جامعة غرداية - الجزائر -

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم المالية والمحاسبة

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر أكاديمي

في ميدان: العلوم الاقتصادية وعلوم التسيير والعلوم التجارية

فرع: العلوم مالية والمحاسبة، تخصص تكنولوجيا مالية

بعنـوان:

دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني (تصميم انموذج)

من اعداد الطالبة: اكرام معطاالله

تحت اشراف ا. الدكتورة: شرع مريم

الأستاذة المساعدة: بقدور فاطمة الزهراء

نوقشت واجيزت علنا بتاريخ :01 /06/ 2026

أمام اللجنة المكونة من السادة:

الاسم واللقب	الرتبة	الجامعة	الصفة
رواني بوحفص	استاذ	جامعة غرداية	رئيساً
شرع مريم	استاذ	جامعة غرداية	مشرفاً ومقرراً
بوقدور فاطمة الزهراء	أستاذ مشارك	جامعة غرداية	مشرف مساعداً
بن طاجين عبد الرحمان	أستاذ محاضر	جامعة غرداية	مناقشاً

السنة الجامعية: 2026/2025م

جامعة غرداية - الجزائر -

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم العلوم المالية والمحاسبة

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر أكاديمي

في ميدان: العلوم الاقتصادية وعلوم التسيير والعلوم التجارية

فرع: العلوم مالية والمحاسبة، تخصص تكنولوجيا مالية

بعنـوان:

دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني (تصميم انموذج)

من اعداد الطالبة: تحت اشراف ا. الدكتورة: شرع مريم

اكرام معطاالله الأستاذة المساعدة: بقدور فاطمة الزهراء

نوقشت واجيزت علنا بتاريخ :01 /06/ 2026

أمام اللجنة المكونة من السادة: أمام اللجنة المكونة من السادة:

الاسم واللقب	الرتبة	الجامعة	الصفة
رواني بوحفص	استاذ	جامعة غرداية	رئيساً
شرع مريم	استاذ	جامعة غرداية	مشرفاً ومقرراً
بوقدور فاطمة الزهراء	أستاذ مشارك	جامعة غرداية	مشرف مساعداً
بن طاجين عبد الرحمان	أستاذ محاضر	جامعة غرداية	مناقشاً

السنة الجامعية: 2026/2025م



إهداء

أهذي عملي هذا الى من كان لهم الفضل الأكبر بعد الله سبحانه وتعالى
في مسيرتي:

إلى من جعل الله الجنة تحت اقدامها واحتضنتني قلبا قبل يدها

الى مصدر الدعاء الشديد الذي لا ينقطع

الى القلب الحنون والشمعة المضيئة والنور الذي لا يخبو

الى سر قوتي ونجاحي إلى أمي الغالية "فرج الله غنية"

إلى الذي دعمني بلا حدود واعطاني بلا مقابل ومن علمني أن الدنيا كفاح وسلاحه العلم والمعرفة

الى دعمي الأول في مسيرتي وسندي وقوتي وملاذي بعد الله

إلى فخري واعتزازي

إلى من زين اسمي بأجمل الألقاب إلى ابي الغالي: "معطاالله لخضر"

أهديكم تمرة جهد صغير أمام عطاءكم الكبير

إلى بركة العائلة وأمي الثانية الى جدتي الغالية: "بيتور فاطنة" اطال الله في عمرها

إلى ضلعي الثابت ورفقاء قلبي وامان ايامي ونبضها الى من شددت عضدي بهم فكانوا لي ينابيع ارتوي منها

الى قرة عيني وتواءم روحي اخوتي: "عبد الصمد، شيماء، هاجر، عبد الرؤوف"

اللذان تقاسما معي لحظات النجاح والفشل مند بداية المشوار.

الى زملائي في مشواري الدراسي بتخصص التكنولوجيا المالية.

الى الطلبة الدين يتخوفون من دراسة مواضيع الذكاء الاصطناعي
وتصميم نماذج خوارزميات تعلم الالة.

الى من كان لي عونا وسندا في هذا الطريق وافاضني بنصائحه المخلصة.

الى كل من يذكره قلبي ولم يذكره قلمي.

