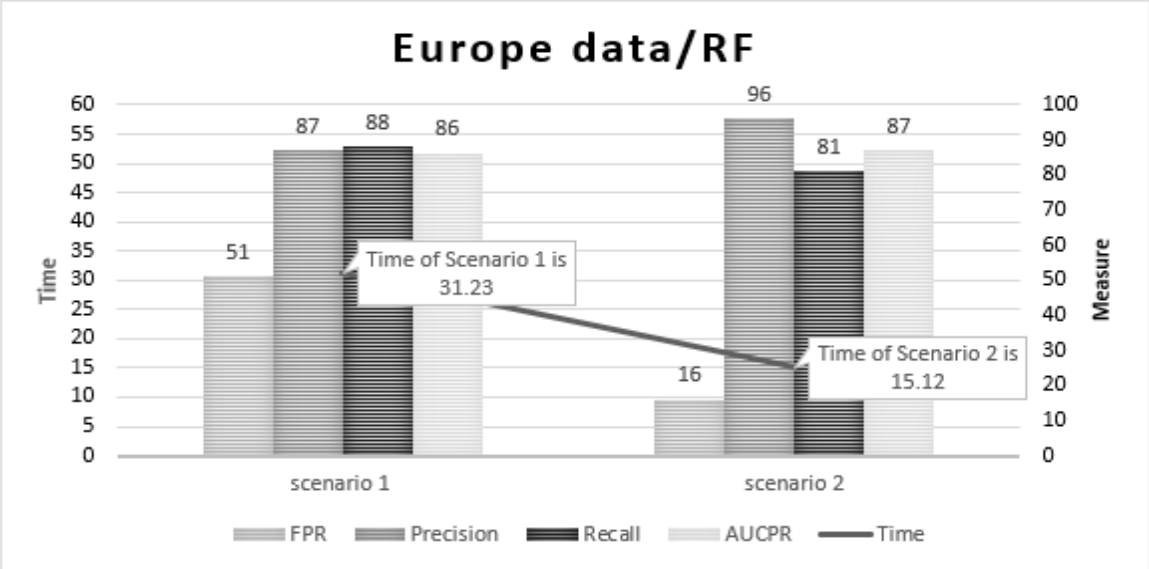
الجدول 7−5 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.96	0.81	0.88	0.88	0.87	0.16	0.036

أظهرت النتائج المبينة في الجدول السابق تحسيناً بسيطاً في أداء الخوارزمية بالنسبة لقيمة AUCPR حيث بلغت قيمتهُ **87%**، وانخفاضاً في نسبة الفشل $(Failure\ rate = 0.036)$ مقارنة بالمرحلة الأولى من هذا السيناريو؛ بالمقابل لم يحدث تغيير في معدل الإيجابيات الخاطئة وبقيت **16%**. بلغَ الزمن اللازم لبناء النظام في هذا السيناريو **15.12** دقيقة (أقل بحوالي 16 دقيقة عن السيناريو السابق). لذلك إن بناء النموذج وفقاً للسيناريو الثاني، يُقلص من زمن البناء بنسبة **51.5%**، ومن معدل الإيجابيات الخاطئة بنسبة **35%** عما هو عليه في السيناريو الأول، بالإضافة إلى تحسين معظم قيم المقاييس الأخرى.

يوضح **الشكل 7−1** مقارنة بين السيناريوهين الْمُقْتَرَحين لبناء نظام كشف الشُّذُوذ باستخدام الغابات العشوائية، وذلك عند تطبيقه على مجموعة الاحتيال الأوروبية. يظهر بوضوح تفوق السيناريو الثاني من خلال تقليص الزمن المستغرق لبناء (تدريب) النظام بنسبة **51.5%** (حوالي 16د، من 31د إلى 15د)، بالإضافة إلى انخفاض كبير في معدل الإيجابيات الخاطئة (FPR) بنسبة **35%** (من 51% إلى 16%)، حيث يعد ذلك من أهم الأهداف التي يسعى إليها أيُّ نظام كشف شُذُوذ. ومن جهة أخرى تنخفض قيمة الاسترجاع (Recall) بنسبة **7%** (من 88% إلى 81%)؛ لكن بالمقابل يوجد تحسين كبير جداً في

مقياس الدقة (Precision) بنسبة 11% (من87% إلى 96%)، وهذا مؤشر جيد للغاية في أنظمة كشف الشَذُوذ وبخاصّةٍ المتعلقة بالمؤسسات والشركات المالية.



الشكل 7-1 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام الغابات العشوائية وفق لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات الأوروبية)

- **مجموعة الاحتيال المجردة**

I. السيناريو الأول (Scenario 1)

1. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-7** نتائج ضبط البارامترات الفائقة باستخدام البحث العشوائي. بينما يظهر أداء الخوارزمية في **الجدول 7-8** باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المستخدمة.

الجدول 7-6 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الأول (البيانات المجردة)

البارامترات الفائقة	القيمة
الحد الأعظمي لعمق الشجرة	50
الحد الأدنى للعينات المطلوبة للتقسيم	5
عدد الأشجار	50
العدد الأعظمي للعينات	$RoundUp(\sqrt{\#\ featuers\ of\ data})$
الحد الأدنى للعينات ضمن الأوراق	1
Bootstrap	True

الجدول 7–7 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المجردة – السيناريو الأول

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.78	0.79	0.79	0.74	0.86	0.54	7.059

يوضح الجدول السابق أداء الخوارزمية في المرحلة الأولى من السيناريو الأول، إذ بلغت قيمة MCC **74%**، وقيمة AUCPR **86%**، مع معدل إيجابيات خاطئة **54%** ($FPR = 0.54$). ولذلك فإن للغابة في هذه المرحلة أداء مقبول في اكتشاف الحالات الشاذة.

2. اختيار الميزات

يُبَيِّن **الجدول 7–9** أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم الميزات.

الجدول 7–8 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الأول

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.54	0.68	0.60	0.52	0.64	0.66	14.518
2	0.63	0.68	0.65	0.58	0.56	0.75	11.701
3	0.68	0.75	0.71	0.65	0.58	0.81	9.859
4	**0.78**	**0.79**	**0.79**	**0.75**	**0.52**	**0.87**	**6.934**
5	0.70	0.71	0.71	0.73	0.54	0.84	7.123

يظهر بوضوح من خلال الجدول السابق، أن نموذج الغابة العشوائية، يحقق أفضل نتيجة له في السيناريو الأول، عند استخدام توليفة من قيم البارامترات الفائقة المحددة من المرحلة السابقة وأهم **4** ميزات وهي: **عدد حالات الرفض خلال اليوم الواحد، كميلة المناقلة، هل المناقلة أجنبية؟ هل البلد مصنف على أنه ضمن البلدان ذات الخطورة العالية؟** وذلك وفقاً لترتيب أهميتها ضمن **الجدول 2–5**. إذ تصل قيمة AUCPR إلى **87%** وقيمة MCC إلى **75%**، مع معدل إيجابيات خاطئة مرتفع **52%**، وتقابل تلك القيم أقل قيمة لنسبة الفشل ($Failure\ rate\ = 6.934$)، لذلك يوجد تحسين في أداء النموذج مقارنةً بالمرحلة الأولى من هذا السيناريو بنسب تتراوح بين **1%** و**2%** لمعظم المقاييس. بينما بلغ الزمن اللازم لبناء النظام في هذا السيناريو ثلاث دقائق (**3** دقيقة).

II. السيناريو الثاني (Scenario 2)

1. اختيار الميزات

يُبَيِّن **الجدول 7-10** أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم الميزات.

الجدول 7-9 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.54	0.68	0.60	0.52	0.64	0.66	14.518
2	0.63	0.63	0.63	0.55	0.50	0.74	12.134
3	0.71	0.75	0.73	0.67	0.55	0.80	9.101
4	**0.81**	**0.79**	**0.80**	**0.76**	**0.46**	**0.87**	**6.392**
5	0.78	0.79	0.79	0.73	0.52	0.84	7.010

أظهرت نتائج المرحلة الحالية المبينة في الجدول السابق، أن أفضل أداء لنموذج الغابات العشوائية باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم الميزات، يكون عند اختيار أهم **4** ميزات آنفة الذكر ضمن مجموعة البيانات المستخدمة وفقاً لترتيبها في **الجدول 2-5**، إذ بلغت قيمة AUCPR **87%** وقيمة MCC **76%**، مع معدل إيجابيات خاطئة مرتفع نسبياً **46%** $(FPR = 0.46)$، وذلك عندما تكون نسبة الفشل أقل ما يمكن $(Failure\ rate = 6.392)$.

2. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-11** نتائج ضبط البارامترات الفائقة لخوارزمية الغابات العشوائية باستخدام تقنية البحث العشوائي. بينما يُبَيِّن **الجدول 7-12** أداء الخوارزمية باستخدام توليفة من أفضل قيم البارامترات الفائقة المحددة في المرحلة الحالية وأهم الميزات المحددة من المرحلة السابقة.

الجدول 7-10 نتائج البحث العشوائي لبارامترات الغابات العشوائية – السيناريو الثاني (البيانات المجردة)

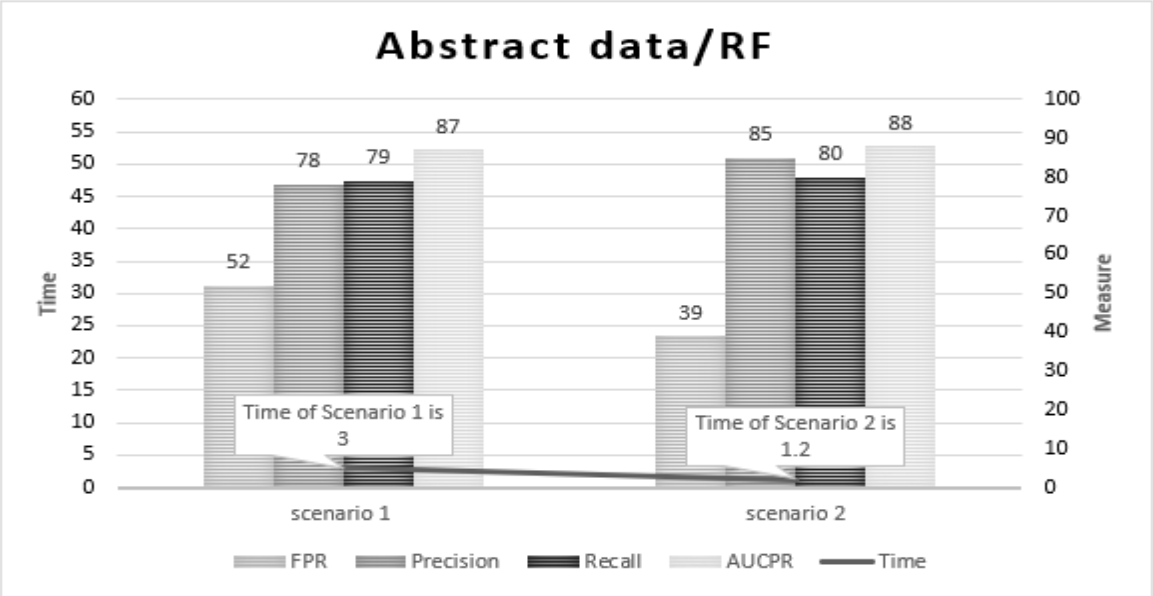
البارامترات الفائقة	القيمة
الحد الأعظمي لعمق الشجرة	10
الحد الأدنى للعينات المطلوبة للتقسيم	5
عدد الأشجار	100
العدد الأعظمي للعينات	$RoundUp(\sqrt{\#\ selected\ features})$
الحد الأدنى للعينات ضمن الأوراق	1
Bootstrap	True

الجدول 7−11 نتائج أداء خوارزمية الغابات العشوائية باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.85	0.80	0.83	0.80	0.88	0.39	5.309

أظهرت النتائج المبينة في الجدول السابق تحسين في أداء الخوارزمية بالنسبة لكل من AUCPR وMCC حيث بلغت قيمتهُم **88%** و**80%** على الترتيب، بالإضافة لانخفاض كل من معدل الإيجابيات الخاطئة إلى **39%** $(FPR = 0.39)$، ونسبة الفشل إلى $(Failure\ rate = 5.309)$ مقارنة بالمرحلة الأولى للسيناريو الثاني. كما بلغَ الزمن اللازم لبناء النظام **1.2** دقيقة. لذلك إن بناء النموذج وفقاً للسيناريو الثاني، يقلص من زمن البناء بنسبة **60%** (من 3د إلى 1.2د)، ومن معدل الإيجابيات الخاطئة بنسبة **13%** (من 52% إلى 39%) عما هو عليه في السيناريو الأول، بالإضافة لتحسين معظم قيم المقاييس الأخرى.

يظهر بوضوح في **الشكل 7−2** تفوق السيناريو الثاني لنموذج الغابات العشوائية، عند تطبيقه على مجموعة البيانات المجردة، من خلال تقليص الزمن المستغرق لبناء النظام بنسبة **60%**، بالإضافة لانخفاض كبير في معدل الإيجابيات الخاطئة (FPR) بنسبة **13%**، كما يوجد تحسين في جميع مقاييس الأداء بنسب تتراوح بين **1%** و**5%**.



الشكل 7−2 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام الغابات العشوائية وفق لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات المجردة)

7-1-2- تحليل أداء خوارزمية آلة شعاع الدعم في اكتشاف الشُّذُوذ

فيما يلي نتائج أداء خوارزمية آلة شعاع الدعم (SVM) في اكتشاف الشُّذُوذ وفق السيناريوهين الْمُقْتَرَحين، وبالاعتماد على مجموعتي البيانات المستخدمة (الاحتيال الأوروبية، الاحتيال المجردة).

- **مجموعة الاحتيال الأوربية**

I. السيناريو الأول (Scenario 1)

1. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-13** نتائج ضبط البارامترات الفائقة باستخدام تقنية البحث العشوائي، بينما يظهر أداء الخوارزمية في **الجدول 7-14** باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المستخدمة.

الجدول 7-12 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الأول (البيانات الأوروبية)

البارامترات الفائقة	القيمة
التنظيم	3000.0
Gamma	1e-3
النواة	rbf

الجدول 7-13 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات الأوروبية – السيناريو الأول

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.79	0.82	0.81	0.81	0.77	0.55	0.063

يَبْرُز من خلال النتائج الموضحة أعلاه ضمن الجدول السابق، أداء جيد لآلة شعاع الدعم في اكتشاف الحالات الشاذة ضمن المرحلة الأولى من السيناريو الأول، إذ وصلت قيمة MCC إلى **81%**، وقيمة AUCPR **إلى 77%**، وبمعدل إيجابيات خاطئة مرتفع **55%** ($FPR = 0.55$).

2. اختيار الميزات

يُبَيِّن **الجدول 7-15** أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم الميزات.

الجدول 7-14 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الأول

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.79	0.36	0.49	0.53	0.13	0.61	0.117
2	0.74	0.40	0.52	0.55	0.19	0.67	0.117
3	0.84	0.57	0.68	0.69	0.20	0.73	0.087
4	0.85	0.62	0.71	0.72	0.22	0.76	0.078
5	0.85	0.76	0.81	0.81	0.37	0.76	0.059
6	0.84	0.76	0.80	0.80	0.37	0.75	0.061
7	**0.86**	**0.79**	**0.82**	**0.82**	**0.36**	**0.76**	**0.055**
8	0.84	0.80	0.82	0.82	0.42	0.76	0.056
9	0.84	0.80	0.82	0.82	0.44	0.77	0.056
10	0.82	0.82	0.82	0.82	0.48	0.77	0.057

يظهر بوضوح من خلال الجدول السابق، أن نموذج آلة شعاع الدعم، يحقق أفضل نتيجة له في المرحلة الثانية والأخيرة من السيناريو الأول، عند استخدام توليفة من قِيَم البارامترات الفائقة المحددة من المرحلة السابقة وأهم **7** ميزات وفقاً لترتيب أهميتها في **الجدول 5-1**، حيث تصل قيمة AUCPR إلى **76%** وقيمة MCC إلى **82%**، مع قِيَم عالية أيضاً لباقي المقاييس، كما ينخفض معدل الإيجابيات الخاطئة بنسبة **19%** عن المرحلة الأولى من هذا السيناريو (من 55% إلى 36%)، إذ بلغت قيمتهُ في هذا المرحلة **36%** $(FPR = 0.36)$، وتقابل تلك القيم أقل قيمة $(Failure\ rate\ = 0.055)$ لنسبة الفشل. لذلك إن نموذج آلة شعاع الدعم في السيناريو الأول، يصنف معظم الحالات الشاذة (الاحتيالية) على نحوٍ صحيح وبمعدل إيجابيات خاطئة مقبول نسبياً **36%**. بلغ الزمن اللازم لتدريب النظام في هذا السيناريو **15.74** دقيقة.

II. السيناريو الثاني (Scenario 2)

1. اختيار الميزات

تُظهر نتائج المرحلة الحالية المبينة في **الجدول 7-16** أن أفضل أداء لنموذج آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم الميزات، يكون عند اختيار أهم **6** ميزات ضمن مجموعة البيانات المستخدمة وفقاً لترتيبها في **الجدول 5-1**، إذ تبلغ قيمة AUCPR **77%** وقيمة MCC **83%**، مع قيم عالية أيضاً لباقي المقاييس، وبعدل إيجابيات خاطئة (FPR) **43%**، وذلك عندما تكون قيمة نسبة الفشل أقل ما يمكن $(Failure\ rate\ = 0.054)$.

الجدول 7-15 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate
1	0.71	0.53	0.61	0.61	0.32	0.51	0.109
2	0.78	0.53	0.63	0.67	0.29	0.62	0.098
3	0.85	0.63	0.73	0.73	0.23	0.66	0.076
4	0.85	0.68	0.76	0.76	0.27	0.71	0.069
5	0.85	0.80	0.83	0.83	0.41	0.75	0.055
6	**0.85**	**0.81**	**0.83**	**0.83**	**0.43**	**0.77**	**0.054**
7	0.85	0.82	0.83	0.83	0.44	0.73	0.054
8	0.82	0.82	0.82	0.82	0.51	0.77	0.057
9	0.81	0.83	0.82	0.82	540.	0.77	0.059
10	0.79	0.83	0.81	0.81	560.	0.76	0.062

2. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-17** نتائج ضبط البارامترات الفائقة لخوارزمية آلة شعاع الدعم باستخدام تقنية البحث العشوائي. بينما يُبَيِّن **الجدول 7-18** أداء الخوارزمية باستخدام توليفة من أفضل البارامترات الفائقة المحددة في المرحلة الحالية وأهم الميزات المحددة من المرحلة السابقة.

الجدول 7-16 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الثاني (البيانات الأوروبية)

البارامترات الفائقة	القيمة
التنظيم	1000.0
Gamma	1e-2
النواة	rbf

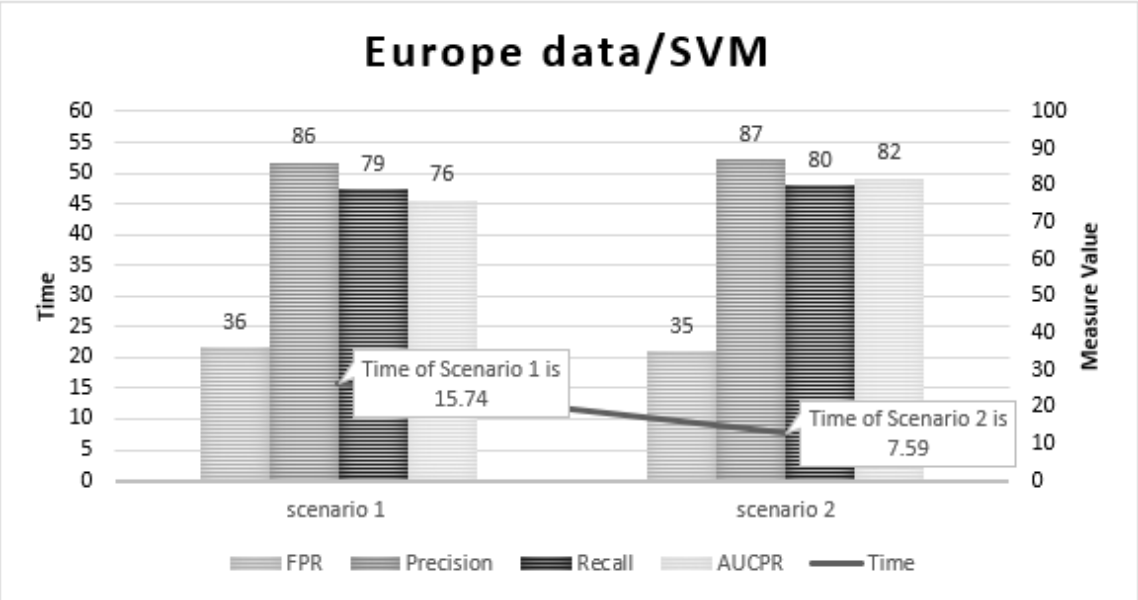
الجدول 7-17 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات الأوروبية – السيناريو الثاني

Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
0.87	0.8	0.83	0.83	0.35	0.82	0.051

أظهرت النتائج المبينة في الجدول السابق تحسين في أداء الخوارزمية مقارنة مع المرحلة الأولى من هذا السيناريو، حيث ازدادت قيمة مقياس AUCPR بنسبة **5%** وبلغت قيمتهُ **82%**، بالإضافة

لانخفاض معدل الإيجابيات الخاطئة بنسبة **8%** ($FPR = 0.35$). بلغَ الزمن لبناء النظام **7.59** دقيقة. بالتالي إن بناء النموذج وفقاً للسيناريو الثاني، يقلص من زمن البناء بنسبة **51.7%** (حوالي 8.15د: من 15.74د إلى 7.59د)، ومن معدل الإيجابيات الخاطئة بنسبة **1%** (من 36% إلى 35%) عما هو عليه في السيناريو الأول، بالإضافة إلى تحسين معظم قيم المقاييس الأخرى.

يظهر في **الشكل 7-3** تفوق السيناريو الثاني لنموذج آلة شعاع الدعم، عند تطبيقه على البيانات الأوروبية، من خلال تقليص زمن البناء (التدريب) بنسبة **51.7%**، بالإضافة إلى انخفاض في معدل الإيجابيات الخاطئة (FPR) بنسبة **1%**. كما يوجد تحسين في جميع مقاييس الأداء بنسب تتراوح من **1%** إلى **6%**.



الشكل 7-3 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام آلة شعاع الدعم وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات الأوروبية)

- **مجموعة الاحتيال المجردة**

I. السيناريو الأول (Scenario 1)

1. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-19** نتائج ضبط البارامترات الفائقة باستخدام تقنية البحث العشوائي، بينما يظهر **الجدول 7-20** أداء الخوارزمية باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المستخدمة.

الجدول 7−18 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الأول (البيانات المجردة)

البارامترات الفائقة	القيمة
التنظيم	1000.0
Gamma	1e−3
النواة	rbf

الجدول 7−19 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وجميع ميزات البيانات المجردة – السيناريو الأول

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.93	0.47	0.63	0.63	0.72	0.42	6.003

يَبْرُز من خلال النتائج الموضحة أعلاه ضمن الجدول السابق، أداء مقبول لآلة شعاع الدعم في اكتشاف الحالات الشاذة، إذ وصلت قيمة MCC إلى **63%**، وقيمة AUCPR **إلى 72%**، وبمعدل إيجابيات خاطئة **42%** ($FPR = 0.42$).

2. اختيار الميزات

يُبَيِّن **الجدول 7−21** أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم الميزات.

الجدول 7−20 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الأول

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.96	0.31	0.46	0.51	0.02	0.64	11.484
2	0.93	0.47	0.63	0.63	0.06	0.73	9.101
3	0.88	0.63	0.73	0.70	0.19	0.86	7.476
4	**0.95**	**0.73**	**0.82**	**0.80**	**0.13**	**0.89**	**5.092**
5	0.92	0.70	0.79	0.77	0.15	0.87	6.132

يظهر بوضوح من خلال الجدول السابق، أن نموذج آلة شعاع الدعم، يحقق أفضل نتيجة له في المرحلة الأخيرة من السيناريو الأول، عند استخدام توليفة من قيم البارامترات الفائقة المحددة من المرحلة السابقة وأهم **4** ميزات وفقاً لترتيب أهميتها، إذ تصل قيمة AUCPR إلى **89%** وقيمة MCC إلى **80%**، كما تزداد قيم جميع المقاييس بنسب من **2%** إلى **26%** عن المرحلة الأولى للسيناريو الأول. بالإضافة

إلى انخفاض معدل الإيجابيات الخاطئة بنسبة **29%** (من 42% إلى 13%) أي يصل إلى **13%** ($FPR = 0.13$)، وتقابل تلك القيم أقل قيمة لنسبة الفشل ($Failure\ rate\ = 5.092$). لذلك إن نموذج آلة شعاع الدعم ضمن السيناريو الأول، يصنف معظم الحالات الشاذة وبمعدل إيجابيات خاطئة لا تتجاوز **13%**. بلغ الزمن اللازم لبناء النظام في هذا السيناريو **1.76** دقيقة.

II. السيناريو الثاني (Scenario 2)

1. اختيار الميزات

تظهر نتائج المرحلة الحالية المبينة في **الجدول 7-22** أن أفضل أداء لنموذج آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الافتراضية وأهم الميزات، يكون عند اختيار أهم **4** ميزات ضمن مجموعة البيانات المستخدمة وفق لترتيبها في **الجدول 5-2**، إذ تبلغ قيمة AUCPR **85%** وقيمة MCC **82%**، مع قيم عالية أيضاً لباقي المقاييس، وبعدل إيجابيات خاطئة **21%**، وذلك عندما تكون قيمة نسبة الفشل أقل ما يمكن ($Failure\ rate\ = 4.659$). لذلك فإن للخوارزمية أداء جيداً في كشف الحالات الشاذة.

الجدول 7-21 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من القيم الافتراضية للبارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني

#Features	Precision	Recall	F1	MCC	FPR	AUCPR	Failure Rate (%)
1	0.96	0.31	0.46	0.51	0.02	0.54	11.484
2	0.92	0.53	0.67	0.66	0.09	0.68	8.451
3	0.86	0.67	0.75	0.72	0.24	0.81	7.151
4	**0.93**	**0.77**	**0.84**	**0.82**	**0.21**	**0.85**	**4.659**
5	0.88	0.63	0.73	0.70	0.19	0.84	7.476

2. ضبط البارامترات الفائقة

يُبَيِّن **الجدول 7-23** نتائج ضبط البارامترات الفائقة لخوارزمية آلة شعاع الدعم باستخدام تقنية البحث العشوائي. بينما يُبَيِّن **الجدول 7-24** أداء الخوارزمية باستخدام توليفة من أفضل البارامترات الفائقة المحددة في المرحلة الحالية وأهم الميزات المحددة من المرحلة السابقة.

الجدول 7-22 نتائج البحث العشوائي لبارامترات آلة شعاع الدعم – السيناريو الثاني (البيانات المجردة)

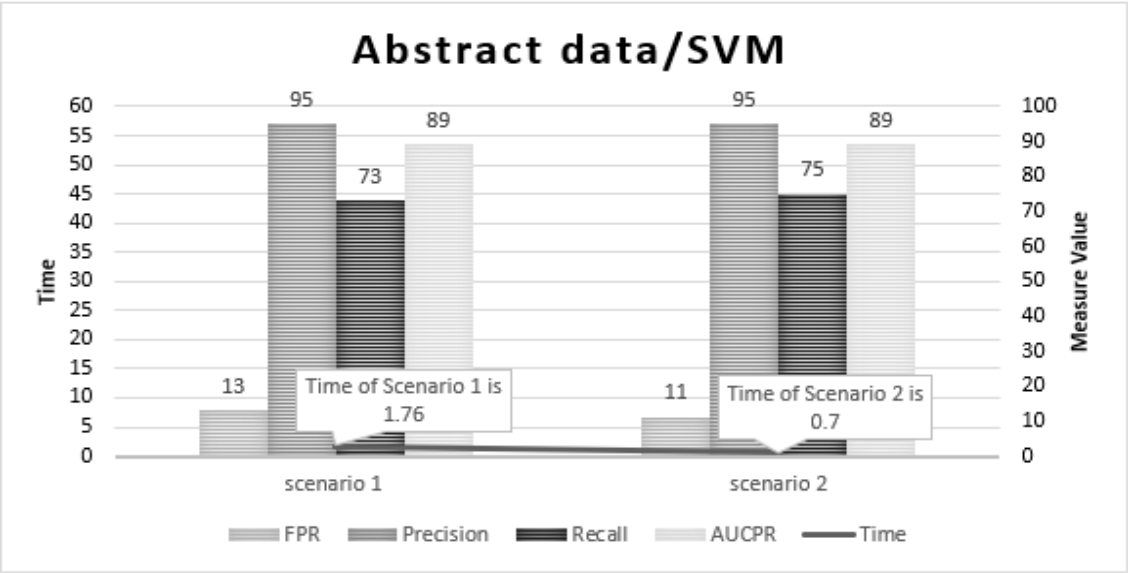
البارامترات الفائقة	القيمة
التنظيم	50.0
Gamma	1e-2
النواة	rbf

الجدول 7–23 نتائج أداء خوارزمية آلة شعاع الدعم باستخدام توليفة من أفضل قيم البارامترات الفائقة وأهم ميزات البيانات المجردة – السيناريو الثاني

Precision	Recall	F1	MCC	AUCPR	FPR	Failure Rate (%)
0.95	0.75	0.84	0.82	0.89	0.11	4.659

أظهرت النتائج المبينة في الجدول السابق تحسيناً في أداء الخوارزمية مقارنة مع المرحلة الأولى من هذا السيناريو، إذ ازدادت قيمة مقياس AUCPR بنسبة **4%** وبلغت قيمتهُ **89%**، بالإضافة إلى انخفاض معدل الإيجابيات الخاطئة بنسبة **10%** (من 21% إلى 11%). من جهة أخرى تنخفض قيمة الاسترجاع بنسبة **2%** (من 77% إلى 75%)، لكن بالمقابل ترتفع الدقة بمقدار **2%** (من 93% إلى 95%). بلغَ الزمن اللازم لبناء النظام **0.7** دقيقة. لذلك إن بناء النموذج وفقاً للسيناريو الثاني، يقلص من زمن البناء بنسبة **60.2%** (حوالي 1.06د: من 1.76د إلى 0.7 د)، ومن معدل الإيجابيات الخاطئة بنسبة **2%** (من 13% إلى 11%) عما هو عليه في السيناريو الأول، بالإضافة إلى تحسين معظم قِيَم المقاييس الأخرى.

يظهر بوضوح في **الشكل 4–7** تفوق السيناريو الثاني لنموذج آلة شعاع الدعم، عند تطبيقه على البيانات المجردة، من خلال تقليص زمن بناء النظام بنسبة **60.2%**، بالإضافة إلى انخفاض في معدل الإيجابيات الخاطئة (FPR) بنسبة **2%**. كما يوجد تحسين في مقاييس الاسترجاع بنسبة **2%** (من 73% إلى 75%).

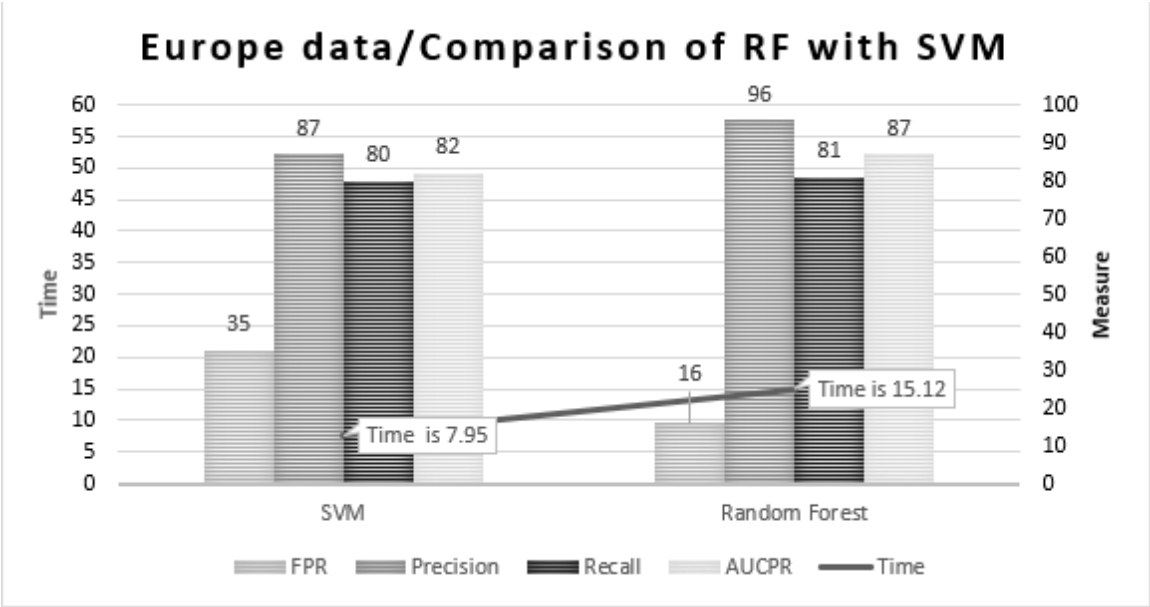


الشكل 7–4 نتائج أداء النظام الكلاسيكي لكشف الشُذُوذ باستخدام آلة شعاع الدعم وفقاً لمنهجية التحليل الْمُقْتَرَحة ضمن الدراسة (البيانات المجردة)

تَوَصَّلَت نتائج تحليل أنظمة كشف الشُّذُوذ المتبعة ضمن الدراسة إلى أن أفضل سياق لبناء الأنظمة الكلاسيكية لكشف الشُّذُوذ هو اختيار الميزات الأكثر أهمية ضمن مجموعة البيانات متبوعاً بضبط البارامترات الفائقة (السيناريو الثاني). إذ أظهرت التجارب العملية عند استخدام السياق المحدد على خوارزميتي الغابات العشوائية وآلة شعاع الدعم، تقليص كل من الزمن المستغرق لبناء هذه الأنظمة بنسبٍ تراوحت بين **51.5%** و**60.2%**، ومعدل الإيجابيات الخاطئة (FPR) بين **1%** و**35%**، بالإضافة إلى زيادة في كشف الحالات الشاذة وذلك بالنظر إلى قيم AUCPR بين **1%** و**6%**، كما يوجد تَحسِين في معظم قيم مقاييس الأداء، مما يُؤَكِّد على التحسين الحاصل عند اعتماد الترتيب المذكور.

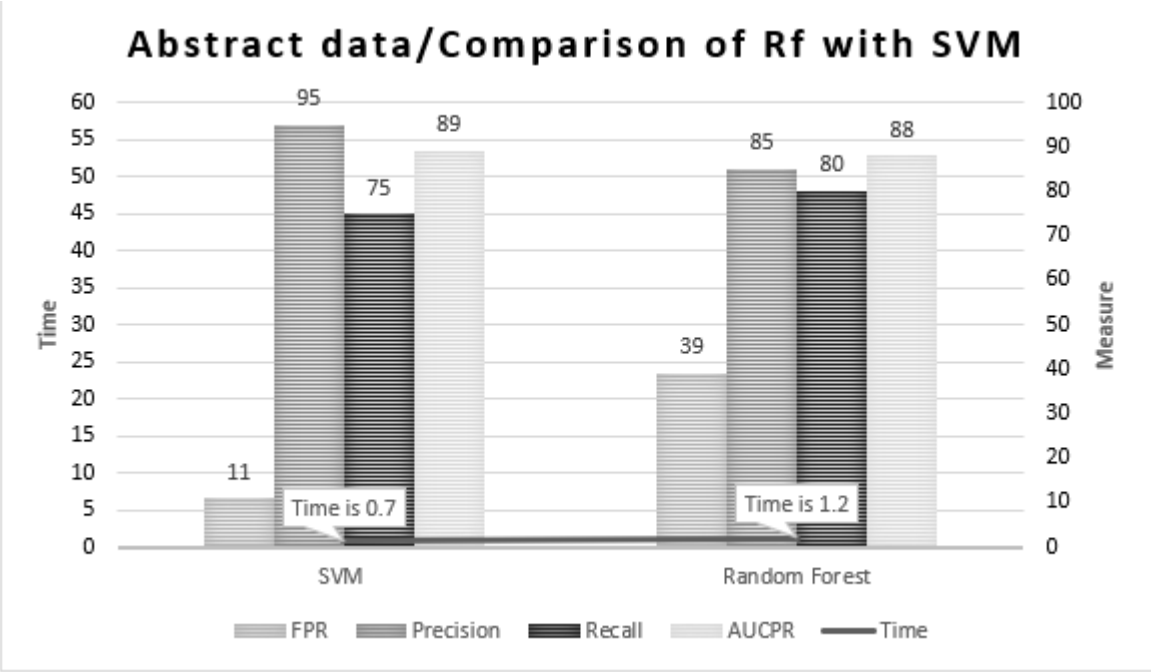
بالإضافة إلى ذلك تظهر النتائج تفوق خوارزمية الغابات العشوائية على خوارزمية آلة شعاع الدعم من حيث نسبة كشف الشُّذُوذ، بالمقابل حققت خوارزمية آلة شعاع الدعم أداء أفضل من حيث الزمن؛ وذلك من أجل مجموعات البيانات الأوروبية، أما بالنسبة للبيانات المجردة فقد استطاعت خوارزمية آلة شعاع الدعم التفوق على الغابات العشوائية من حيث الزمن ونسبة الكشف.

يوضح المخطط في **الشكل 7-5** أداء الخوارزميات من أجل البيانات الأوروبية، إذ يظهر تفوّق الغابات العشوائية على آلة شعاع الدعم من حيث انخفاض معدل الإيجابيات الخاطئة (FPR) بنسبة **19%** (من 35% إلى 16%)، وازدياد مساحة السطح تحت منحني الدقة والاسترجاع (AUCPR) بنسبة **5%** (من 82% إلى 87%). بالمقابل استطاعت آلة شعاع الدعم التفوق على الغابات العشوائية من حيث الزمن بنسبة **47.4%** (حوالي 7.17د: من 15.12د إلى 7.95د)



الشكل 7-5 مقارنة أداء خوارزمية الغابات العشوائية وآلة شعاع الدعم في اكتشاف الشُذُوذ – حالة البيانات الأوروبية

يوضح المخطط في **الشكل 7-6** أداء الخوارزميات من أجل البيانات المجردة، إذ يظهر في هذه الحالة تفوق آلة شعاع الدعم على الغابات العشوائية من حيث انخفاض معدل الإيجابيات الخاطئة (FPR) بنسبة **28%** (من 39% إلى 11%)، وانخفاض الزمن بنسبة **41.6%** (حوالي 0.5د: من 1.2د إلى 0.7د)، وازدياد مساحة السطح تحت منحني الدقة والاسترجاع (AUCPR) بنسبة **1%** (من 88% إلى 89%). إن السبب الرئيسي لتفوق آلة شعاع الدعم هو حجم البيانات الصغير، إذ تحتاج الغابات العشوائية إلى حجم أكبر من العيانات من أجل عملية Bootstrap.



الشكل 7-6 مقارنة أداء خوارزمية الغابات العشوائية وآلة شعاع الدعم في اكتشاف الشُذُوذ – حالة البيانات المجردة

في ختام هذا القسم، يبدو واضحاً من خلال النتائج التي تَمّ الحصول عليها من تحليل طرائق تَعلُّم الآلة في اكتشاف الشُذُوذ التأكيد على ضرورة توخي الحذر في اعتمادها، إذ يمكن الوصول إلى نتائج جيدة بسهولة بسبب ما تفرضه مشكلة شح البيانات الشاذة وهذا ما يظهر واضحاً في انخفاض نسبة الفشل.

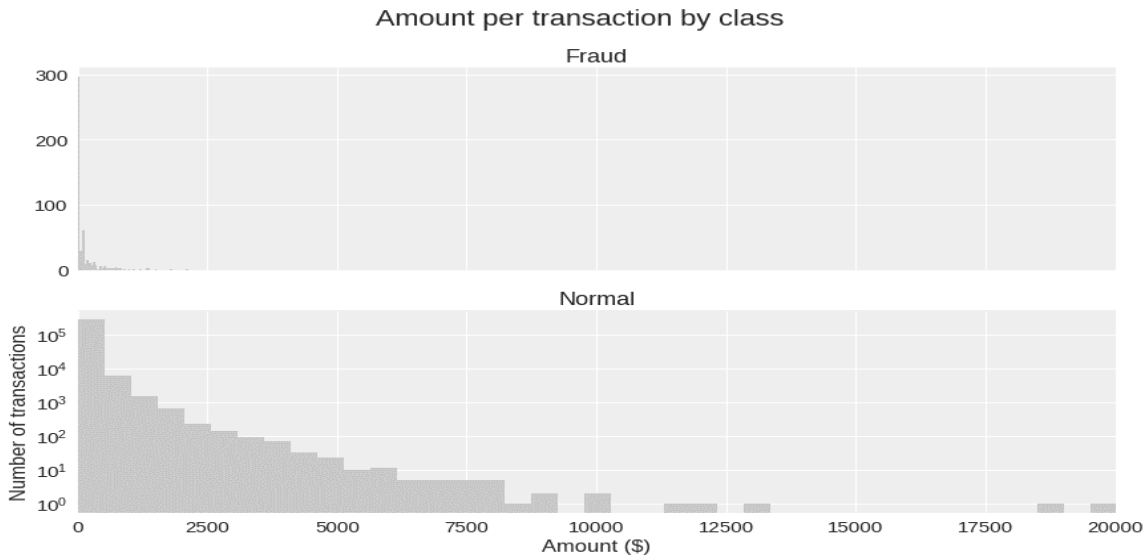
7-2- نظام كشف الشُذُوذ الْمُقْتَرَح (Proposed Anomaly Detection System)

يَعَرّض القسم الحالي النتائج وتقييم الأداء لنظام كشف الشُذُوذ الديناميكي الْمُقْتَرَح بحالتيه، من دون ذاكرة (AEDT-ADS) ومع ذاكرة (AEDTM-ADS)، وذلك عند تطبيقه على مجموعات بيانات حقيقية وهما: مجموعة الاحتيال الأوروبية، ومجموعة كسر الورق.