وفي الأخير اسال الله ان يجعل هذا العمل خالصاً لوجهه الكريم،
وان ينفع به، ويوفق الجميع لما فيه الخير والسداد،
فإن أصبنا فمن الله وحده، وان اخطانا فمن أنفسنا،
والله ولي التوفيق



أكرام

شكر وعرفان

أتقدم أولا بالحمد والشكر لله الكريم العظيم لأنه سهل لي هذا العمل ووفقني لإنجازه وهداني الى طريق المعرفة فله الحمد إذا رضي وله الحمد حتى يرضى وله الحمد بعد الرضا والصلاة والسلام على أشرف المرسلين محمد صلى الله عليه وسلم

أتوجه بالشكر الجزيل وعظيم الامتنان الى الأستاذة المشرفة الأستاذة الدكتورة **شرع مريم** على ما قدمته من نصائح سديدة وارشادات ومتابعتها المستمرة طوال مراحل انجاز هذه المذكرة، التي كان لها اتر في استكمال هدا العمل.

اسال الله ان يجازيها خير الجزاء ويبارك لها في علمها وعملها.

أتوجه بالشكر الجزيل الى المشرفة المساعدة الأستاذة: **بقدور فاطمة الزهراء** على ما قدمته من نصائح وارشادات وعلى مرافقتها العلمية التي كان لها اتر في استكمال هذا العمل.

اسال الله ان يجازيها خير الجزاء ويبارك لها في علمها وعملها.

هدان اللذان لن تكفي حروف هذه الكلمات لشكرهم وإيفائهم حقهم بصبرهم الكبير وتوجيهاتهم العلمية التي لا تقدر بتمن وكان لعطاءهم أثر بالغ لا ينسى وشرفاني بقبولهم الاشراف على هده المذكرة.

كما أتقدم بالشكر الخالص الى كافة أساتذة قسم المالية والمحاسبة والى عميد كلية العلوم الاقتصادية والتجارية وعلوم التسيير بجامعة غرداية ا.د رواني بوحفص، لما قدموه لنا من علم ومعرفة طيلة سنوات الدراسة والى كل من علمني حرفا في هده الدنيا الفانية،

ومن حملوا رسالة العلم بإخلاص وكانوا لنا نبراسا نهتدي به بعد الله تعالى، اسأل الله ان يجعل ذلك في ميزان حسناتهم.

ولا يفوتني ان اشكر كل من ساهم في انجاز هدا العمل من قريب او بعيد وأقول لهم جزاكم الله عني خيرا.



إكرام

ملخص الدراسة

ملخص الدراسة

الملخص:

تهدف هده الدراسة الى التعرف على دور خوارزميات تعلم الالة ومدى فعاليتها في كشف الاحتيال المالي الالكتروني المرتبط بالمعاملات المالية اليومية الرقمية، وذلك باعتباره النوع الأكثر انتشـــارا في البيئة الجزائرية، وذلك من خلال تصـميم أنموذج باسـتخدام خوارزمية تعلم الالة الغابة العشـوائية (Random Forest) بتطبيق جميع مراحل التصـــميم اللازمة لدراســة عبر برنامج (Orange Data Mining) وتقييم اداءه عبر مقاييس الأداء الشـاملة بالإضـافة الى تحديد المتغيرات الأكثر تأثيرا في الكشـف عن الاحتيال، ولتحقيق ذلك، تم اختيار قاعدة بيانات اصطناعية محاكاة من منصة (kaggle) تخص معاملات مالية لسنة 2023 بعنوان (Fraud Detection Transactions Dataset) تضم 50000 معاملة مالية و21 ميزة منها 18 خاصية مستقلة وخاصية تابعة واحدة (Fraud Label) .

وأظهرت النتائج فعالية أنموذج الدراسة في كشف الاحتيال المالي الالكتروني، حيت حقق دقة كلية بلغت 95,8% وقيمة (Auc) بلغت 99,6% ومعامل ارتباط ما تيوس 90,4%، مما يؤكد أهمية خوارزميات تعلم الالة في دعم المؤسسات المالية وتعزيز أنظمة الحماية والكشف المبكر عن المعاملات الاحتيالية في ظل تطورات عصر التكنولوجيا المالية.