7-2-1- حالة النظام بدون ذاكرة AEDT-ADS

- **مجموعة بيانات الاحتيال الأوروبية**

يَهدُف تطبيق نظام AEDT-ADS على مجموعة البيانات الأوروبية، إلى دراسة مدى فعالية النظام في التعامل مع حالات شُذُوذ النقطة واكتشافها **(راجع الفصل الأول للتذكير بأنواع الشذوذ)**. يظهر من خلال الشكل الآتي أن أغلب المعاملات الاحتيالية تتركز تحت 500 دولار، ولذلك يمكن حصر المعاملات الاحتيالية من خلال المبلغ المصروف، وهذا ما يسمى شُذُوذ نقطة.



الشكل 7-7 العلاقة بين نوع المعاملة وكمية المبلغ المصروف

I. نمذجة النظام (AEDT-ADS Modeling)

تَتَضَمَّن نمذجة النظام، نتائج كل من ضبط البارامترات الفائقة، ومعمارية الشبكة، وقياس الأهمية النسبية للميزات.

1. ضبط البارامترات الفائقة (Hyperparameters Tuning)

يوضح **الجدول 7-25** بعضاً من أهم نتائج البحث العشوائي، فيما يتعلق بالتكوينات المرشحة للبارامترات الفائقة، والتي تَمَّ تلخيصها في **الجدول 6-1** ضمن الفصل السادس. تَمَّ تدريب AEDT على مجموعات مختلفة من هذه التكوينات؛ إن اختيار أفضل تكوينة للبارامترات الفائقة، تمَّ بناءً على أقل قيمة لخسارة شبكة AEDT والمشار إليها في المعادلة (7-6) من الفصل السادس، ونتيجة لذلك يستخدم النظام تكوينة البارامترات الفائقة التي تقابل ($MSE = 0.455$)، (انظر إلى السطر الأخير من الجدول الآتي). علماً أن الزمن المستغرق لضبط البارامترات الفائقة في هذه الحالة **2.37** ساعة.

الجدول 7–24 نتائج البحث العشوائي لشبكة AEDT – حالة البيانات الأوروبية

Hyperparameters Configurations							MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation (hidden)**	**Activation (out layer)**	
20	50	128	0.0001	0.3	Relu	Sigmoid	0.871
14	75	256	0.0001	0.1	Relu	Linear	0.721
16	50	32	0.001	0.5	Tanh	Tanh	0.731
16	50	128	0.0001	0.3	Tanh	Linear	0.598
14	50	32	0.0001	0.3	Tanh	Tanh	0.684
16	50	32	0.0001	0.1	Tanh	Sigmoid	0.781
20	**50**	**64**	**0.0001**	**0.0**	**Tanh**	**Linear**	**0.455**

2.معمارية الشبكة (Architecture of AEDT)

تتكون شبكة AEDT من ثلاث طبقات تشفير (Encoder)، وثلاث طبقات فك تشفير (Decoder)، وطبقة تسريب (Dropout). بالاعتماد على نتائج البحث العشوائي في الجدول السابق، وبالنظر إلى عدد العصبونات (Neurons)؛ إن حجم طبقة التشفير الأولى هو 20 عصبوناً، ثم تتناقص عدد العصبونات تدريجياً إلى النصف من أجل كل طبقة تشفير تَالِيَة، بينما يَتُمّ مضاعفتها تدريجياً في طبقات فك التشفير. يوضح **الجدول 7–26** أنواع طبقات AEDT مع عدد العصبونات في كل طبقة.

الجدول 7–25 بنية شبكة AEDT – البيانات الأوربية

Layer (type)	Output Shape
Input Layer	(-,30)
Dropout Layer	(-,30)
Encoder-1	(-,20)
Encoder-2	(-,10)
Encoder-3	(-,5)
Decoder-1	(-,5)
Decoder-2	(-,10)
Decoder-3	(-,20)
Output Layer	(-,30)

3. أهمية الميزات (Features Importance)

يَعرُض **الجدول 7–27** ترتيب أهمية ميزات بيانات الاحتيال الأوربية وفقاً لمقياس الحجم (انظر المعادلات (6-4) (6-5) (6-6) من الفصل السادس)، وبناءً عليه إن الميزات الأكثر أهمية والمُبيّنة

في الجدول الآتي (V26, V13, V18, V15, V24) تُسهم على نحوٍ أكبر في زيادة قدرة النظام على كشف الحالات الشاذة، إذ يكون لجميعها أهمية ≤ 93%.

الجدول 7-26 حجم مساهمة الميزات في أداء النظام – أهمية ميزات البيانات الأوروبية

Rank	Feature	Importance	Rank	Feature	Importance
1	**V26**	**100%**	16	V21	9%
2	**V13**	**97%**	17	V11	9%
3	**V18**	**96%**	18	V12	9%
4	**V15**	**94%**	19	V27	9%
5	**V24**	**93%**	20	V23	9%
6	V20	12%	21	V17	9%
7	V22	12%	22	V14	9%
8	V25	11%	23	V5	9%
9	V16	11%	24	V19	8%
10	V7	11%	25	V1	8%
11	V10	11%	26	V4	8%
12	V9	10%	27	V6	8%
13	Amount	10%	28	V2	8%
14	V8	10%	29	V3	8%
15	V28	10%	30	Time	0%

4. توزيع البيانات (Data Distribution)

يَدرُس النظام الْمُقْتَرَح مدى ملاءمة البيانات الطبيعية لأحد التوزيعات الاحتمالية، إذ تمَّ اختبار البيانات على مجموعة واسعة من التوزيعات المحتملة، التي تمَّ ترتيبها بالاعتماد على مربع كاي. أظهرت النتائج أن البيانات المدروسة تتلاءم على نحوٍ أفضل مع توزيع $Genextreme$، وهذا ما تؤكده نتائج اختبار كولموغوروف سميرنوف في الجدول الآتي.

الجدول 7-27 نتائج اختبار كولموغوروف سميرنوف – البيانات الأوروبية

البارامتر	القيمة
$t_statistic$: القيمة الإحصائية (Statistic Value)	0.025
a: معامل الثقة (Significance Level)	0.05
p_{value}	0.262
$t_critical$: القيمة الحرجة (Critical Value)	0.043

أن $t_statistic < t_critical$ ولذلك يتم قبول النظرية الصفرية (H0) التي تنص على أن البيانات مأخوذة من التوزيع المحدد ($genextreme$)، وبما أن البيانات لا تتبع التوزيع الطبيعي لذلك يستخدم النظام نظرية تشيبيشيف لتحديد المجال الذي يقع ضمنه معظم البيانات الطبيعية.

II. أداء النظام (AEDT–ADS Performance)

يَعرُض القسم الحالي تَقييم أداء AEDT–ADS باستخدام مقاييس الأداء المشار إليها في الفصل الثالث من هذه الأطروحة.

1. تفاضل العَتَبَة (Threshold Tradeoff)

يختار النظام عَتَبَة التصنيف التي يَتُمَّ إيجادها على نحوٍ ديناميكي من ضمن المجال [0.4,2.84] المحدد من قبلهِ، إذ تمثل القيمة 0.4 الحد الأدنى لعَتَبَة التصنيف، والقيمة 2.84 الحد الأعلى؛ كما أن جميع قيم العتبات ضمن المجال مقبولة. يظهر **الجدول 7–29** أداء AEDT–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن وخارج المجال المحدد.

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **90%**، من أجل $1.04 \leq T \leq 2.84$، أما أفضل قيمة للدقة (Precision) فتصل إلى **94%** من أجل $T \geq 2.54$، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **9%** عند العَتَبَة ($T = 2.84$).

الجدول 7–28 نتائج أداء AEDT–ADS – البيانات الأوروبية

Range	Threshold	F1Score	Recall	Precision	FPR	Failure rate (%)
Outside	0.2	0.65	0.72	0.72	0.92	35.56
	0.3	0.77	0.81	0.77	0.79	22.87
Inside	Min:0.4	0.82	0.85	0.82	0.68	16.73
	0.74	0.87	0.88	0.87	0.46	11.4
	1.04	0.90	0.90	0.90	0.28	8.84
	1.34	0.91	0.90	0.92	0.21	7.76
	1.94	0.91	0.90	0.93	0.17	7.56
	2.54	0.92	0.90	0.94	0.11	7.09
	Max:2.84	**0.92**	**0.90**	**0.94**	**0.09**	**6.95**
Outside	3.44	0.92	0.90	0.94	0.09	7.35
	3.9	0.91	0.89	0.94	0.09	7.62

– تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة

– تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

يَتِمُّ التفاضل بَيْن قِيَم العَتَبَة حَسَبَ طبيعة المسألة. تهدف عادةً أنظمة كشف الشُّذُوذ ضمن مجموعات البيانات المالية إلى تحقيق توزان مقبول بين مقياسي الاسترجاع والدقة، ومع التنبيه على ألا يتجاوز معدل الإيجابيات الخاطئة (FPR) حداً معيناً موصى به [147]. لذلك بالنظر إلى $T = 2.84$، نجد أن AEDT–ADS يحقق تفاضل العَتَبَة المطلوب، إذ يستطيع استرجاع **90%** ($Recall = 0.9$) من الحالات الشاذة (الاحتيالية)، وبدقة كبيرة تصل إلى **94%** ($Precision = 0.94$)، وبمعدل إنذارات كاذبة لا تتجاوز **9%** ($FPR = 0.09$).

من جهة أخرى، تَمَّ اختبار AEDT–ADS باستخدام عتبات تصنيف تقع خارج المجال المحدد. فمن أجل $T: 0.2 , 3.9$، يتراجع أداء النظام مقارنةً مع أدائه عند استخدام عَتَبَة التصنيف ($T = 2.84$)، إذ ينخفض الاسترجاع إلى **72%** عند ($T = 0.2$)، وإلى **89%** عند ($T = 0.39$)، بالإضافة إلى أن معدل الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل ($failure\ rate = 6.95$) عند العَتَبَة ($T = 2.84$).

بناءً على نتائج هذه التجربة فإن النظام الْمُقْتَرَح AEDT–ADS، يستطيع تحقيق توازن كبير بين الدقة والاسترجاع عند قيم عالية، بالإضافة إلى انخفاض في معدل الإنذارات الكاذبة، وذلك عند اعتماده على عتبات تقع ضمن المجال الذي يحدده النظام بشكل ديناميكي [0.4,2.84]؛ وأن النظام AEDT–ADS يمكنه التعامل مع حالات شُذُوذ النقطة بكفاءة عالية.

- **مجموعة بيانات كسر الورق**

يَهدُف تطبيق نظام AEDT–ADS على مجموعة بيانات كسر الورق، إلى دراسة مدى فعالية النظام في اكتشاف الحالات الشاذة ضمن سياق زمني مُعيَّن قبل حدوثها بوقت مناسب.

I. نمذجة النظام (AEDT–ADS Modeling)

1. ضبط البارامترات الفائقة

يوضح **الجدول 7–30** بعضاً من أهم نتائج البحث العشوائي. يستخدم النظام في هذه الحالة تكوينة البارامترات الفائقة التي تقابل ($MSE = 0.185$)، (انظر إلى السطر الأخير في الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة في هذه الحالة **15** دقيقة.

الجدول 7–29 نتائج البحث العشوائي لشبكة AEDT – حالة بيانات كسر الورق

Hyperparameters Configurations							MSE
Nodes	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation (hidden)**	**Activation (out layer)**	
12	200	128	0.01	0.2	Sigmoid	Tanh	0.724
12	50	256	0.001	0.3	Tanh	Tanh	0.691
16	150	256	0.0001	0.3	Tanh	Tanh	0.548
16	75	64	0.001	0.2	Tanh	Tanh	0.468
32	50	256	0.001	0.5	Tanh	Linear	0.399
32	50	32	0.001	0.2	Relu	Linear	0.200
32	**200**	**64**	**0.001**	**0.4**	**Tanh**	**Linear**	**0.185**

2. معمارية الشبكة

تتكون شبكة AEDT من طبقتي تشفير وطبقتي فك تشفير وطبقة تسريب. بالاعتماد على نتائج البحث العشوائي في الجدول السابق، وبالنظر إلى عدد العصبونات، وعلى نحوٍ مشابه لآلية ضبط حجم الطبقة (عدد العصبونات) في حالة البيانات الأوروبية، تَمَّ ضبط حجم الطبقات في هذه الحالة. يوضح الجدول الآتي أنواع طبقات AEDT مع عدد العصبونات في كل طبقة.

الجدول 7–30 بنية شبكة AEDT – بيانات كسر الورق

Layer (type)	Output Shape
Input Layer	(-,59)
Dropout Layer	(-,59)
Encoder-1	(-,32)
Encoder-2	(-,16)
Decoder-1	(-,16)
Decoder-2	(-,32)
Output Layer	(-,59)

3. أهمية الميزات

يعرض **الجدول 7–32** ترتيب أهمية ميزات بيانات كسر الورق وفقاً لمقياس الحجم، وبناءً عليه يَعتَمد النظام الْمُقْتَرَح على الميزات (x3, x19, x4, x42) الأكثر أهمية بشكل أكبر في عملية الكشف عن الحالات الشاذة، حيث يكون لجميعها أهمية > 75%.

الجدول 7−31 حجم مساهمة الميزات في أداء النظام − أهمية ميزات بيانات كسر الورق

Rank	Feature	Importance	Rank	Feature	Importance	Rank	Feature	Importance
1	**x3**	100%	21	x52	50%	41	x45	20%
2	**x19**	90%	22	x24	49%	42	x12	19%
3	**x4**	87%	23	x54	49%	43	x48	19%
4	**x42**	78%	24	x40	49%	44	x8	19%
5	x20	74%	25	x50	45%	45	x32	19%
6	x29	74%	26	x33	45%	46	x15	17%
7	x22	73%	27	x34	44%	47	x7	16%
8	x58	70%	28	x57	43%	48	x51	16%
9	x2	69%	29	x1	41%	49	x39	15%
10	x26	67%	30	x37	41%	50	x31	15%
11	x53	65%	31	x21	38%	51	x41	14%
12	x47	60%	32	x6	37%	52	x38	14%
13	x23	60%	33	x5	37%	53	x43	14%
14	x27	58%	34	x18	31%	54	x30	14%
15	x55	55%	35	x49	28%	55	x46	13%
16	x56	54%	36	x17	25%	56	x36	12%
17	x35	54%	37	x16	24%	57	x10	12%
18	x60	53%	38	x11	24%	58	x14	12%
19	x13	52%	39	x59	22%	59	x9	10%
20	x44	51%	40	x25	21%	60	x28, x61	0%

4. توزيع البيانات

بالآلية المتبعة في البيانات الأوروبية نفسها، يحدد النظام التوزيع $Burr$ هو التوزيع الملائم للبيانات وهذا ما يؤكده نتائج اختبار كولموغوروف سميرنوف في الجدول الآتي.

الجدول 7−32 نتائج اختبار كولموغوروف سميرنوف – بيانات كسر الورق

البارامتر	القيمة
$t_statistic$: القيمة الإحصائية (Statistic Value)	0.011
a: معامل الثقة (Significance Level)	0.05
p_{value}	0.384
$t_critical$: القيمة الحرجة (Critical Value)	0.022

نجد أن $t_statistic < t_critical$ ولذلك يَتِمُّ قبول النظرية الصفرية (H0) التي تنص على أن البيانات مأخوذة من التوزيع الأفضل وفقاً لمربع كاي ($Burr$)، وبما أن البيانات لا تتبع التوزيع الطبيعي، يستخدم النظام الْمُقْتَرَح نظرية تشيبيشيف لتحديد المجال الذي يقع ضمنه معظم البيانات الطبيعية.

5. زمن الكشف

تَمَّ تَعْيِين $s = 2$ ضِمْنَ المعادلة (3-6) من الفصل السادس، مما يعني أن النظام قادر على توقع الشَذُوذ قبل حدوثه بمقدار 4 دقائق (يفصل بين كل قراءة دقيقتين). يجب التنبيه على أن قيمة s تُحدّد وفقاً للنموذج المدروس، فمن أجل حالة كسر الورق يعتبر الكشف قبل أربع دقائق وقتاً مناسباً لتفادي عملية الكسر [46].

II. أداء النظام (AEDT–ADS Performance)

يَعرُض القسم الحالي تقييم أداء AEDT–ADS باستخدام مقاييس الأداء المشار إليها في الفصل الثالث من هذه الأطروحة.

1. تفاضل العَتَبَة

يختار النظام عَتَبَة التصنيف التي يَتُمَّ إيجادها على نحوٍ ديناميكي من ضمن المجال [0.2,1.4] المحدد من قبلهِ. إن جميع قيم العتبات ضمن المجال مقبولة. يظهر **الجدول 7–34** أداء AEDT–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن وخارج المجال المحدد.

الجدول 7–33 نتائج أداء AEDT–ADS – بيانات كسر الورق

Rang	Threshold	F1Score	Recall	Precision	FPR	Failure rate (%)
Outside	0.05	0.33	0.47	0.50	1.0	92.7
	0.1	0.35	0.52	0.49	0.98	66.23
Inside	Min:0.2	0.49	0.56	0.50	0.84	24.03
	0.5	0.52	0.51	0.53	0.42	9.48
	0.8	0.52	0.49	0.55	0.25	7.48
	1.1	0.51	0.49	0.56	0.15	7.06
	Max:1.4	**0.51**	**0.49**	**0.57**	**0.14**	**6.86**
Outside	1.7	0.51	0.49	0.62	0.15	6.90
	2.0	0.50	0.48	0.62	0.16	6.91

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **56%**، عند العَتَبَة ($T = 0.2$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **57%** عند العَتَبَة ($T = 1.4$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **14%** عند العَتَبَة ($T = 1.4$).

تَهدُف أنظمة كشف كسر الورق لِإسترِجاع أكبر قدر مُمْكِن من حالات الكسر، تفادياً لتوقف الآلات لساعات طويلة، إذ يبقى زمن فحص الحالة والتأكد من صحتها، أقل تكلفة مادية وزمنية من حدوث الكسر، لكن بالمقابل يجب ألا تتجاوز نسبة الإيجابيات الخاطئة (FPR) حَداً مُعيناً موصى به. لذلك بالنظر إلى $T = 1.4$، يحقق AEDT–ADS تفاضل العَتَبَة المطلوب، إذ يستطيع كشف **49%** من حالات الكسر قبل 4 دقائق من حدوثها ($Recall = 0.49$)، بنسبة إنذارات خاطئة **14%** ($FPR = 0.14$).

يظهر بوضوح من خلال الجدول السابق عند اختبار أداء AEDT–ADS باستخدام عتبات تصنيف تقع خارج المجال المحدد، تراجع أدائه مقارنةً باستخدام عتبات من ضمن المجال، فمن أجل $T \leq 0.1$ يرتفع معدل الإيجابيات الخاطئة على نحوٍ كبير ($FPR \geq 98$)، وهذا مؤشر سَيِّئ للغاية في أداء أنظمة كشف الشَذُوذ عموماً. أما بالنسبة $T = 2.0$ فينخفض معدل الاسترجاع إلى **48%**، كما يرتفع معدل الإيجابيات الخاطئة إلى **16%**. بالإضافة إلى أن نسبة الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل ($failure\ rate = 6.86$) عند العَتَبَة ($T = 1.4$)، مما يؤكد على ضرورة استخدام عتبات من ضمن المجال المحدد بشكل ديناميكي.

2. تحليل التكاليف والفوائد (Cost Benefit Analysis)

تَمَّ تَحْليل مساهمة AEDT–ADS في الحَدّ من الخسارة المالية في مشكلة كسر الورق. إذ تمَّ اِحتِساب الربح على أساس الاسترجاع، والخسارة الناتجة على أساس معدل الإيجابيات الخاطئة، علماً أنه قُدرت تكلفة كُلّ عملية كسر بحوالي 10,000 دولار أمريكي، بينما تكلفة كل إنذار خاطئ بحوالي 100 دولار أمريكي فقط [46]. يُبيّن الجدول الآتي مقدار الخسارة الذي يوفره AEDT–ADS في كل عام، والتي تجاوزت **7** ملايين دولار سنوياً عن كل خط إنتاج، أي بمعدل **46%** من الخسارة الإجمالية البالغة **15** مليون دولار عن كل خط انتاج [148].

الجدول 7−34 تحليل التكلفة والفائدة لنظام AEDT−ADS− بيانات كسر الورق

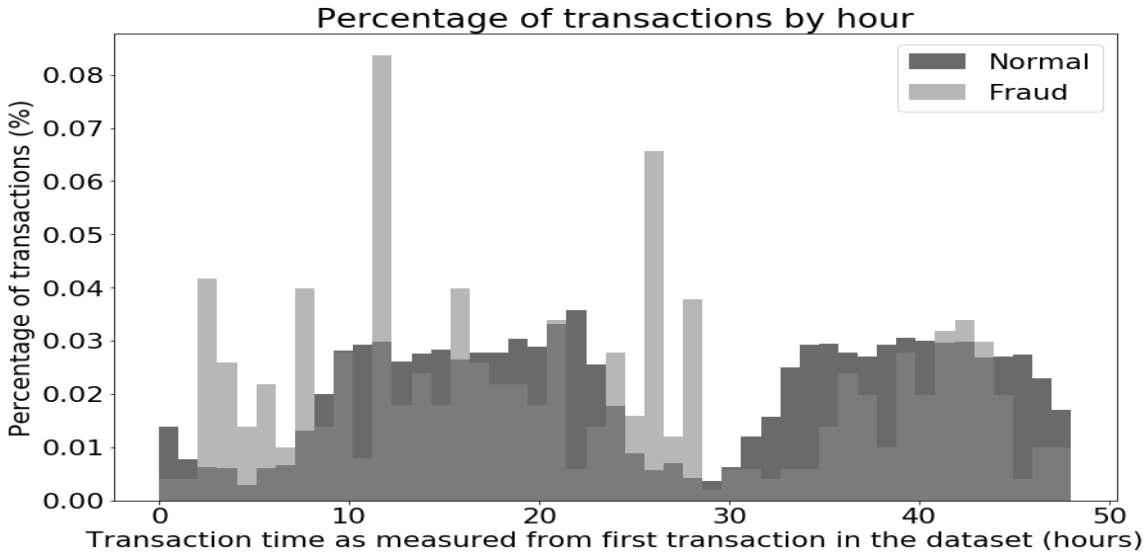
Item	Gain (by TPR)	Loss (by FPR)	Remark
تكلفة	10,000$	100$	−
عدد الحالات	124x12month=1488	(2 minx30x24 hr.x365 d)−1488=524112	1 year
معدل الحالات	Recall=49%	FPR=14%	Test Result
تكلفة/ سنة	7,291,200$	−73,375$	
الإجمالي	7,217,825$		

بناءً على نتائج هذه التجربة، يمكن استخدام النظام الْمُقْتَرَح AEDT−ADS، كطريقة سريعة في تحديد الحالات الشاذة ضمن السلاسل الزمنية. استطاع النظام عند اختياره لقيم عتبات من المجال المحدد بشكل ديناميكي [0.2,1.4]، تحقيق نتائج مقبولة بالنسبة لمشكلة كسر الورق، حيث كشف **49%** من حالات الكسر قبل **4** دقائق من حدوثها، وبنسبة إنذارات خاطئة **14%** عند العَتَبَة ($T = 1.4$)، بينما بلغت نسبة الحد من الخسائر الناتجة عن هذه المشكلة **46%**.

7−2−2− حالة النظام مع ذاكرة AEDTM−ADS

- **مجموعة بيانات الاحتيال الأوروبية**

يَهدُف تطبيق نظام AEDTM−ADS على مجموعة البيانات الأوروبية، دراسة مدى فعالية النظام في اكتشاف الحالات الشاذة للأحداث المجمعة بطريقة ما، حتى ولو كانت غير متسلسلة بوضوح. حيث يظهر من خلال الشكل الآتي وجود معاملات احتيالية على مدار الساعة؛ بالمقابل تنخفض عدد المعاملات الطبيعية بين الساعة **1−8**، ومرة أخرى بين الساعة **24−32**، بالتالي يمكن وضع فرضية أن هناك تسلسل ما للعمليات الاحتيالية في أوقات معينة كأوقات الليل. يبقى ذلك فرضية ولا يمكن تحديد الأوقات بدقة بسبب عدم معرفة الوقت الفعلي للمعاملة، أي إن سياق المعاملات الاحتيالية غير واضح. لكن في حال معرفة الوقت الحقيقي من قبل الجهة المنفذة للنظام يمكن عندئذٍ تحديد السياق الصحيح.



الشكل 7–8 العلاقة بين نوع المعاملة ووقت حدوثها

I. نمذجة النظام (AEDTM–ADS Modeling)

1. حجم النافذة الزمنية (Time Window Size)

يتُمَّ زيادة حجم النافذة ضِمْنَ النظام بناءً على التجربة، والتوقف عن زيادة الحجم عندما يبدأ أداء النظام بالتراجع. علماً أنه تَمَّ البدء بحجم $m = 3$ والزيادة بمقدار 2 على كل حجم تالٍ بحيث يكون هناك تأثير واضح لحجم النافذة.

2. ضبط البارامترات الفائقة

يوضح **الجدول 7–36** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 3$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.020)$، (انظر إلى السطر الأخير في الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **4** ساعات.

الجدول 7–35 نتائج البحث العشوائي لشبكة LSTM–AEDT عند حجم نافذة m = 3 – البيانات الأوروبية

Hyperparameters Configurations						MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation**	
10	50	64	0.0001	0.3	Sigmoid	0.844
50	30	32	0.01	0.3	Relu	0.896
70	30	32	0.001	0.0	Tanh	0.052
20	30	64	0.001	0.1	Relu	0.563
10	30	256	0.0001	0.2	Tanh	0.903
50	30	32	0.01	0.0	Tanh	0.161
100	**30**	**32**	**0.001**	**0.0**	**Tanh**	**0.020**

يوضح **الجدول 7−37** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 5$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.064)$، (انظر إلى السطر الأول في الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **5** ساعات.

الجدول 7−36 نتائج البحث العشوائي لشبكة LSTM−AEDT عند حجم نافذة $m = 5$ – البيانات الأوروبية

Hyperparameters Configurations						MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation**	
100	**30**	**32**	**0.001**	**0.0**	**Tanh**	**0.064**
50	25	64	0.0001	0.4	Tanh	0.519
70	30	32	0.001	0.0	Tanh	0.138
80	50	128	0.001	0.5	Tanh	0.525
100	50	128	0.0001	0.1	Sigmoid	0.923
50	25	64	0.0001	0.1	Relu	0.668
100	30	256	0.001	0.5	Relu	1.004

3. معمارية الشبكة

إنّ شبكة LSTM−AEDT من النوع المتناثر (Sparse)، ولذلك فإن عدد العصبونات في الطبقة المخفية أكثر من طبقة الدخل. بالاعتماد على نتائج البحث العشوائي في الجَدْوَلَيْن السابقين، وبالنظر إلى عدد العصبونات، تمَّ ضبط حجم كل من طبقة التشفير وفك التشفير إلى 100 عصبون. يوضح الجدول الآتي أنواع طبقات LSTM−AEDT مع عدد العصبونات في كل طبقة.

الجدول 7−37 بنية شبكة LSTM−AEDT – البيانات الأوروبية

Layer (type)	Output Shape
Input Layer	(-, win-size,30)
LSTM (Encoder-1)	(-,100)
Dropout Layer	(-,100)
Repeat Vector Layer	(-, win-size,100)
LSTM (Decoder-1)	(-, win-size,100)
Time Distributed (Output)	(-, win-size,30)

4. توزيع البيانات

بناءً على نتائج اختبار كولموغوروف سميرنوف على البيانات الأوروبية، والموضحة في **الجدول 7−28**؛ تبيّن إن البيانات لا تتبع توزيعاً طبيعياً، ولذلك يستخدم النظام نظرية تشيبيشيف لتحديد المجال الذي يقع ضمنه معظم البيانات.

II. أداء النظام (AEDTM–ADS Performance)

1. تفاضل العَتَبَة

a. من أجل حجم نافذة $m = 3$

يختار النظام من أجل حجم نافذة $m = 3$ عَتَبَة التصنيف التي يتُمَّ إيجادها على نحوٍ ديناميكي من ضمن المجال المحدد بواسطته $[0.02,1.02]$، إذ إن جميع قيم العتبات ضمن المجال مقبولة. يظهر الجدول الآتي أداء AEDTM–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن وخارج المجال المحدد.

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **91%**، عند العَتَبَة ($T = 0.22$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **85%** عند العَتَبَة ($T \geq 0.92$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **39%** عند العَتَبَة ($0.92 \leq T \leq 1.02$).

الجدول 7–38 نتائج أداء AEDTM–ADS عند حجم نافذة $m = 3$ – البيانات الأوروبية

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.01	0.47	0.85	0.52	21.57	1.0
Inside	Min:0.02	0.53	0.89	0.53	10.63	0.99
	0.22	0.76	0.91	0.69	9.27	0.88
	0.42	0.82	0.90	0.77	8.75	0.77
	0.62	0.84	0.87	0.82	8.58	0.61
	0.82	0.83	0.82	0.84	7.56	0.46
	0.92	**0.82**	**0.80**	**0.85**	**7.55**	**0.39**
	Max:1.02	0.81	0.78	0.85	7.59	0.39
Outside	1.1	0.80	0.76	0.85	7.59	0.40
	1.2	0.8	0.75	0.85	7.59	0.40

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

يحقق AEDTM–ADS تفاضل العَتَبَة المطلوب في الأنظمة المالية عند $T = 0.92$، إذ يستطيع استرجاع **80%** ($Recall = 0.8$) من الحالات الشاذة (الاحتيالية)، وبدقة جيدة جداً تصل إلى **85%** ($Precision = 0.85$)، وبمعدل إنذارات كاذبة مقبولة **39%** ($FPR = 0.39$)، وبلغ الزمن اللازم لتدريب النظام بالاعتماد على البارامترات الفائقة الأمثل حوالي **23** دقيقة.

من جهة أخرى، تَمَّ اختبار AEDTM–ADS باستخدام عتبات تصنيف تقع خارج المجال المحدد. فمن أجل $T = 0.01$ تنخفض الدقة بشكل كبير إلى **52%**. أما بالنسبة $T = 1.2$ فينخفض معدل الاسترجاع إلى **75%**. بالإضافة إلى أن نسبة الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل ($failure\ rate = 7.55$) عند العَتَبَة ($T = 0.92$). لذلك يتراجع أداء النظام مقارنةً مع أدائه عند استخدام عتبات تصنيف من ضمن المجال المحدد بشكل ديناميكي، كما أن قيم العتبات التي تقع خارج المجال لا تستطيع تحقيق التوزان الأفضل بين الدقة والاسترجاع.

b. من أجل حجم نافذة $m = 5$

يختار النظام من أجل حجم نافذة $m = 5$ عَتَبَة التصنيف التي يَتِمُّ إيجادها على نحوٍ ديناميكي من ضمن المجال المحدد من قبلهِ $[0.06,1.06]$، إذ إن جميع قيم العتبات ضمن المجال مقبولة. يظهر الجدول الآتي أداء AEDTM–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن وخارج المجال المحدد.

الجدول 7–39 نتائج أداء AEDTM–ADS عند حجم نافذة $m = 5$ – البيانات الأوربية

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.02	0.36	0.73	0.51	47.66	1.0
	0.04	0.45	0.82	0.51	27.48	1.0
Inside	Min:0.06	0.49	0.85	0.52	18.67	1.0
	0.26	0.63	0.89	0.58	13.72	0.96
	0.46	0.71	0.89	0.64	11.87	0.91
	0.66	0.76	0.89	0.70	11.23	0.86
	0.86	0.79	0.88	0.73	8.94	0.78
	Max:1.06	**0.80**	**0.86**	**0.76**	**8.78**	**0.70**
Outside	1.26	0.80	0.82	0.78	8.79	0.59
	1.4	0.80	0.80	0.80	8.96	0.62

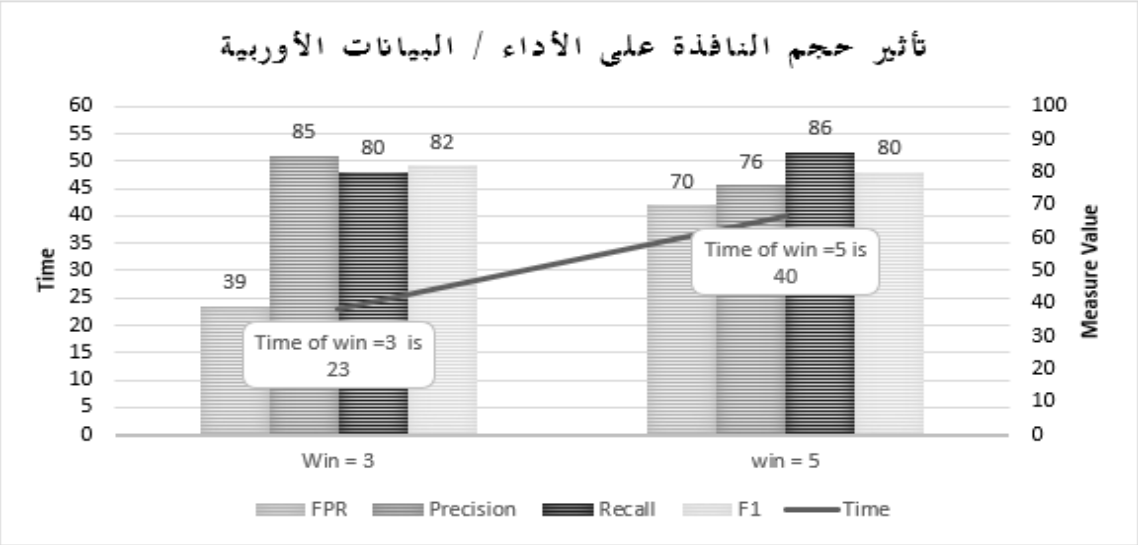
- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **89%**، عند العَتَبات ($0.26 \leq T \leq 0.66$)، أما أفضل قيمة للدقة (Precision) فهي **76%** عند العَتَبَة ($T = 1.06$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **70%** عند العَتَبَة ($T = 1.06$). إن أفضل

تفاضل بين هذه المقاييس هو عند العَتَبَة ($T = 1.06$)، إذ يستطيع النظام استرجاع **86%** ($Recall = 0.86$) من الحالات الشاذة، وبدقة جيدة بلغت **76%** ($Precision = 0.76$)، لكن بنسبة إنذارات كاذبة مرتفعة بلغت **70%** ($FPR = 0.70$). بلغ الزمن اللازم لتدريب النظام بالاعتماد على البارامترات الفائقة الأمثل **40** دقيقة.

يظهر بوضوح من خلال الجدول السابق عند اختبار أداء AEDTM–ADS باستخدام عتبات تصنيف تقع خارج المجال المحدد، تراجع أدائه مقارنةً مع استخدام عتبات من ضمن المجال، فمن أجل $T \leq 0.04$ تنخفض الدقة على نحوٍ كبير إلى **51%**. أما بالنسبة $T = 1.4$ ينخفض معدل الاسترجاع إلى **80%**. بالإضافة إلى أن نسبة الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل للنظام ($failure\ rate = 8.78$) عند العَتَبَة ($T = 1.06$).

من جهة أخرى، بمقارنة أداء AEDTM–ADS عند استخدام حجوم نافذة مختلفة، يتراجع أداؤه بشكل ملحوظ من أجل $m = 5$ عما هو عليه عند $m = 3$، إذ ينخفض معدل الدقة بنسبة **9%** (من 85% إلى 76%)، ويرتفع معدل الإيجابيات الخاطئة بنسبة **31%** (من 70% إلى 39%)، كما يزاد الزمن اللازم لتدريب النظام بنسبة **73.9%** (من 23د إلى 40د)؛ لذلك يفضل استخدام حجم نافذة 3. يوضح المخطط الآتي نتائج أداء النظام باستخدام حجوم النافذة المختلفة.



الشكل 7–9 تأثير حجم النافذة الزمنية على أداء AEDTM–ADS – البيانات الأوروبية

تؤكد نتائج هذه التجربة أن النظام الْمُقْتَرَح AEDTM–ADS، يسمح بفرض وجود علاقة مسبقة بين الأحداث بناء على ميزة الوقت "Time"، لذلك يمكن تطبيقه إذا كانت الأحداث مجمعة بطريقة ما، حتى لو كانت غير متسلسلة بدقة. استطاع النظام تحقيق نتائج مقبولة إلى حد ما، وذلك عند اعتماده على

عتبات تقع ضمن المجال المحدد. يلعب زيادة حجم النافذة في هذه التجربة، دوراً في تراجع أداء عمل النظام، نتيجةً لعدم وجود تسلسل واضح ودقيق بين الأحداث.

- **مجموعة بيانات كسر الورق**

يَهدِف تطبيق نظام AEDTM–ADS على مجموعة بيانات كسر الورق، إلى دراسة مدى فعالية النظام في تذكر الحالات الشاذة للأحداث المتسلسلة زمنياً على نحوٍ واضح، واكتشافها قبل حدوثها بوقت مناسب.

I. نمذجة النظام (AEDTM–ADS Modeling)

1. حجم النافذة الزمنية

كما هو موضح سابقاً يَتِمُّ تَعْيِين $m = 3$ في بداية عملية النمذجة ولذلك يكون النظام قادراً على التقاط التبعيات الزمنية للشَذُوذ ضِمْنَ 6 دقائق (نظراً لأنه يفصل بين القراءات دقيقتان)، ومع ازدياد حجم النافذة تزداد قدرة النظام على التقاط تلك التبعيات ضمن فترات أطول.

2. زمن الكشف

كما هو موضح سابقاً إن الكشف عن عملية كسر الورق قبل حدوثها بأربع دقائق يعتبر وقتاً كافياً لتفادي وقوع المشكلة، لذا تَمَّ تَعْيِين $s = 2$ ضِمْنَ المعادلة (3-6) من الفصل السادس، مع الانتباه إلى إنه يفصل بين كل قراءة دقيقتان.

3. ضبط البارامترات الفائقة

يوضح **الجدول 7–41** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 3$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.140)$، (انظر إلى السطر الأخير في الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **1.16** ساعة.

الجدول 7–40 نتائج البحث العشوائي لشبكة LSTM–AEDT عند حجم نافذة $m = 3$ – بيانات كسر الورق

Hyperparameters Configurations						MSE
Neurons	#Epochs	#Batch	Learn Rate	Dropout	Activation	
12	150	128	0.1	0.3	Tanh	0.541
8	200	256	0.001	0.5	Sigmoid	0.756
16	100	32	0.1	0.2	Sigmoid	0.537
32	50	128	0.01	0.0	Relu	0.147
8	75	64	0.001	0.3	Sigmoid	0.656
16	75	64	0.001	0.2	Relu	0.268
32	**200**	**256**	**0.001**	**0.0**	**Tanh**	**0.140**

يوضح **الجدول 7−42** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 5$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.172)$، (انظر إلى السطر الأول من الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **1.29** ساعة.

الجدول 7−41 نتائج البحث العشوائي لشبكة LSTM−AEDT عند حجم نافذة m = 5 – بيانات كسر الورق

Hyperparameters Configurations						MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation**	
32	**50**	**128**	**0.01**	**0.0**	**Relu**	**0.172**
16	200	64	0.0001	0.4	Sigmoid	0.643
8	150	256	0.0001	0.4	Tanh	0.652
12	50	64	0.1	0.2	Relu	0.853
32	200	256	0.001	0.1	Sigmoid	0.298
8	200	128	0.0001	0.3	Relu	0.525
32	100	256	0.1	0.2	Tanh	0.254

يوضح **الجدول 7−43** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 7$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.187)$، (انظر إلى السطر الأخير من الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **1.29**ساعة.

الجدول 7−42 نتائج البحث العشوائي لشبكة LSTM−AEDT عند حجم نافذة m = 7 – بيانات كسر الورق

Hyperparameters Configurations						MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation**	
12	50	256	0.001	0.4	Sigmoid	0.742
12	75	128	0.0001	0.3	Sigmoid	0.779
32	50	128	0.01	0.0	Relu	0.328
16	150	128	0.001	0.5	Sigmoid	0.529
8	200	64	0.1	0.3	Relu	1.027
12	200	256	0.01	0.0	Relu	0.342
32	**50**	**32**	**0.01**	**0.0**	**Tanh**	**0.187**

يوضح **الجدول 7−44** بعضاً من أهم نتائج البحث العشوائي عند حجم نافذة $m = 9$، ونتيجة لذلك يستخدم النظام من أجل هذه الحالة تكوينة البارامترات الفائقة التي تقابل $(MSE = 0.202)$، (انظر إلى السطر الأخير في الجدول الآتي). بلغ الزمن المستغرق لضبط البارامترات الفائقة **2.47** ساعة.

الجدول 7–43 نتائج البحث العشوائي لشبكة LSTM–AEDT عند حجم نافذة $m = 9$ – بيانات كسر الورق

Hyperparameters Configurations						MSE
Neurons	**#Epochs**	**#Batch**	**Learn Rate**	**Dropout**	**Activation**	
32	200	256	0.0001	0.0	Sigmoid	0.639
16	200	256	0.1	0.1	Sigmoid	0.561
12	200	256	0.0001	0.1	Relu	0.465
16	75	128	0.01	0.3	Sigmoid	0.397
12	75	64	0.001	0.0	Sigmoid	0.434
32	50	128	0.01	0.0	Relu	0.247
32	**50**	**32**	**0.001**	**0.2**	**Tanh**	**0.202**

4. معمارية الشبكة

تتكون شبكة LSTM–AEDT من طبقتي تشفير وطبقتي فك تشفير، بالإضافة إلى طبقة تسريب وطبقة مكرر المتجهة، أما طبقة الخرج فهي من النوع (Time Distributed). بالاعتماد على نتائج البحث العشوائي الموضحة أعلاه، وبالنظر إلى عدد العصبونات، وعلى نحوٍ مشابه لآلية ضبط حجم الطبقة في الحالات السابقة، تمَّ ضبط حجم الطبقة في هذه الحالة. يوضح الجدول الآتي أنواع طبقات الشبكة الْمُقْتَرَحة LSTM–AEDT مع عدد العصبونات لكل طبقة.