الكلمات المفتاحية: احتيال مالي الكتروني، خوارزميات تعلم الالة، كشـــف الاحتيال المالي، تصـــميم انموذج، برمجية أورانج، بيانات اصطناعية محاكاة، التحقق المتقاطع، الغابة العشوائية.

Abstract:

This study aims to identify the role of Machine Learning algorithms and evaluate their effectiveness in Detecting electronic financial fraud associated with daily digital financial transaction, as This type of fraud is considered one of the Most widespread in the Algerian environment. This was achieved by designing a model using the Random Forest machine learning Algorithm through applying all the necessary design stages within the orange data mining, evaluating its Performance using comprehensive evaluation metrics, and identifying the most influential variables in fraud detection. To achieve This objective, a Simulated Synthetic Dataset was selected from kaggle platform, The Dataset represents financial transactions for the Year 2023 and contains 50000 financial transactions and 21 features, including 18 independent variables and one dependent variable.

The resultes demonstrated the effectiveness of the proposed model in Detecting electronic financial fraud, achieving an overall Accuracy of 95,8%, and Auc value of 99 ,6%, and à Matthews Correlation Cofficient of 90 ,4%, these findings confirm the importance of Machine Learning algorithms in supporting financial institutions, enhancing protection Systems, and enabling the early detection of Fraudulent transactions in light of the developments of the financial technology era.

Keywords: Electronic Financial Fraud, Machine Learning Algorithms, Financial Fraud detection, Model design, orange data mining, Synthetic Simulated Data, Cross Validation, Random Forest.

فهرس المحتويات

فهرس المحتويات

العنوان	الصفحة
الإهداء	I
الشكر وعرفان	II
فهرس المحتويات	III
قائمة الجداول والاشكال	IV
قائمة الاختصارات والرموز	V
مقدمة	أ–و
الفصل الأول: الأدبيات النظرية للاحتيال المالي الالكتروني وخوارزميات تعلم الالة	
تمهيد	08
المبحث الأول: الإطار المفاهيمي للاحتيال المالي الالكتروني	09
المطلب الأول: مفاهيم الاحتيال المالي الالكتروني	09
المطلب الثاني: أنواع وأساليب الاحتيال المالي الالكتروني	17
المطلب الثالث: اثار الاحتيال المالي الالكتروني وقصور الطرق التقليدية في كشفه	34
المبحث الثاني: الإطار المفاهيمي لخوارزميات التعلم الالي ودورها في كشف الاحتيال المالي الالكتروني	38
المطلب الأول: مفاهيم حول الذكاء الاصطناعي	38
المطلب الثاني: تعلم الالة كفرع من فروع الذكاء الاصطناعي	45
المطلب الثالث: خوارزميات تعلم الالة	
المطلب الرابع: دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني	63
المبحث الثالث: مراجعة الدراسات السابقة المتعلقة بالدراسة الحالية	68
المطلب الأول: الدراسات عربية	68

فهرس المحتويات

المطلب الثاني: الدراسات الأجنبية	70
المطلب الثالث: المقارنة بين الدراسة الحالية والدراسات السابقة	82
خلاصة الفصل الاول	88
الفصل الثاني: تصميم أنموذج خوارزمية تعلم الالة لكشف الاحتيال المالي الالكتروني	
تمهيد	37
المبحث الأول: منهجية الدراسة التطبيقية ومراحل بناء انموذج خوارزمية التعلم الالي	91
المطلب الأول: مجتمع وعينة الدراسة	91
المطلب الثاني: متغيرات الدراسة والفحص الاولي للبيانات	92
المطلب الثالث: تعريف بيئة العمل البرمجية (Orange Data Mining) وأسباب اختيارها	94
المطلب الرابع : المراحل النظرية لتصميم أنموذج خوارزمية تعلم الالة	96
المبحث الثاني: التصميم الفعلي لأنموذج خوارزمية تعلم الالة (الغابة العشوائية) وتقييم اداءه	103
المطلب الأول: جمع البيانات والتحليل الاستكشافي لها	104
المطلب الثاني: التطبيق العملي لمراحل تصميم أنموذج خوارزمية الغابة العشوائية	111
المطلب الثالث: تقييم أداء أنموذج خوارزمية الغابة العشوائية	114
المطلب الرابع: تحليل المتغيرات الأكثر تأثيرا في كشف الاحتيال	124
خلاصة الفصل الثاني	125
الخاتمة	127
قائمة المراجع	132