الجدول 7–44 بنية شبكة LSTM–AEDT – بيانات كسر الورق

Layer (type)	Output Shape
Input Layer	(-, win-size,59)
LSTM (Encoder-1)	(-, win-size,32)
Dropout Layer	(-, win-size,32)
LSTM (Encoder-2)	(-,16)
Repeat Vector Layer	(-, win-size,16)
LSTM (Decoder-1)	(-, win-size,16)
LSTM (Decoder-2)	(-, win-size,32)
Time Distributed (Output)	(-, win-size,59)

5. توزيع البيانات

بناءً على نتائج اختبار كولموغوروف سميرنوف على بيانات كسر الورق، والموضحة سابقاً في **الجدول 7–33**؛ إن البيانات لا تتبع توزيعاً طبيعياً، ولذلك يستخدم النظام نظرية تشيبيشيف لتحديد المجال الذي يقع ضمنه معظم البيانات.

II. أداء النظام (AEDTM–ADS Performance)

1. تفاضل العَتَبَة

a. من أجل حجم نافذة $m = 3$

يختار النظام من أجل حجم نافذة $m = 3$ عَتَبَة التصنيف التي يتُمَّ إيجادها على نحوٍ ديناميكي من ضمن المجال المحدد من قبلهِ $[0.2,1.85]$، إذ إن جميع قيم العتبات ضمن المجال مقبولة. يظهر **الجدول 7–46** أداء AEDTM–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن المجال المحدد وخارجه.

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **59%**، عند العَتَبَة ($T = 0.2$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **62%** عند العَتَبَة ($T = 1.85$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **9%** عند العَتَبَة ($T = 1.85$).

يحقق AEDTM–ADS أفضل تفاضل للعَتَبَة في أنظمة الكشف المبكر عن كسر الورق عند $T = 1.85$، إذ يستطيع كشف **52%** ($Recall = 0.52$) من حالات كسر الورق قبل حدوثها بأربع دقائق، وبدقة مقبولة تصل إلى **62%** ($Precision = 0.62$)، وبمعدل إنذارات كاذبة لا تتجاوز **9%** ($FPR = 0.9$)، زمن تدريب النظام بالاعتماد على البارامترات الفائقة الأمثل هو **2.5** دقيقة.

الجدول 7–45 نتائج أداء AEDTM–ADS عند حجم نافذة $m = 3$ – بيانات كسر الورق

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.05	0.52	0.55	0.53	80.04	1.0
	0.1	0.48	0.61	0.53	41.48	0.95
Inside	Min:0.2	0.54	0.59	0.54	16.95	0.74
	0.5	0.56	0.54	0.58	7.96	0.27
	0.8	0.53	0.52	0.56	7.41	0.18
	1.1	0.54	0.52	0.60	7.0	0.13
	1.4	0.54	0.52	0.59	6.92	0.11
	1.7	0.53	0.51	0.60	6.82	0.11
	Max:1.85	**0.54**	**0.52**	**0.62**	**6.69**	**0.09**
Outside	1.95	0.53	0.51	0.61	6.71	0.09
	2.0	0.53	0.51	0.61	6.71	0.09

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

تَمَّ اختبار AEDTM–ADS باستخدام عتبات تصنيف تقع خارج المجال المحدد. فمن أجل العتبات $T \leq 0.1$ يرتفع معدل الإيجابيات الخاطئة على نحوٍ كبير $(FPR \geq 95)$، وهذا مؤشر سَيِّئ للغاية في أنظمة كشف الشَذُوذ عامةً. أما بالنسبة $T \geq 1.95$ فينخفض معدل الاسترجاع إلى **51%** ومعدل الدقة إلى **61%**. بالإضافة إلى أن نسبة الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل $(failure\ rate = 6.69)$ عند العَتَبَة $(T = 1.85)$. إن أداء النظام يتراجع عند اعتماده على عتبات تقع خارج المجال مقارنةً بأدائه عند استخدام عتبات تصنيف من ضمن المجال المحدد، مما يؤكد على ضرورة اختيار عتبات ضمن المجال المحدد بشكل ديناميكي للتقليل من خسائر المشكلة.

b. من أجل حجم نافذة $m = 5$

يختار النظام من أجل حجم نافذة $m = 5$ عَتَبَة التصنيف التي يَتِمُّ إيجادها على نحوٍ ديناميكي من ضمن المجال المحدد من قبلهِ $[0.2,1.58]$؛ إن جميع قيم العتبات ضمن المجال مقبولة. يظهر الجدول الآتي أداء AEDTM–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن المجال المحدد وخارجه.

الجدول 7–46 نتائج أداء AEDTM–ADS عند حجم نافذة $m = 5$ – بيانات كسر الورق

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.05	0.51	0.52	0.53	90.52	1.0
	0.1	0.41	0.58	0.52	60.44	0.98
Inside	Min:0.2	0.53	0.61	0.54	23.13	0.84
	0.5	0.56	0.55	0.57	9.32	0.41
	0.8	0.56	0.53	0.58	7.58	0.22
	1.1	0.55	0.52	0.60	7.11	0.15
	1.4	0.54	0.52	0.60	6.98	0.10
	Max:1.58	**0.55**	**0.52**	**0.61**	**6.93**	**0.10**
Outside	1.7	0.54	0.52	0.60	6.95	0.11
	1.85	0.53	0.51	0.60	6.99	0.12

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **61%**، عند العَتَبَة ($T = 0.2$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **61%** عند العَتَبَة ($T = 1.58$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **10%** عند العَتَبَة ($T = 1.58$).

يحقق AEDTM–ADS أفضل تفاضل للعَتَبَة عند $T = 1.58$، إذ يستطيع كشف **52%** ($Recall = 0.52$) من حالات كسر الورق قبل حدوثها بأربع دقائق، وبدقة مقبولة تصل إلى **61%** ($Precision = 0.61$)، وبمعدل إنذارات كاذبة **10%** ($FPR = 0.10$)، علماً أن الزمن اللازم لتدريب النظام بالاعتماد على البارامترات الفائقة الأمثل هو **3.2** دقيقة. إن النظام من أجل حجم نافذة $m = 5$ ومع تراجع معدل الدقة بشكل طفيف، يحافظ على استقراره مقارنةً بحجم النافذة $m = 3$، لذلك لا بد من تجريب حجوم نافذة إضافية.

باختبار أداء AEDTM–ADS عند حجم نافذة $m = 5$، وباستخدام عتبات تصنيف تقع خارج المجال المحدد، يظهر بوضوح من خلال الجدول السابق تراجع أدائه مقارنةً باستخدام عتبات من ضمن المجال، فمن أجل $T \leq 0.1$ يرتفع معدل الإيجابيات الخاطئة بشكل كبير ($FPR \geq 98$). أما بالنسبة $T = 1.85$ ينخفض معدل الاسترجاع إلى 51%، ويرتفع معدل الإيجابيات الخاطئة إلى 12%. بالإضافة إلى أن نسبة الفشل للنظام عند تلك العتبات، أكبر من نسبة الفشل ($failure\ rate = 6.93$) عند العَتَبَة ($T = 1.58$).

c. من أجل حجم نافذة $m = 7$

يختار النظام من أجل حجم نافذة $m = 7$ عَتَبَة التصنيف التي يَتِمُّ إيجادها على نحوٍ ديناميكي من ضمن المجال المحدد من قبلهِ [0.2,1.63]؛ إن جميع قيم العتبات ضمن المجال مقبولة. يظهر أداء AEDTM–ADS في **الجدول 48–7** عند اختباره على قيم عتبات تصنيف T تقع ضمن وخارج المجال المحدد.

بالنظر إلى الجدول الآتي إن أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور تصل إلى **62%**، عند العَتَبَة ($T = 0.2$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **60%** عند العَتَبَة ($T = 1.63$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **9%** عند العَتَبَة ($T = 1.4$).

الجدول 7–47 نتائج أداء AEDTM–ADS عند حجم نافذة $m = 7$ – بيانات كسر الورق

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.05	0.51	0.52	0.53	88.32	1.0
	0.1	0.44	0.61	0.53	53.76	0.97
Inside	Min:0.2	0.54	0.62	0.54	21.21	0.82
	0.5	0.55	0.54	0.55	9.53	0.41
	0.8	0.55	0.53	0.57	8.18	0.28
	1.1	0.56	0.53	0.59	7.45	0.21
	1.4	**0.54**	**0.53**	**0.58**	**7.0**	**0.09**
	Max:1.63	0.54	0.52	0.60	6.96	0.12
Outside	1.7	0.52	0.51	0.58	7.01	0.12
	1.8	0.52	0.51	0.56	7.01	0.11

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

يحقق AEDTM–ADS أفضل تفاضل للعَتَبَة من أجل حجم نافذة $m = 7$ عند $T = 1.4$، إذ يستطيع كشف **53%** ($Recall = 0.53$) من حالات كسر الورق قبل حدوثها بأربع دقائق، وبدقة تصل إلى **58%** ($Precision = 0.58$)، وبمعدل إنذارات كاذبة **9%** ($FPR = 0.09$)، علماً أن الزمن اللازم لتدريب النظام بالاعتماد على البارامترات الفائقة الأمثل هو **5.3** دقيقة. إن النظام عند حجم نافذة $m = 7$ يظهر تفوقاً بمعدل الكشف بمقدار **1%** مقارنةً مع حجوم النافذة المختلفة.

تمَّ اختبار أداء AEDTM–ADS من أجل حجم نافذة $m = 7$ باستخدام عتبات تصنيف تقع خارج المجال المحدد، فمن أجل $T \leq 0.1$ يرتفع معدل الإيجابيات الخاطئة بشكل كبير ($FPR \geq 97$). أما عند $T \geq 1.7$ فينخفض معدل الاسترجاع إلى 51%، ويرتفع معدل الإيجابيات الخاطئة إلى **12%**. بالإضافة إلى أن نسبة الفشل عند تلك العتبات، أكبر من نسبة الفشل ($failure\ rate = 7.0$) عند العَتَبَة ($T = 1.4$)، لذلك يتراجع أداء النظام مقارنةً بأدائه باستخدام عتبات من ضمن المجال.

d. من أجل حجم نافذة $m = 9$

يختار النظام من أجل حجم نافذة $m = 9$ عَتَبَة التصنيف والتي تَمَّ إيجادها بشكل ديناميكي من ضمن المجال المحدد من قبلهِ [0.2,2.0]؛ إن جميع قيم العتبات ضمن المجال مقبولة. يوضح الجدول الآتي أداء AEDTM–ADS عند اختباره على قيم عتبات تصنيف T تقع ضمن المجال المحدد وخارجه.

الجدول 7−48 نتائج أداء AEDTM−ADS عند حجم نافذة $m = 9$ – بيانات كسر الورق

Range	Threshold	F1Score	Recall	Precision	Failure Rate (%)	FPR
Outside	0.05	0.51	0.53	0.52	86.16	1.0
	0.1	0.44	0.60	0.53	53.18	0.97
Inside	Min:0.2	0.53	0.60	0.54	21.19	0.81
	0.5	0.57	0.55	0.57	9.15	0.4
	0.8	0.56	0.53	0.59	7.72	0.24
	1.1	0.57	0.53	0.6	7.33	0.19
	1.4	0.56	0.53	0.61	7.12	0.16
	1.7	0.55	0.52	0.60	7.01	0.13
	Max:2.0	**0.52**	**0.51**	**0.57**	**7.06**	**0.12**
Outside	2.1	0.52	0.50	0.57	7.01	0.12
	2.5	0.51	0.50	0.56	7.01	0.11

- تشير inside إلى نتائج الاختبارات على قيم العتبات ضمن المجال الْمُقْتَرَح للعَتَبَة المقبولة
- تشير outside إلى نتائج الاختبارات على قيم العتبات خارج المجال المحدد (قبله وبعده)

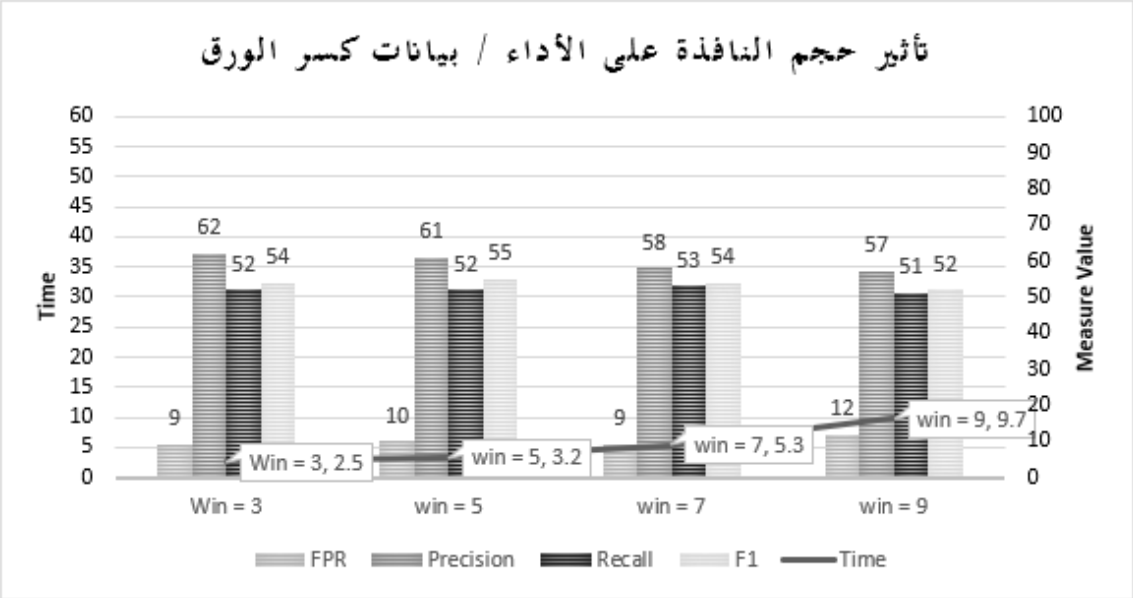
تصل أفضل قيمة لمقياس الاسترجاع (Recall) ضمن المجال المذكور إلى **60%**، عند العَتَبَة ($T = 0.2$)، أما أفضل قيمة للدقة (Precision) فتصل إلى **61%** عند العَتَبَة ($T = 1.4$)، بينما كانت أقل نسبة لمعدل الإيجابيات الخاطئة (FPR) هي **12%** عند العَتَبَة ($T = 2.0$).

يحقق AEDTM−ADS أفضل تفاضل للعَتَبَة من أجل حجم نافذة $m = 9$ عند $T = 2.0$، إذ يستطيع كشف **51%** ($Recall = 0.51$) من حالات كسر الورق قبل حدوثها بأربع دقائق، وبدقة تصل إلى **57%** ($Precision = 0.57$)، وبمعدل إنذارات كاذبة **12%** ($FPR = 0.12$)، علماً أن الزمن اللازم لتدريب النظام بالاعتماد على البارامترات الفائقة الأمثل هو **9.7** دقيقة. إن النظام عند حجم نافذة $m = 9$ يتراجع أداؤه مقارنةً بحجم النافذة السابقة، إذ ينخفض معدل الكشف بمقدار **2%**، ويرتفع معدل الإيجابيات الخاطئة بمقدار **3%**، كما يزداد زمن تدريب النظام بنسبة مرتفعة **83%** (حوالي 4.4د: من 5.3د إلى 9.7د)؛ ونتيجةً لذلك تمّ التوقف عن زيادة حجم النافذة عند هذا الحد.

يظهر بوضوح من خلال الجدول تراجع أداء AEDTM−ADS من أجل حجم نافذة $m = 9$ باستخدام عتبات تصنيف تقع خارج المجال المحدد، فمن أجل $T \leq 0.1$ يرتفع معدل الإيجابيات الخاطئة

على نحوٍ كبير ($FPR \geq 97$). أما بالنسبة إلى $T \geq 2.1$ فينخفض معدل الاسترجاع إلى **50%**، لذلك يتراجع أداء النظام مقارنةً بأدائه عند استخدام عتبات من ضمن المجال.

يوضح المخطط الآتي تأثير حجوم النافذة الزمنية على أداء AEDTM–ADS في الكشف المبكر عن الشَذُوذ (كسر الورق).



الشكل 7–10 تأثير حجم النافذة الزمنية على أداء AEDTM–ADS – بيانات كسر الورق

يظهر من خلال الشكل السابق أن لحجم النافذة دوراً مهماً في تَحسين أداء AEDTM–ADS، لكن من جهة أخرى، يجب المحافظة على حَدّ مُعيّن لحجم النافذة، إذ إن النموذج يسلك سلوكاً عكسياً بعد حجم مُعيّن. حَقَّقَ نظام الكشف الْمُقْتَرَح أفضل أداء له من أجل حجم نافذة $m = 7$ ، من حيث نسبة الكشف ($Recall = 53\%$)، والإيجابيات الخاطئة ($FPR = 9\%$). بينما سلك النموذج بعد حجم نافذة $m = 7$ سلوكاً معاكساً، فمن أجل حجم نافذة $m = 9$، اِنخَفَضَت نسبة الكشف بمقدار **2%** وبلغت **51%** (من 53% إلى 51%)، واِرْتَفَعَت الإيجابيات الخاطئة بمقدار **3%** وبلغت **12%** (من 9% إلى 12%). كما يزداد زمن تدريب النظام بنسبة **83%** (من 5.3د إلى 9.7د)؛ إن زمن التدريب يشكل أحد القيود الرئيسية في زيادة حجم النافذة.

2. تحليل التكاليف والفوائد (Cost Benefit Analysis)

يُبيّن **الجدول 7–50** مقدار الخسارة الذي يوفره النموذج الْمُقْتَرَح من أجل حجم نافذة $m = 7$ في كل عام. نُلَاحظ أن AEDTM–ADS اِستَطاعَ مع عدد ليس بالكبير من عمليات الكشف المبكر، أن

يوفر قدراً كبيراً من تكاليف الخسارة وصلت لحوالي 8 ملايين دولار سنوياً عن كل خط إنتاج، وبمعدل **54%** من الخسارة الإجمالية.

الجدول 7-49 تحليل التكلفة والفائدة لنظام AEDTM-ADS- بيانات كسر الورق

Item	Gain (by TPR)	Loss (by FPR)	Remark
تكلفة	10,000$	100$	-
عدد الحالات	124x12month=1488	(2 minx30x24 hr.x365 d)-1488=524112	1 year
معدل الحالات	Recall=53%	FPR=9%	Test Result
تكلفة/ سنة	7,886,400$	-47,170$	
الإجمالي	7,839,230$		

بناءً على نتائج هذه التجربة، يمكن استخدام النظام الْمُقْتَرَح AEDTM-ADS، لالتقاط التبعيات الزمنية لتسلسل الشُّذُوذ ضمن سلاسل البيانات. إن النظام من أجل حجم نافذة $\boldsymbol{m = 7}$، وعند اعتماده على عتبات تقع ضمن المجال المحدد [0.2,1.63]، حقق نتائج مقبولة بالنسبة إلى مشكلة كسر الورق، إذ كشف **53%** من حالات الكسر قبل 4 دقائق من حدوثها، وبنسبة إيجابيات خاطئة لا تتجاوز **9%** عند العَتَبَة ($T = 1.4$)، بينما بلغت نسبة الحد من الخسائر الناتجة عن هذه المشكلة **54%**.

تؤكد نتائج التجارب التي أجرتها الدراسة، قدرة النظام الْمُقْتَرَح على تحديد عَتَبَة التصنيف ديناميكياً، والتعامل مع حالات الشُّذُوذ المختلفة. بالإضافة إلى قدرته على اختيار قِيَم البارامترات الفائقة الأفضل، والميزات الأكثر أهمية في عملية الكشف.

استطاع AEDT-ADS عند اختباره على مجموعة الاحتيال الأوربية، والتي تصنف معظم حالاتها الاحتيالية على أنها شُذُوذ النقطة، اكتشاف نسبة عالية من الحالات الشاذة (الاحتيالية) بلغت **90%** ($Recall = 0.9$)، وبدقة كبيرة تصل إلى **94%** ($Precision = 0.94$)، وبمعدل إنذارات كاذبة لا تتجاوز **9%** ($FPR = 0.09$)، وذلك عند اعتماده على عَتَبَة التصنيف المحددة من قبل النظام. كما استطاع AEDTM-ADS تذكر والتقاط التبعيات الزمنية لتسلسل الحالات الشاذة ضمن شُذُوذ السياق، إذ إن النظام عند اختباره على مجموعة بيانات كسر الورق، تمكن من اكتشاف **53%** من الحالات

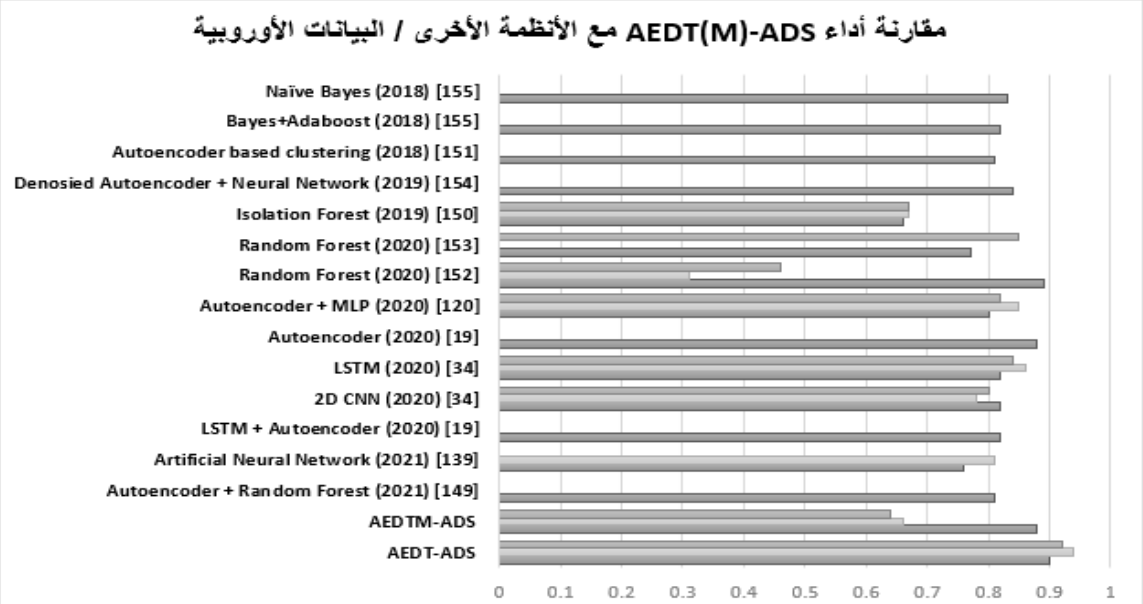
الشاذة قبل حدوثها بأربع دقائق، وبمعدل إنذارات كاذبة لا تتجاوز **9%** ($FPR = 0.09$)، والحد من الخسائر الناتجة عن كسر الورق بنسبة **54%**.

مما سبق يفضل استخدام النظام بحالته من دون ذاكرة عند التعامل مع حالات شذوذ النقطة، بينما يفضل استخدام النظام مع ذاكرة عند التعامل مع شذوذ السياق.

7-2-3- مقارنة أداء نظام كشف الشُّذُوذ الْمُقْتَرَح مع الأنظمة الأخرى

- **مجموعة بيانات الاحتيال الأوروبية**

يوضح المخطط الآتي، تفوق نظام كشف الشُّذُوذ الْمُقْتَرَح AEDT-ADS على الأنظمة الأخرى. إن نسبة كشف الحالات الشاذة للنظام الْمُقْتَرَح، ارتفعت بمقدار **2%** وحتى **36%** مقارنةً بباقي الأنظمة. بالإضافة إلى أن جميع هذه الأنظمة استخدمت عَتَبَة تصنيف ثابتة. كما يُبَيِّن المخطط ضرورة استخدام النظام بحالته من دون ذاكرة (AEDT-ADS)، عند التعامل مع بيانات يَغلُب عليها شُذُوذ النقطة.

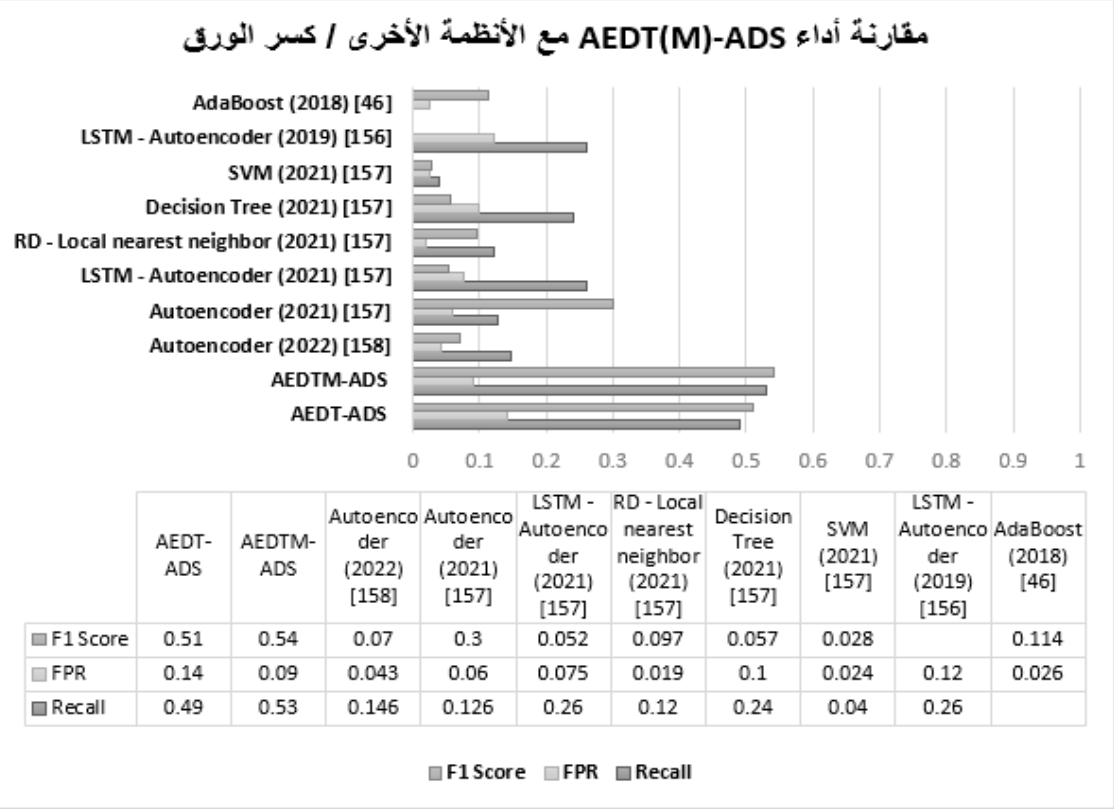


	AEDT-ADS	AEDTM-ADS	Autoencoder + Random Forest (2021) [149]	Artificial Neural Network (2021) [139]	LSTM + Autoencoder (2020) [19]	2D CNN (2020) [34]	LSTM (2020) [34]	Autoencoder (2020) [19]	Autoencoder + MLP (2020) [120]	Random Forest (2020) [152]	Random Forest (2020) [153]	Isolation Forest (2019) [150]	Denosied Autoencoder + Neural Network (2019) [154]	Autoencoder based clustering (2018) [151]	Bayes+Adaboost (2018) [155]	Naïve Bayes (2018) [155]
F1 Score	0.92	0.64				0.8	0.84		0.82	0.46	0.85	0.67				
Precision	0.94	0.66		0.81		0.78	0.86		0.85	0.31		0.67				
Recall	0.9	0.88	0.81	0.76	0.82	0.82	0.82	0.88	0.8	0.89	0.77	0.66	0.84	0.81	0.82	0.83

الشكل 7-11 مقارنة أداء AEDT(M)-ADS بالأنظمة الأخرى – البيانات الأوروبية: المصدر الدراسة الحالية

- **مجموعة بيانات كسر الورق**

يوضـــح المخطط الآتي، تفوق نظام كشــف الشُّــذُوذ الْمُقْتَرَح AEDTM–ADS على الأنظمة الأخرى. ومع ارتفاع معدل الإيجابيات الخاطئة للنظام الْمُقْتَرَح بنســـب تراوحت من **2%** إلى **5%**، ارتفعت نسبة كشف الحالات الشاذة بمقدار **27%** على الأقل مقارنةً بباقي الأنظمة. بالإضـافة إلى أن جميع هذه الأنظمة استخدمت عَتَبَة تصنيف ثابتة. كما يُبَيِّن المخطط ضرورة استخدام النظام بحالته مع ذاكرة (AEDTM–ADS)، عند التعامل مع بيانات السلاسل الزمنية الشاذة (شُذُوذ السياق).



	AEDT-ADS	AEDTM-ADS	Autoencoder (2022) [158]	Autoencoder (2021) [157]	LSTM - Autoencoder (2021) [157]	RD - Local nearest neighbor (2021) [157]	Decision Tree (2021) [157]	SVM (2021) [157]	LSTM - Autoencoder (2019) [156]	AdaBoost (2018) [46]
F1 Score	0.51	0.54	0.07	0.3	0.052	0.097	0.057	0.028		0.114
FPR	0.14	0.09	0.043	0.06	0.075	0.019	0.1	0.024	0.12	0.026
Recall	0.49	0.53	0.146	0.126	0.26	0.12	0.24	0.04	0.26	

الشكل 7–12 مقارنة أداء AEDT(M)–ADS بالأنظمة الأخرى – بيانات كسر الورق

المصدر الدراسة الحالية

الفصل الثامن

الخاتمة والدراسات المستقبلية

8-1- الخاتمة والاستنتاجات

أَصْبَحَ واضحاً من خلال ما قدمتهُ الدراسة الحالية، أنه من المهم جداً في أثناء عملية تحليل البيانات اكتشاف السلوكيات غير الطبيعية ضِمْنَ النظام المدروس. إن هذه السلوكيات تُدلُّ إمَّا على تلاعب من قبل شخص أو جهة مجهولة للحصول على فوائد ومكاسب من النظام بطرق غير شرعية، أو على وجود خلل مَا ضِمْنَ النظام.

تَعدُّ أدوات وأنظمة الْكَشْف عَنِ الشُّذُوذ من أهم الوسائل لاكتشاف هذه الحالات المغايرة للسلوك الطبيعي وفقاً لعمل النظام المدروس. تُعْتَبِرُ طرائق تَعَلُّم الآلة بشقيها الكلاسيكي والعميق من أهم طرائق الكشف استناداً لمّا تَمَّ الإشارة إليه ضِمْنَ أدبيات الدراسات المرجعية.

تُوَاجِه أنظمة كَشْف الشُّذُوذ الحالية وفقاً للدراسات السابقة مجموعة مَنِ التَّحَدِّيَات، ومن أهمها دراسة الميزات الأكثر أهمية في اكتشاف الحالات الشَّاذَّةِ واختيار قَيِّم البارامترات الفائقة الأمثل؛ إضافةً إلى تحديد عَتَبَةِ التَّصْنِيفِ بشكل ديناميكي.

تَلَخَّصت المساهمة المقدمة ضِمْنَ هذه الدراسة في ثلاثة اتجاهات: **الأول**، في تحليل عمل أنظمة كشف الشُّذُوذ، والوصول إلى المنهجية الأفضل لبنائها والتي تساهم في تحسين أدائها. **الثاني**، في بناء نظام متكامل لكشف الشُّذُوذ في البيانات قادر على تحديد عَتَبَة التَّصْنِيف ديناميكياً، واكتشاف الميزات غير المرتبطة خطياً واختيار قَيِّم البارامترات الفائقة. **الثالث**، تطوير واجهات تخاطبية للنظام الْمُقْتَرَح لبيان إمكانية استثماره مباشرةً في أي تطبيق من تطبيقات العالم الحقيقي بعد ملاءمته ليناسب البيانات المدخلة.

- **تحليل أنظمة كشف الشذوذ**

تَوَصَّلَت الدِّرَاسَة من خلال هذا الاتجاه إلى أن أفضل أداء لأنظمة كشف الشذوذ، يكون عند اختيار الميزات الأكثر أهمية متبوعاً بضبط البارامترات الفائقة. اعتَمَدَت الدِّرَاسَة لتحليل أداء هذه الأنظمة على سيناريوهين يختلفان بترتيب إِجْرَاءات ضبط البارامترات الفائقة واختيار الميزات الأكثر أهمية. إذ كان الترتيب في السيناريو الأول هو: ضبط البارامترات الفائقة ثُمَّ اختيار الميزات الأكثر أهمية، بينما كان الترتيب في السيناريو الثاني هو: اختيار الميزات الأكثر أهمية ثُمَّ ضبط البارامترات الفائقة.

اِسْتَخْدَمَت الدِّرَاسَة ضِمْنَ هذا الاتجاه خوارزميتي الغابات العشوائية وآلة شعاع الدعم كطرائق كشف شذوذ. أظهرت التجارب العملية لاختبار هذه الأنظمة على مجموعات خاصة بالشُّذُوذ، **أن اختيار الميزات الأكثر أهمية ضمن مجموعة البيانات متبوعاً بضبط البارامترات الفائقة**، يُسهم في تَقَلّص كُلٌّ من الزمن المستغرق لبناء هذه الأنظمة بِنِسَبٍ تراوحت بين **51.5%** و**60.2%**، ومعدل الإيجابيات الخاطئة (FPR) بين **1%** و**35%**، بالإضافة إلى زيادة في كشف الحالات الشاذة بين **1%** و**6%** بالنظر إلى مساحة السطح تحت منحني الدقة والاسترجاع (AUCPR)، كما أن هناك تحسيناً في معظم قيم مقاييس الأداء. مِمَّا يُؤَكِّد على التحسين الحاصل لأداء أنظمة كشف الشُّذُوذ عند اعتماد الترتيب المذكور.

فِيمَا يَلِي عَرْض للتوليفات الْأَفْضَل من الميزات الأكثر أهمية وقيم البارامترات الفائقة لِكُلِّ خوارزمية:

– خوارزمية الغابات العشوائية

- **البيانات الأوروبية**

Features:	$\{V14, V4, V10, V12, V17, V3\}$
Hyperparameters:	$\{max_depth: 150,\ min_samples_split: 2,\ n_estimators: 250,\ max_features: \sqrt{6},\ min_samples_leaf: 1,\ bootstrap: \text{True}\}$

- **البيانات المجردة**

Features:	$\{Total\ Number\ of\ declines/days, Transaction\ amount, Is\ Foreign\ Transaction?\ Is\ High\ Risk\ Country?\}$
Hyperparameters:	$\{max_depth: 10,\ min_samples_split: 5,\ n_estimators: 100,\ max_features: \sqrt{4},\ min_samples_leaf: 1,\ bootstrap: \text{True}\}$

– خوارزمية آلة شعاع الدعم

- **البيانات الأوروبية**

Features:	$\{V14, V4, V10, V12, V17, V3\}$
Hyperparameters:	$\{regularization: 1000,\ gamma: 1e{-}2,\ kernel: rbf\}$

- **البيانات المجردة**

Features:	$\{Total\ Number\ of\ declines/days, Transaction\ amount, Is\ Foreign\ Transaction?\ Is\ High\ Risk\ Country?\}$
Hyperparameters:	$\{regularization: 50,\ gamma: 1e{-}2,\ kernel: rbf\}$

- **تطوير نظام كشف شذوذ ديناميكي**

بَيَّنَتْ هذه الدراسة من خلال ما قَدَّمَتهُ من مسح شامل للدراسات المرجعية، تَفَوُّق أنظمة كشف الشُّذُوذ العميقة (القائمة على طرائق التَعلُّم العميق) على باقي الأنظمة. بالمقابل تُعَاني هذه الأنظمة من مجموعة من التَّحَدِّيَاتِ، لعلَّ من أهمها تحديد عَتَبَة التَّصْنِيف على نحوٍ ديناميكي يتلاءم مع تغير السلوكيات غير الطبيعية بمرور الوقت، إضافةً إلى اختيار الميزات الأكثر أهمية وَقِيَم البارامترات الفائقة.

قَدَّمت الدراسة الحالية نسخة مُعَدَّلَة من شبكة الترميز الآلي (Autoencoder)، تَتَمَتَّع بقدرتها على تحديد عَتَبَة الْكَشْف على نحوٍ ديناميكي. سُمِّيت النسخة المعدلة شبكة الترميز الآلي مع عَتَبَة ديناميكية (AEDT: Auto–Encoder with a Dynamic Threshold). إن الفكرة الرئيسية لعمل الخوارزمية المقترحة هي نمذجة خصائص البيانات الطبيعية أولاً، ومن ثم حساب عتبة التصنيف ديناميكياً بناءً على نوع التوزيع الاحتمالي لخطأ إعادة البناء للبيانات الطبيعية. يحدد نوع التوزيع الإجراء اللازم لإيجاد المجال الذي تقع ضمنه معظم قِيَم متجهة الخطأ للبيانات الطبيعية. تستخدم AEDT القاعدة التجريبية (Empirical Rule) من أجل التوزيع الطبيعي، أما فيما عدا ذلك فإنها تستخدم نظرية تشيبيشيف (Chebyshev's Theory) كطريقة غير معلميه.

أُسْتُخدِمْت خوارزمية الكشف المقترحة AEDT لبناء نظام كشف شذوذ ديناميكي AEDT–ADS، يمكنه التعامل بكفاءة مع البيانات عالية الأبعاد وإنشاء تمثيل للبيانات بِبُعد أقل، مع القدرة على اكتشاف الميزات غير المرتبطة خطياً، وتحديد البارامترات الفائقة أوتوماتيكياً. ومن جهة أخرى يستخدم عَتَبَة تصنيف ديناميكية قادرة على التكيف مع تباين البيانات بمرور الوقت. بهدف تَمْكِينِ النظام من تذكر الحالات السياقية للبيانات الشاذة، تَمَّ إضافة وحدة الذاكرة طويلة المدى (LSTM) إلى بنية النظام، وَرُمِزَ من أجل هذه الحالة بـ AEDTM–ADS. إن تفعيل وحدة الذاكرة أو الغاؤها يَعْتَمِد على مُقْتَضَيَات الحالة المدروسة.

تَمَّ اختبار النظام الْمُقْتَرَح بحالتيه مع ذاكرة ومن دونها على اثنين من تطبيقات الشُّذُوذ الأكثر أهمية في العالم الحقيقي، وهما كشف الاحتيال المالي وكشف العيوب الصناعية.

1. كشف الاحتيال المالي

بَيَّنَت الدراسة من خلال هذا التطبيق مدى فعالية النظام الْمُقْتَرَح في اكتشاف حالات شُذُوذ النقطة من جهة، ومن جهة أخرى اكتشاف الأحداث المجمعة بطريقة غير مُتَسَلْسِلَة بوضوح.

أَكَّدَتْ نتائج التجربة التي أُجْرِيَت على مجموعة البيانات الخاصة بهذا التطبيق، قدرة النظام الْمُقْتَرَح على التعامل بكفاءة مع حالات شُذُوذ النقطة. فاستطاع النظام AEDT–ADS كشف الحالات الشاذة

بنسبة **%90** ($Recall = 0.9$)، وبدقة كبيرة تصل إلى **%94** ($Precision = 0.94$)، وبمعدل إنذارات كاذبة لا تتجاوز **%9** ($FPR = 0.09$)، عند عَتَبَة التصنيف المختارة ديناميكياً $T = 2.84$.

كما تشير نتائج التجربة إلى إمكانية استخدام نظام الكشف الْمُقْتَرَح عند تفعيل وحدة الذاكرة في حال كانت الأحداث مجمعة بطريقة غير مُتَسَلْسِلَة بوضوح. إذ استطاع النظام AEDTM–ADS كشف الحالات الشاذة بنسبة **%80** ($Recall = 0.8$)، وبدقة تصل إلى **%85** ($Precision = 0.85$)، وبمعدل إنذارات كاذبة **%39** ($FPR = 0.39$)، عند عَتَبَة التصنيف المختارة ديناميكياً $T = 0.92$، وحجم نافذة $m = 3$.

فِيمَا يَلِي عَرَّضَ لإعدادات AEDT–ADS التي حقق أفضل النتائج عندها:

Features:	$\{\boldsymbol{V26}, \boldsymbol{V13}, \boldsymbol{V18}, \boldsymbol{V15}, \boldsymbol{V24}\}$
Hyperparameters:	$\{neurons$: **20**, n_epochs: **50**, n_batch: **64**, lr: **0.0001**, $dropout$: **0**, $activation$: **Tanh**, $out_activation$: **Linear**$\}$
Threshold:	T: 2.84

2. كشف العيوب الصناعية (مشكلة كسر الورق)

بَيَّنَت الدراسة من خلال هذا التطبيق مدى فعالية النظام الْمُقْتَرَح في تذكر الحالات الشاذة للأحداث المُتَسَلْسِلَة زمنياً على نحوٍ واضح، واكتشافها قبل حدوثها بوقت مناسب.

أَكَّدَتْ نتائج التجربة التي أُجْرِيَت على مجموعة البيانات الخاصة بهذا التطبيق، قدرة النظام الْمُقْتَرَح على التقاط التبيعات الزمنية لتسلسل الشذوذ واكتشافها قبل حدوثها بوقت مناسب. إذ بَلَغَت نسبة الكشف للنظام AEDTM–ADS **%53** من الحالات قبل حدوثها بأربع دقائق، وبنسبة إنذارات خاطئة لم تتجاوز **%9**. كما اِستَطاعَ الحد من الخسارة الإجمالية لِكُلّ خط إنتاج، بحوالي 8 ملايين دولار سنوياً وبمعدل **%54**. وذلك من أجل عَتَبَة التصنيف المختارة ديناميكياً ($T = 1.4$)، وحجم نافذة $m = 7$.