قائمة الجداول والاشكال والاختصارات

قائمة الجداول

الرقم	العنوان	الصفحة
01 – 01	خصائص الاحتيال المالي الالكتروني	15
01 –02	اركان الاحتيال المالي الالكتروني	16
01 –03	الاحتيال ببطاقة الدفع الالكتروني	18
01 –04	الاحتيال البنكي الالكتروني	20
01 –05	الاحتيال في التجارة الالكترونية	21
01–06	الاحتيال في السوق المالي والبورصات	22
01 –07	الاحتيال الالكتروني في التامين	23
01 –08	الاحتيال في العملات المشفرة	24
01 –09	الاحتيال في التمويل الجماعي	26
01 –10	مراحل وتقنيات التصيد الاحتيالي	28
01 –11	ركائز التصيد الاحتيالي المدعوم بالذكاء الاصطناعي	30
01 –12	التزييف العميق واليته	31
01 –13	الاحتيال عبر انترنت الأشياء	32
01 –14	أنماط تعلم الالة	44
01 –15	المقارنة بين الطرق التقليدية وخوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني	65
02 –16	وصف خصائص بيانات الدراسة التطبيقية	93
02 –17	مؤشرات قياس الأداء الأساسية لنماذج تعلم الالة	99
02 –18	الأدوات الوظيفية لبرنامج (Orange) المستخدمة في دراستنا التطبيقية	103
02 –19	التحليل الوصفي للمتغيرات العددية	107
02 –20	التحليل الوصفي للمتغيرات الفئوية	108
02 –21	الية عمل التحقق المتقاطع دي الـ 5 طيات	112
02 –22	تفسير قيم مصفوفة الارتباك	114

قائمة الأشكال

الرقم	العنوان	الصفحة
01 -01	مثلث الاحتيال المالي	11
01 -02	معين الاحتيال المالي	12
01 -03	خماسي الاحتيال المالي	13
01 -04	سداسي الاحتيال المالي لفوسيناس	13
01 -05	خصائص الذكاء الاصطناعي	39
01 -06	العلاقة بين الذكاء الاصطناعي وتعلم الالة	41
01 -07	الية عمل تعلم الالة	42
01 -08	الإطار العام لعمل خوارزميات التعلم الالي	46
01 -09	الية عمل خوارزمية الانحدار اللوجستي	46
01 -10	الية عمل خوارزمية شجرة القرار	47
01 -11	الية عمل خوارزمية الغابة العشوائية	48
01 -12	الية عمل خوارزمية (XGBoost)	49
01 -13	الية عمل خوارزمية AdaBoost	49
01 -14	الية عمل خوارزمية الة المتجهات الداعمة	50
01 -15	الية عمل خوارزمية الجيران الأقرب	51
01 -16	الية عمل خوارزمية ساذج بايز	51
01 -17	معمارية الشبكة العصبية الاصطناعية	52
01 -18	الية عمل خوارزمية (k-Means)	53
01 -19	الية عمل خوارزمية عامل الخروج المحلي	54
01 -20	رسم بياني يوضح الية عمل تحليل المكونات الأساسية	55
01 -21	الإطار العام لمبدأ عمل خوارزميات التعلم شبه خاضع للأشراف	56
01- 22	مبدا عمل خوارزميات التعلم المعزز	57
01 -23	معمارية الشبكات العصبية العميقة	59
01 -24	معمارية الشبكات العصبية الالتفافية	59
01 -25	معمارية الشبكات العصبية المتكررة	60