بالإضافة إلى ذلك، أَظْهَرَت النتائج إمكانية استخدام النظام الْمُقْتَرَح من دون ذاكرة، كطريقة سريعة في تحديد الحالات الشاذة ضمن السلاسل الزمنية، من خلال تدريب النظام على السلاسل الطبيعية وإعادة بنائها بطريقة صحيحة. بَلَغَت نسبة الكشف للنظام AEDT–ADS **%49**، وبنسبة إنذارات خاطئة **%14**، بينما بَلَغَتْ نسبة الحد من تكاليف الخسار **%46**، عند عَتَبَة التصنيف المختارة ديناميكياً ($T = 1.4$).

فِيمَا يَلِي عَرّض لإعدادات AEDTM–ADS التي حقق أفضل النتائج عندها:

Features:	$\{x3, x19, x4, x42\}$
Hyperparameters:	$\{neurons: 32,\ n_epochs: 50,\ n_batch: 32,\ lr: 0.01,\ dropout: 0,\ activation:$ **Tanh**$\}$
Threshold:	$T: 1.4$
Window Size:	$m = 7$

كما بَيَّنَتْ النتائج التي تَمَّ الحصول عليها في الدراسة الحالية، تفوق النظام الْمُقْتَرَح على أنظمة كشف الشذوذ الأخرى. فمن أجل مجموعة البيانات الخاصة بالاحتيال المالي، ارْتَفَعَت نسبة كشف الشُّذُوذ (الاحتيال) بمقدار **2%** إلى **36%**. كذلك ارتفعت نسبة الكشف بمقدار **27%** على الأقل بالنسبة إلى مجموعة البيانات الصناعية (كسر الورق). مِمَّا يُؤَكِّد على تفوق النظام الْمُقْتَرَح على باقي الأنظمة الأخرى، فضلاً عن قدرة النظام على حساب عتبة التصنيف ديناميكياً.

في الختام يكمن تلخيص الاستنتاجات التي توصلت إليها الدراسة الحالية وفق الآتي:

1) يُساهم اختيار الميزات الأكثر أهمية ضمن مجموعة البيانات متبوعاً بضبط البارامترات الفائقة في تحسين أداء أنظمة كشف الشذوذ الكلاسيكية على نحوٍ كبير من حيث دقة الكشف وزمن التدريب.
2) اقتراح طريقة كشف (AEDT) قادرة على حساب عَتَبَة التصنيف ديناميكياً، على نحوٍ يتلاءم مع تغير السلوكيات غير الطبيعية بمرور الوقت، ومن دون وضع فرضيات حول حجم البيانات وتوزيعها.
3) تطوير نظام كشف شذوذ AEDT(M)–ADS يتمتع بـ:
   I. التعامل مع البيانات عالية الأبعاد واختزالها في بُعد أقل.
   II. اختيار الميزات الأكثر أهمية.
   III. اختيار قَيّمِ البارامترات الفائقة أوتوماتيكياً.
   IV. حساب عَتَبَة التصنيف ديناميكياً.
   V. التعامل مع أنواع الشذوذ (شذوذ نقطة – شذوذ السياق).
4) تفوق النظام المقترح على الأنظمة الأخرى.
   I. ارْتَفَعَت نسبة الكشف من **2%** إلى **36%** في تطبيق اكتشاف الاحتيال المالي.
   II. ارْتَفَعَت نسبة الكشف بمقدار **27%** على الأقل في تطبيق اكتشاف كسر الورق.

8-2- الدراسات المستقبلية

بناءً على التَّجَارِب الَّتِي تَوَصَّلَتْ إِلَيْهَا الدِّرَاسَة، يُمْكِن أَنْ تقترح ما يلي:

1. استخدام تقنيات تحويل البيانات (Data Transformation)، بهدف تحويل توزيع متجهات الخطأ إلى توزيع طبيعي. ومن ثَمَّ تخفيف هامش الخطأ الناتج عن الأساليب غير المعلميه
2. تحديد حجوم النوافذ الزمنية على نحوٍ ديناميكي.

قائمة المراجع

[1] J. Bulao, "How Much Data Is Created Every Day in 2022?," *Techjury*, 2022. https://techjury.net/blog/how-much-data-is-created-every-day/ (accessed Jun. 30, 2022).

[2] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15:1-15:58, Jul. 2009, doi: 10.1145/1541880.1541882.

[3] H. Zenati, M. Romain, C. S. Foo, B. Lecouat, and V. R. Chandrasekhar, "Adversarially Learned Anomaly Detection," *ArXiv181202288 Cs Stat*, Dec. 2018, Accessed: Mar. 29, 2022. [Online]. Available: http://arxiv.org/abs/1812.02288

[4] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep Learning for Anomaly Detection: A Review," *ACM Comput. Surv.*, vol. 54, no. 2, p. 38:1-38:38, Mar. 2021, doi: 10.1145/3439950.

[5] "An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems - Ye - 2001 - Quality and Reliability Engineering International - Wiley Online Library." https://onlinelibrary.wiley.com/doi/abs/10.1002/qre.392 (accessed Mar. 29, 2022).

[6] T.-Y. Kim and S.-B. Cho, "Web traffic anomaly detection using C-LSTM neural networks," *Expert Syst. Appl.*, vol. 106, pp. 66–76, Sep. 2018, doi: 10.1016/j.eswa.2018.04.004.

[7] Bharadwaj, K. B. Prakash, and G. R. Kanagachidambaresan, "Pattern Recognition and Machine Learning," in *Programming with TensorFlow: Solution for Edge Computing Applications*, K. B. Prakash and G. R. Kanagachidambaresan, Eds. Cham: Springer International Publishing, 2021, pp. 105–144. doi: 10.1007/978-3-030-57077-4_11.

[8] G. S. Budhi, R. Chiong, and Z. Wang, "Resampling imbalanced data to detect fake reviews using machine learning classifiers and textual-based features," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 13079–13097, Apr. 2021, doi: 10.1007/s11042-020-10299-5.

[9] A. Zimek, E. Schubert, and H.-P. Kriegel, "A survey on unsupervised outlier detection in high-dimensional numerical data," *Stat. Anal. Data Min. ASA Data Sci. J.*, vol. 5, no. 5, pp. 363–387, 2012, doi: 10.1002/sam.11161.

[10] G. Pang, L. Cao, L. Chen, D. Lian, and H. Liu, "Sparse Modeling-Based Sequential Ensemble Learning for Effective Outlier Detection in High-Dimensional Numeric Data," *Proc. AAAI Conf. Artif. Intell.*, vol. 32, no. 1, Art. no. 1, Apr. 2018, doi: 10.1609/aaai.v32i1.11692.

[11] G. Pang, L. Cao, and C. Aggarwal, "Deep Learning for Anomaly Detection: Challenges, Methods, and Opportunities," in *Proceedings of the 14th ACM International Conference on Web Search and Data Mining*, New York, NY, USA, Mar. 2021, pp. 1127–1130. doi: 10.1145/3437963.3441659.

[12] G. Pang, L. Cao, L. Chen, and H. Liu, "Learning Representations of Ultrahigh-dimensional Data for Random Distance-based Outlier Detection," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, New York, NY, USA, Jul. 2018, pp. 2041–2050. doi: 10.1145/3219819.3220042.

[13] M.-N. Nguyen and N. A. Vien, "Scalable and Interpretable One-Class SVMs with Deep Learning and Random Fourier Features," in *Machine Learning and Knowledge Discovery in Databases*, Cham, 2019, pp. 157–172. doi: 10.1007/978-3-030-10925-7_10.

[14] B. Zong *et al.*, "DEEP AUTOENCODING GAUSSIAN MIXTURE MODEL FOR UNSUPERVISED ANOMALY DETECTION," p. 19, 2018.

[15] S. Ustebay, Z. Turgut, and M. A. Aydin, "Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier," in *2018*

International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Dec. 2018, pp. 71–76. doi: 10.1109/IBIGDELFT.2018.8625318.

[16] M. Oh and G. Iyengar, "Sequential Anomaly Detection using Inverse Reinforcement Learning," Apr. 2020, doi: 10.48550/arXiv.2004.10398.

[17] T. Chen, L.-A. Tang, Y. Sun, Z. Chen, and K. Zhang, "Entity Embedding-based Anomaly Detection for Heterogeneous Categorical Events." arXiv, Aug. 26, 2016. doi: 10.48550/arXiv.1608.07502.

[18] P. Lin, K. Ye, and C.-Z. Xu, "Dynamic Network Anomaly Detection System by Using Deep Learning Techniques," in *Cloud Computing – CLOUD 2019*, Cham, 2019, pp. 161–176. doi: 10.1007/978-3-030-23502-4_12.

[19] C. Nordling, *Anomaly Detection in Credit Card Transactions using Autoencoders*. 2020.

[20] T. P. Quinn, T. Nguyen, S. C. Lee, and S. Venkatesh, "Cancer as a Tissue Anomaly: Classifying Tumor Transcriptomes Based Only on Healthy Data," *Front. Genet.*, vol. 10, 2019, Accessed: May 27, 2022. [Online]. Available: https://www.frontiersin.org/article/10.3389/fgene.2019.00599

[21] H. D. Nguyen, K. P. Tran, S. Thomassey, and M. Hamad, "Forecasting and Anomaly Detection approaches using LSTM and LSTM Autoencoder techniques with the applications in supply chain management," *Int. J. Inf. Manag.*, vol. 57, p. 102282, Apr. 2021, doi: 10.1016/j.ijinfomgt.2020.102282.

[22] A. Cutler, D. R. Cutler, and J. R. Stevens, "Random Forests," in *Ensemble Machine Learning: Methods and Applications*, C. Zhang and Y. Ma, Eds. Boston, MA: Springer US, 2012, pp. 157–175. doi: 10.1007/978-1-4419-9326-7_5.

[23] O. Mbaabu, "Introduction to Random Forest in Machine Learning | Engineering Education (EngEd) Program | Section," 2020. https://www.section.io/engineering-education/introduction-to-random-forest-in-machine-learning/ (accessed May 23, 2022).

[24] R. Primartha and B. A. Tama, "Anomaly detection using random forest: A performance revisited," in *2017 International Conference on Data and Software Engineering (ICoDSE)*, Nov. 2017, pp. 1–6. doi: 10.1109/ICODSE.2017.8285847.

[25] "sklearn.ensemble.RandomForestClassifier — scikit-learn 1.1.1 documentation." Accessed: May 23, 2022. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html

[26] F. Cady, "The Data Science Handbook | Wiley Online Books," 2017. https://onlinelibrary.wiley.com/doi/book/10.1002/9781119092919 (accessed May 23, 2022).

[27] "support vector machines succinctly.pdf." Accessed: May 23, 2022. [Online]. Available: https://timofey.pro/static/pdfdocs/AI_024_support_vector_machines_succinctly.pdf

[28] C. Zoltan, "SVM and Kernel SVM. Learn about SVM or Support Vector," 2018. https://towardsdatascience.com/svm-and-kernel-svm-fed02bef1200 (accessed May 23, 2022).

[29] "[1804.00057] Understanding Autoencoders with Information Theoretic Concepts." https://arxiv.org/abs/1804.00057 (accessed May 23, 2022).

[30] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[31] M. Sakurada and T. Yairi, "Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction," in *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis*, New York, NY, USA, Dec. 2014, pp. 4–11. doi: 10.1145/2689746.2689747.

[32] J. An and S. Cho, "Variational Autoencoder based Anomaly Detection using Reconstruction Probability," *undefined*, 2015, Accessed: May 23, 2022. [Online]. Available: https://www.semanticscholar.org/paper/Variational-Autoencoder-based-Anomaly-Detection-An-Cho/061146b1d7938d7a8dae70e3531a00fceb3c78e8

[33] F. Karim, S. Majumdar, H. Darabi, and S. Harford, "Multivariate LSTM-FCNs for Time Series Classification," *Neural Netw.*, vol. 116, pp. 237–245, Aug. 2019, doi: 10.1016/j.neunet.2019.04.014.

[34] T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep Learning Methods for Credit Card Fraud Detection," arXiv, arXiv:2012.03754, Dec. 2020. doi: 10.48550/arXiv.2012.03754.

[35] S. Larabi Marie-Sainte, M. Bin Alamir, D. Alsaleh, G. Albakri, and J. Zouhair, "Enhancing Credit Card Fraud Detection Using Deep Neural Network," 2020, pp. 301–313. doi: 10.1007/978-3-030-52246-9_21.

[36] P. Malhotra, A. Ramakrishnan, G. Anand, L. Vig, P. Agarwal, and G. Shroff, "LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection," arXiv, arXiv:1607.00148, Jul. 2016. doi: 10.48550/arXiv.1607.00148.

[37] Valentina Alto, "Neural Networks: parameters, hyperparameters and optimization strategies | by Valentina Alto | Towards Data Science," 2019. https://towardsdatascience.com/neural-networks-parameters-hyperparameters-and-optimization-strategies-3f0842fac0a5 (accessed May 06, 2022).

[38] M. Sokolova, N. Japkowicz, and S. Szpakowicz, "Beyond Accuracy, F-Score and ROC: A Family of Discriminant Measures for Performance Evaluation," in *AI 2006: Advances in Artificial Intelligence*, Berlin, Heidelberg, 2006, pp. 1015–1021. doi: 10.1007/11941439_114.

[39] D. M. W. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation," arXiv, arXiv:2010.16061, Oct. 2020. doi: 10.48550/arXiv.2010.16061.

[40] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation | BMC Genomics | Full Text," 2020. https://bmcgenomics.biomedcentral.com/articles/10.1186/s12864-019-6413-7 (accessed May 24, 2022).

[41] B. Rocca, "Handling imbalanced datasets in machine learning | by Baptiste Rocca | Towards Data Science," 2019. https://towardsdatascience.com/handling-imbalanced-datasets-in-machine-learning-7a0e84220f28 (accessed May 24, 2022).

[42] D. Chicco, "Ten quick tips for machine learning in computational biology | BioData Mining | Full Text," 2017. https://biodatamining.biomedcentral.com/articles/10.1186/s13040-017-0155-3 (accessed May 24, 2022).

[43] A. Dubey and S. Tarar, "Evaluation of Approximate Rank-Order Clustering using Matthews Correlation Coefficient," vol. 8, no. 2, p. 8, 2018.

[44] "Credit card fraud detection anonymized credit card transaction labeled as fraudulent or genuine," 2013. https://www.kaggle.com/mlg-ulb/creditcardfraud (accessed May 25, 2022).

[45] "Abstract data set for Credit card fraud detection," 2018. https://www.kaggle.com/shubhamjoshi2130of/abstract-data-set-for-credit-card-fraud-detection (accessed May 25, 2022).

[46] C. Ranjan, M. Reddy, M. Mustonen, K. Paynabar, and K. Pourak, "Dataset: Rare Event Classification in Multivariate Time Series," arXiv, arXiv:1809.10717, May 2019. doi: 10.48550/arXiv.1809.10717.

[47] Chakravarti, Laha, and Roy, "Handbook of Methods of Applied Statistics," 1967. https://ideas.repec.org/a/bla/jorssc/v17y1968i3p293-294.html (accessed May 08, 2022).

[48] "Kolmogorov-SmirnovDTable.pdf." Accessed: May 08, 2022. [Online]. Available: https://luk.staff.ugm.ac.id/stat/ks/Kolmogorov-SmirnovDTable.pdf

[49] G. Alsmeyer, "Chebyshev's Inequality," 2011, pp. 239–240. doi: 10.1007/978-3-642-04898-2_167.

[50] R. M. Warren, "Visual intensity judgments: An empirical rule and a theory.," *Psychol. Rev.*, vol. 76, no. 1, pp. 16–30, 1969, doi: 10.1037/h0026732.

[51] R. Joseph, "Grid Search for model tuning. A model hyperparameter is a… | by Rohan Joseph | Towards Data Science," 2018. https://towardsdatascience.com/grid-search-for-model-tuning-3319b259367e (accessed May 11, 2022).
[52] A.-C. Florea and R. Andonie, "Weighted Random Search for Hyperparameter Optimization," *Int. J. Comput. Commun. Control*, vol. 14, no. 2, pp. 154–169, Apr. 2019, doi: 10.15837/ijccc.2019.2.3514.
[53] T. Tr, "Dimensionality Reduction: A Comparative Review," p. 36, 2009.
[54] J. Tang, S. Alelyani, and H. Liu, "Feature Selection for Classification: A Review," p. 33, 2014.
[55] J. Cai, J. Luo, S. Wang, and S. Yang, "Feature selection in machine learning: A new perspective," *Neurocomputing*, vol. 300, pp. 70–79, Jul. 2018, doi: 10.1016/j.neucom.2017.11.077.
[56] S. K. Trivedi, "A study on credit scoring modeling with different feature selection and machine learning approaches," *Technol. Soc.*, vol. 63, p. 101413, Nov. 2020, doi: 10.1016/j.techsoc.2020.101413.
[57] N. Gui, D. Ge, and Z. Hu, "AFS: An Attention-based mechanism for Supervised Feature Selection," *ArXiv190211074 Cs Stat*, Feb. 2019, Accessed: May 10, 2022. [Online]. Available: http://arxiv.org/abs/1902.11074
[58] R. Mbuvha, I. Boulkaibet, and T. Marwala, "Automatic Relevance Determination Bayesian Neural Networks for Credit Card Default Modelling," *ArXiv190606382 Cs Stat*, Jun. 2019, Accessed: May 10, 2022. [Online]. Available: http://arxiv.org/abs/1906.06382
[59] B. Škrlj, S. Džeroski, N. Lavrač, and M. Petkovič, "Feature Importance Estimation with Self-Attention Networks," *ArXiv200204464 Cs Stat*, Feb. 2020, doi: 10.3233/FAIA200256.
[60] C.-H. Chang, L. Rampasek, and A. Goldenberg, "Dropout Feature Ranking for Deep Learning Models," *ArXiv171208645 Cs Stat*, Mar. 2018, Accessed: May 10, 2022. [Online]. Available: http://arxiv.org/abs/1712.08645
[61] T. D. Gedeon, "Data mining of inputs: analysing magnitude and functional measures," *Int. J. Neural Syst.*, vol. 8, no. 2, pp. 209–218, Apr. 1997, doi: 10.1142/s0129065797000227.
[62] "NumPy documentation — NumPy v1.22 Manual." https://numpy.org/doc/stable/ (accessed May 25, 2022).
[63] "pandas documentation — pandas 1.4.2 documentation." https://pandas.pydata.org/docs/ (accessed May 25, 2022).
[64] "scikit-learn Tutorials — scikit-learn 1.1.1 documentation." https://scikit-learn.org/stable/tutorial/index.html (accessed May 25, 2022).
[65] K. Team, "Keras documentation: Getting started." https://keras.io/getting_started/ (accessed May 25, 2022).
[66] "TensorFlow Core | Machine Learning for Beginners and Experts." https://www.tensorflow.org/overview/ (accessed May 25, 2022).
[67] M. A. F. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, "A review of novelty detection," *Signal Process.*, vol. 99, pp. 215–249, Jun. 2014, doi: 10.1016/j.sigpro.2013.12.026.
[68] E. Eskin, "Anomaly Detection over Noisy Data using Learned Probability Distributions," in *Proceedings of the Seventeenth International Conference on Machine Learning*, San Francisco, CA, USA, Jun. 2000, pp. 255–262.
[69] N. H. Pontoppidan and J. Larsen, "Unsupervised condition change detection in large diesel engines," in *2003 IEEE XIII Workshop on Neural Networks for Signal Processing (IEEE Cat. No.03TH8718)*, Sep. 2003, pp. 565–574. doi: 10.1109/NNSP.2003.1318056.
[70] X. Jiang, X. Wen, M. Wu, M. Song, and C. Tu, "A complex network analysis approach for identifying air traffic congestion based on independent component analysis," *Phys. Stat. Mech. Its Appl.*, vol. 523, Feb. 2019, doi: 10.1016/j.physa.2019.01.129.

[71] I. Melnyk, A. Banerjee, B. Matthews, and N. Oza, "Semi-Markov Switching Vector Autoregressive Model-based Anomaly Detection in Aviation Systems," Feb. 2016, doi: 10.48550/arXiv.1602.06550.

[72] I. Melnyk, B. Matthews, H. Valizadegan, A. Banerjee, and N. Oza, "Vector autoregressive model-based anomaly detection in aviation systems," *J. Aerosp. Inf. Syst.*, vol. 13, no. 4, pp. 161–173, 2016, doi: 10.2514/1.I010394.

[73] D. Chen, X. Shao, B. Hu, and Q. Su, "Simultaneous wavelength selection and outlier detection in multivariate regression of near-infrared spectra," *Anal. Sci. Int. J. Jpn. Soc. Anal. Chem.*, vol. 21, no. 2, pp. 161–166, Feb. 2005, doi: 10.2116/analsci.21.161.

[74] A. M. Bianco, M. García Ben, E. J. Martínez, and V. J. Yohai, "Outlier Detection in Regression Models with ARIMA Errors using Robust Estimates," *J. Forecast.*, vol. 20, no. 8, pp. 565–579, 2001, doi: 10.1002/for.768.

[75] S. Mei-Ling, "A Novel Anomaly Detection Scheme Based on Principal Component Classifier," *Proc. IEEE Found. New Dir. Data Min. Workshop Conjunction Third IEEE Int. Conf. Data Min. ICDM03*, pp. 172–179, 2003.

[76] Z. Li, G. Liu, S. Wang, S. Xuan, and C. Jiang, "Credit Card Fraud Detection via Kernel-Based Supervised Hashing," in *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 1249–1254. doi: 10.1109/SmartWorld.2018.00217.

[77] D. Prusti and S. K. Rath, "Web service based credit card fraud detection by applying machine learning techniques," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, Oct. 2019, pp. 492–497. doi: 10.1109/TENCON.2019.8929372.

[78] I. Sohony, R. Pratap, and U. Nambiar, "Ensemble learning for credit card fraud detection," in *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*, New York, NY, USA, Jan. 2018, pp. 289–294. doi: 10.1145/3152494.3156815.

[79] S. Agrawal and J. Agrawal, "Survey on Anomaly Detection using Data Mining Techniques," *Procedia Comput. Sci.*, vol. 60, pp. 708–713, Jan. 2015, doi: 10.1016/j.procs.2015.08.220.

[80] E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decis. Support Syst.*, vol. 50, no. 3, pp. 559–569, 2011, doi: 10.1016/j.dss.2010.08.006.

[81] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," *IEEE Access*, vol. 7, pp. 93010–93022, 2019, doi: 10.1109/ACCESS.2019.2927266.

[82] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, Mar. 2018, pp. 1–6. doi: 10.1109/ICNSC.2018.8361343.

[83] S. V. Suryanarayana, G. N. Balaji, and G. V. Rao, "Machine Learning Approaches for Credit Card Fraud Detection," *Int. J. Eng. Technol.*, vol. 7, no. 2, Art. no. 2, Jun. 2018, doi: 10.14419/ijet.v7i2.9356.

[84] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit Card Fraud Detection - Machine Learning methods," in *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, Mar. 2019, pp. 1–5. doi: 10.1109/INFOTEH.2019.8717766.

[85] V. N. Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," *Procedia Comput. Sci.*, vol. 165, pp. 631–641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.

[86] M.-Y. Su, "Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers," *Expert Syst. Appl.*, vol. 38, no. 4, pp. 3492–3498, Apr. 2011, doi: 10.1016/j.eswa.2010.08.137.

[87] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *2017 International Conference on Computing Networking and Informatics (ICCNI)*, Oct. 2017, pp. 1–9. doi: 10.1109/ICCNI.2017.8123782.

[88] B. Song and Y. Suh, "Narrative texts-based anomaly detection using accident report documents: The case of chemical process safety," *J. Loss Prev. Process Ind.*, vol. 57, pp. 47–54, Jan. 2019, doi: 10.1016/j.jlp.2018.08.010.

[89] T. Ekin, "Application of Bayesian Methods in Detection of Healthcare Fraud," *Chem. Eng. Trans.*, vol. 33, Jan. 2013, doi: 10.3303/CET1333026.

[90] F. Jia, Y. Yan, and J. Zhang, "K-means based feature reduction for network anomaly detection," *Qinghua Daxue XuebaoJournal Tsinghua Univ.*, vol. 58, pp. 137–142, Feb. 2018, doi: 10.16511/j.cnki.qhdxxb.2018.26.005.

[91] R. M. Alguliyev, R. M. Aliguliyev, and F. J. Abdullayeva, "PSO+K-means Algorithm for Anomaly Detection in Big Data," *Stat. Optim. Inf. Comput.*, vol. 7, no. 2, Art. no. 2, May 2019, doi: 10.19139/soic.v7i2.623.

[92] Z. Cheng, C. Zou, and J. Dong, "Outlier detection using isolation forest and local outlier factor," in *Proceedings of the Conference on Research in Adaptive and Convergent Systems*, New York, NY, USA, Sep. 2019, pp. 161–168. doi: 10.1145/3338840.3355641.

[93] P. Jain and R. Pamula, "Two-Step Anomaly Detection Approach Using Clustering Algorithm: ICANI-2018," 2019, pp. 513–520. doi: 10.1007/978-981-13-2673-8_54.

[94] J. Jeba, V. Ramachandran, and K. Ramalakshmi, "Fraud Detection for Credit Card Transactions Using Random Forest Algorithm," 2021, pp. 189–197. doi: 10.1007/978-981-15-5285-4_18.

[95] S. Wang, G. Liu, Z. Li, S. Xuan, C. Yan, and C. Jiang, "Credit Card Fraud Detection Using Capsule Network," in *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct. 2018, pp. 3679–3684. doi: 10.1109/SMC.2018.00622.

[96] S. Dhankhad, E. Mohammed, and B. Far, "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study," in *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, Jul. 2018, pp. 122–125. doi: 10.1109/IRI.2018.00025.

[97] M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini, "Credit Card Fraud Detection Using Random Forest Algorithm," in *2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, Feb. 2019, pp. 149–153. doi: 10.1109/ICCCT2.2019.8824930.

[98] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning," in *2019 9th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, Jan. 2019, pp. 488–493. doi: 10.1109/CONFLUENCE.2019.8776942.

[99] G. Pang, C. Shen, L. Cao, and A. van den Hengel, "Deep Learning for Anomaly Detection: A Review," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–38, Mar. 2022, doi: 10.1145/3439950.

[100] G. Pang, C. Yan, C. Shen, A. van den Hengel, and X. Bai, "Self-trained Deep Ordinal Regression for End-to-End Video Anomaly Detection," arXiv, arXiv:2003.06780, Mar. 2020. doi: 10.48550/arXiv.2003.06780.

[101] J. T. Zhou, J. Du, H. Zhu, X. Peng, Y. Liu, and R. S. M. Goh, "AnomalyNet: An Anomaly Detection Network for Video Surveillance," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2537–2550, Oct. 2019, doi: 10.1109/TIFS.2019.2900907.

[102] G. Pang, A. Hengel, C. Shen, and L. Cao, *Deep Reinforcement Learning for Unknown Anomaly Detection*. 2020.

[103] G. Pang, C. Shen, and A. van den Hengel, "Deep Anomaly Detection with Deviation Networks," arXiv, arXiv:1911.08623, Nov. 2019. doi: 10.48550/arXiv.1911.08623.

[104] S. Fan, C. Shi, and X. Wang, "Abnormal Event Detection via Heterogeneous Information Network Embedding," in *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*, New York, NY, USA, Oct. 2018, pp. 1483–1486. doi: 10.1145/3269206.3269281.

[105] P. Zheng, S. Yuan, X. Wu, J. Li, and A. Lu, "One-Class Adversarial Nets for Fraud Detection," arXiv, arXiv:1803.01798, Jun. 2018. doi: 10.48550/arXiv.1803.01798.

[106] F. Di Mattia, P. Galeone, M. De Simoni, and E. Ghelfi, "A Survey on GANs for Anomaly Detection," arXiv, arXiv:1906.11632, Sep. 2021. doi: 10.48550/arXiv.1906.11632.

[107] H. Zenati, C. S. Foo, B. Lecouat, G. Manek, and V. R. Chandrasekhar, "Efficient GAN-Based Anomaly Detection," arXiv, arXiv:1802.06222, May 2019. doi: 10.48550/arXiv.1802.06222.

[108] A. Creswell and A. A. Bharath, "Inverting the Generator of a Generative Adversarial Network," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 7, pp. 1967–1974, Jul. 2019, doi: 10.1109/TNNLS.2018.2875194.

[109] E. Marchi, F. Vesperini, F. Weninger, F. Eyben, S. Squartini, and B. Schuller, "Non-linear prediction with LSTM recurrent neural networks for acoustic novelty detection," in *2015 International Joint Conference on Neural Networks (IJCNN)*, Jul. 2015, pp. 1–7. doi: 10.1109/IJCNN.2015.7280757.

[110] J. M. Ghawaly *et al.*, "Characterization of the Autoencoder Radiation Anomaly Detection (ARAD) model," *Eng. Appl. Artif. Intell.*, vol. 111, p. 104761, May 2022, doi: 10.1016/j.engappai.2022.104761.

[111] Y. Liu, W. Xie, Y. Li, Z. Li, and Q. Du, "Dual-Frequency Autoencoder for Anomaly Detection in Transformed Hyperspectral Imagery," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, pp. 1–13, 2022, doi: 10.1109/TGRS.2022.3152263.

[112] T. R. Pillai, I. A. T. Hashem, S. N. Brohi, S. Kaur, and M. Marjani, "Credit Card Fraud Detection Using Deep Learning Technique," in *2018 Fourth International Conference on Advances in Computing, Communication Automation (ICACCA)*, Oct. 2018, pp. 1–6. doi: 10.1109/ICACCAF.2018.8776797.

[113] P. Raghavan and N. E. Gayar, "Fraud Detection using Machine Learning and Deep Learning," in *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Dec. 2019, pp. 334–339. doi: 10.1109/ICCIKE47802.2019.9004231.

[114] A. Pumsirirat and L. Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 9, no. 1, Art. no. 1, 55/31 2018, doi: 10.14569/IJACSA.2018.090103.

[115] M. Raza and U. Qayyum, "Classical and Deep Learning Classifiers for Anomaly Detection," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Jan. 2019, pp. 614–618. doi: 10.1109/IBCAST.2019.8667245.

[116] A. Borghesi, A. Bartolini, M. Lombardi, M. Milano, and L. Benini, "Anomaly Detection using Autoencoders in High Performance Computing Systems," *Proc. AAAI Conf. Artif. Intell.*, vol. 33, pp. 9428–9433, Jul. 2019, doi: 10.1609/aaai.v33i01.33019428.

[117] E. Ordway-West, P. Parveen, and A. Henslee, "Autoencoder Evaluation and Hyper-Parameter Tuning in an Unsupervised Setting," in *2018 IEEE International Congress on Big Data (BigData Congress)*, Jul. 2018, pp. 205–209. doi: 10.1109/BigDataCongress.2018.00034.

[118] D. Lakhmiri, R. Alimo, and S. L. Digabel, "Tuning a variational autoencoder for data accountability problem in the Mars Science Laboratory ground data system," arXiv, arXiv:2006.03962, Jun. 2020. doi: 10.48550/arXiv.2006.03962.

[119] A. A. Bataineh, A. Mairaj, and D. Kaur, "Autoencoder based Semi-Supervised Anomaly Detection in Turbofan Engines," *Int. J. Adv. Comput. Sci. Appl. IJACSA*, vol. 11, no. 11, Art. no. 11, 57/01 2020, doi: 10.14569/IJACSA.2020.0111105.

[120] S. Misra, S. Thakur, M. Ghosh, and S. Saha, "An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction," 2020, doi: 10.1016/j.procs.2020.03.219.

[121] B. Esmael, A. Arnaout, R. K. Fruhwirth, and G. Thonhauser, "Improving time series classification using Hidden Markov Models," in *2012 12th International Conference on Hybrid Intelligent Systems (HIS)*, Dec. 2012, pp. 502–507. doi: 10.1109/HIS.2012.6421385.

[122] A. Jović, K. Brkić, and N. Bogunović, "Decision Tree Ensembles in Biomedical Time-Series Classification," in *Pattern Recognition*, Berlin, Heidelberg, 2012, pp. 408–417. doi: 10.1007/978-3-642-32717-9_41.

[123] Z. Cui, W. Chen, and Y. Chen, "Multi-Scale Convolutional Neural Networks for Time Series Classification," arXiv, arXiv:1603.06995, May 2016. doi: 10.48550/arXiv.1603.06995.

[124] C. Zhang, H. Yan, S. Lee, and J. Shi, "Multiple profiles sensor-based monitoring and anomaly detection," *J. Qual. Technol.*, vol. 50, no. 4, pp. 344–362, Oct. 2018, doi: 10.1080/00224065.2018.1508275.

[125] Y. Zheng, Q. Liu, E. Chen, Y. Ge, and J. L. Zhao, "Time Series Classification Using Multi-Channels Deep Convolutional Neural Networks," in *Web-Age Information Management*, Cham, 2014, pp. 298–310. doi: 10.1007/978-3-319-08010-9_33.

[126] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," Apr. 2018, pp. 129–134. doi: 10.1109/SIEDS.2018.8374722.

[127] K. P. Tran, H. D. Nguyen, and S. Thomassey, "Anomaly detection using Long Short Term Memory Networks and its applications in Supply Chain Management," *IFAC-Pap.*, vol. 52, no. 13, pp. 2408–2412, Jan. 2019, doi: 10.1016/j.ifacol.2019.11.567.

[128] D. Li, D. Chen, L. Shi, B. Jin, J. Goh, and S.-K. Ng, "MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks," arXiv, arXiv:1901.04997, Jan. 2019. doi: 10.48550/arXiv.1901.04997.

[129] H. Song, Z. Jiang, A. Men, and B. Yang, "A Hybrid Semi-Supervised Anomaly Detection Model for High-Dimensional Data," *Comput. Intell. Neurosci.*, vol. 2017, p. 8501683, 2017, doi: 10.1155/2017/8501683.

[130] V. L. Cao, M. Nicolau, and J. McDermott, "A Hybrid Autoencoder and Density Estimation Model for Anomaly Detection," in *Parallel Problem Solving from Nature – PPSN XIV*, Cham, 2016, pp. 717–726. doi: 10.1007/978-3-319-45823-6_67.

[131] Z. Chen, C. K. Yeo, B. S. Lee, and C. T. Lau, "Autoencoder-based network anomaly detection," in *2018 Wireless Telecommunications Symposium (WTS)*, Apr. 2018, pp. 1–5. doi: 10.1109/WTS.2018.8363930.

[132] T. Kim, S. C. Suh, H. Kim, J. Kim, and J. Kim, "An Encoding Technique for CNN-based Network Anomaly Detection," in *2018 IEEE International Conference on Big Data (Big Data)*, Dec. 2018, pp. 2960–2965. doi: 10.1109/BigData.2018.8622568.

[133] C. Szegedy *et al.*, "Going Deeper with Convolutions," arXiv, arXiv:1409.4842, Sep. 2014. doi: 10.48550/arXiv.1409.4842.

[134] J. Zhang, Y. Xie, Y. Li, C. Shen, and Y. Xia, "COVID-19 Screening on Chest X-ray Images Using Deep Learning based Anomaly Detection," *ArXiv*, 2020.

[135] X. Zhao, X. Han, W. Su, and Z. Yan, "Time series prediction method based on Convolutional Autoencoder and LSTM," in *2019 Chinese Automation Congress (CAC)*, Nov. 2019, pp. 5790–5793. doi: 10.1109/CAC48633.2019.8996842.

[136] H. Homayouni, S. Ghosh, I. Ray, S. Gondalia, J. Duggan, and M. G. Kahn, "An Autocorrelation-based LSTM-Autoencoder for Anomaly Detection on Time-Series Data," in *2020 IEEE International Conference on Big Data (Big Data)*, Dec. 2020, pp. 5068–5077. doi: 10.1109/BigData50022.2020.9378192.

[137] Z. Ghrib, R. Jaziri, and R. Romdhane, "Hybrid approach for Anomaly Detection in Time Series Data," in *2020 International Joint Conference on Neural Networks (IJCNN)*, Jul. 2020, pp. 1–7. doi: 10.1109/IJCNN48605.2020.9207013.

[138] Z. Que, Y. Liu, C. Guo, X. Niu, Y. Zhu, and W. Luk, "Real-Time Anomaly Detection for Flight Testing Using AutoEncoder and LSTM," in *2019 International Conference on Field-Programmable Technology (ICFPT)*, Dec. 2019, pp. 379–382. doi: 10.1109/ICFPT47387.2019.00072.

[139] A. Rb and S. K. Kr, "Credit card fraud detection using artificial neural network," *Glob. Transit. Proc.*, vol. 2, no. 1, pp. 35–41, Jun. 2021, doi: 10.1016/j.gltp.2021.01.006.

[140] I. SADGALI, N. SAEL, and F. BENABBOU, "Fraud detection in credit card transaction using machine learning techniques," in *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, Oct. 2019, pp. 1–4. doi: 10.1109/ICSSD47982.2019.9002674.

[141] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A Financial Fraud Detection Model Based on LSTM Deep Learning Technique," *J. Appl. Secur. Res.*, vol. 15, no. 4, pp. 498–516, Oct. 2020, doi: 10.1080/19361610.2020.1815491.

[142] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for Anomaly-Based Network Intrusion Detection," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2018, pp. 1–3. doi: 10.1109/ATNAC.2018.8615300.

[143] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Clust. Comput.*, vol. 22, no. 1, pp. 949–961, Jan. 2019, doi: 10.1007/s10586-017-1117-8.

[144] H. Moeini and F. M. Torab, "Comparing compositional multivariate outliers with autoencoder networks in anomaly detection at Hamich exploration area, east of Iran," *J. Geochem. Explor.*, vol. 180, pp. 15–23, Sep. 2017, doi: 10.1016/j.gexplo.2017.05.008.

[145] R. Kohavi, "A Study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection," 1995, pp. 1137–1143.

[146] shipra, "Here's All you Need to Know About Encoding Categorical Data (with Python code) - Google Search," 2020. https://morioh.com/p/7deaea562c63 (accessed Mar. 29, 2022).

[147] K. Corbin, "Marred by High False Positive Rates, Long Processing Times, and Unwieldy Processes Which Continue to Plague the IRS and Harm Legitimate Taxpayers," p. 12, 2018.

[148] P. Pathak and C. Sharma, "Processes and problems of pulp and paper industry: an overview," *Phys. Sci. Rev.*, Feb. 2021, doi: 10.1515/psr-2019-0042.

[149] T.-H. Lin and J.-R. Jiang, "Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest," Mathematics, vol. 9, no. 21, Art. no. 21, Jan. 2021, doi: 10.3390/math9212683.

[150] S P Maniraj, Aditya Saini, Shadab Ahmed, Swarna Deep Sarkar, and SRM Institute of Science and Technology, INDIA, "Credit Card Fraud Detection using Machine Learning and Data Science," Int. J. Eng. Res., vol. 08, no. 09, p. IJERTV8IS090031, Sep. 2019, doi: 10.17577/IJERTV8IS090031.

[151] M. Zamini and G. Montazer, "Credit Card Fraud Detection using autoencoder based clustering," in 2018 9th International Symposium on Telecommunications (IST), Dec. 2018, pp. 486–491. doi: 10.1109/IS^{TEL}.2018.8661129.

[152] S. Bagga, A. Goyal, N. Gupta, and A. Goyal, "Credit Card Fraud Detection using Pipeling and Ensemble Learning," Procedia Comput. Sci., vol. 173, pp. 104–112, Jan. 2020, doi: 10.1016/j.procs.2020.06.014.

[153] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit Card Fraud Detection Using Machine Learning," in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), May 2020, pp. 1264–1270. doi: 10.1109/ICICCS48265.2020.9121114.

[154] J. Zou, J. Zhang, and P. Jiang, "Credit Card Fraud Detection Using Autoencoder Neural Network." arXiv, Aug. 30, 2019. doi: 10.48550/arXiv.1908.11553.

[155] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," IEEE Access, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.

[156] Chitta Ranjan, "LSTM Autoencoder for Extreme Rare Event Classification in Keras," 2019. https://towardsdatascience.com/lstm-autoencoder-for-extreme-rare-event-classification-in-keras-ce209a224cfb?gi=dd56a79139ab (accessed Apr. 22, 2022).

[157] "Early failure detection of paper manufacturing machinery using nearest neighbor-based feature extraction - Lee - 2021 - Engineering Reports - Wiley Online Library." https://onlinelibrary.wiley.com/doi/full/10.1002/eng2.12291 (accessed Oct. 01, 2022).

[158] D. Xu, Z. Zhang, and J. Shi, "Training Data Selection by Categorical Variables for Better Rare Event Prediction in Multiple Products Production Line," Electronics, vol. 11, no. 7, Art. no. 7, Jan. 2022, doi: 10.3390/electronics11071056.

Syrian Arab Republic
Al-Baath University
Faculty of Informatics Engineering
Department of Software Engineering & Information Systems

Analysis of Data Anomalies' Detection Systems and Improving them Using Deep Learning

A Thesis Submitted in Fulfilment of The Requirements for The Doctor of Philosophy Degree in Software Engineering and Information Systems

Prepared By:

Eng. Ali Loai Yassin

Supervised By:

Dr. Kamal Al-Salloum

A Professor at the Department of Software Engineering and Information Systems
Major in Operations Research
Faculty of Informatics Engineering
Al-Baath University

CO-Supervisor:

Dr. Wassim Ramada

A Lecturer at the Department of Agricultural Economics
Major in Programming and Computers
Faculty of Agriculture
Al-Baath University

1444 A.H-2022 A.D