01 -26	معمارية الذاكرة طويلة قصيرة المدى	**61**
01 -27	معمارية التشفير التلقائي	**61**
01 -28	معمارية الشبكات التوليدية التنافسية	**62**
01 -29	رسم توضيحي لدور خوارزميات تعلم الالة (نموذج تنبؤي) في كشف الاحتيال المالي الالكتروني دراسة حالة بطاقة الائتمان	**64**
02 -30	واجهة المستخدم البرمجية المرئية لبرنامج (Orange)	**95**
02 -31	مراحل بناء انموذج خوارزميات تعلم الالة لكشف الاحتيال المالي الالكتروني	**96**
02 -32	مصفوفة الارتباك	**98**
02 -33	منحنى ROC	**100**
02 -34	المساحة تحت منحنى خصائص تشغيل المستقبل	**100**
02 -35	تمتيل نظري لمخطط المعايرة يوضح العلاقة بين الثقة المتوقعة والدقة الفعلية	**101**
02 -36	منحنى الرفع (Lift curve)	**102**
02 -37	عرض اولي لمجموعة البيانات المستخدمة في الدراسة	**105**
02 -38	الإحصاءات الوصفية لمتغيرات الدراسة الخاصة بالبيانات المستخدمة	**106**
02 -39	توزيع المعاملات الاحتيالية والغير احتيالية لمجموعة البيانات المستخدمة	**110**
02 -40	الارتباط بين متغيرات بيانات الدراسة	**110**
02 -41	تحسين وتدريب خوارزمية الغابة العشوائية	**113**
02 -42	مصفوفة الارتباك لأنموذج خوارزمية الغابة العشوائية	**114**
02 -43	مقاييس أداء انموذج خوارزمية الغابة العشواءية	**115**
02 -44	منحنى (ROC) عند الفئة 0 المعاملات الطبيعية	**118**
02 -45	منحنى (ROC) عند الفئة 1 المعاملات الاحتيالية	**119**
02 -46	منحنى الأداء، عند فئة المعاملات الاحتيالية	**120**
02 -47	منحنى الأداء، عند فئة المعاملات الطبيعية	**121**
02 -48	مخطط المعايرة، عند فئة المعاملات الاحتيالية	**121**
02 -49	مخطط المعايرة، عند فئة المعاملات الطبيعية	**122**
02 -50	سير العمل النهائي لأنموذج خوارزمية الغابة العشوائية داخل برنامج (Orange data mining)	**123**
02 -51	أهمية المتغيرات لأنموذج الغابة العشوائية باستخدام مقياس (Recall) مع 5 تبديلات	**124**

قائمة الجداول والاشكال والاختصارات

الاختصار أو الرمز	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
FTFA	Financial Action Task Force	مجموعة العمل المالي
OECD	Organization for -Economic Co - operation and Development	منظمة التعاون والتنمية الاقتصادية
AI	Artificial intelligence	الذكاء الاصطناعي
ML	Machine Learning	تعلم الالة
AUC	Area Under the Curve	المساحة تحت المنحنى
ROC	Recevier Operating Characteristic	منحنى خصائص تشغيل المستقبل
AUROC	Area Under the Roc	المساحة تحت منحنى خصاءص تشغيل المستقبل
DT	Decision Tree	شجرة القرار
RF	Random Forest	الغابة العشوائية
LSTM	Long Short -Term Memory	الشبكات العصبية المتكررة
RNN	Recurrent Neural Network	الشبكات العصبية المتكررة
CNN	Convolutional Neural Network	الشبكات العصبية الالتفافية
DNN	Deep Neural Network	الشبكات العصبية العميقة
GB	Gradient Boosting	التعزيز بالتدرج
GBM	Gradient Boosting Machine	نموذج التعزيز التدريجي
SVM	Support Vector Machine	الة المتجهات الداعمة
GAN	Generation Adversarial Network	الشبكات التوليدية التنافسية
DQL	Deep Q Learning	التعلم العميق Q
PCA	Principal Component Analysis	تحليل المكونات الأساسية
LOF	Local Outlier Factor	عامل القيم الشاذة المحلي
IF	Isolation Forest	غابة الغزل
KNN	K-Nearest Neighbors	خوارزمية أقرب الجيران
ANN	Artificial Neural Network	الشبكات العصبية الاصطناعية
MCC	Matthews Correlation Cofficient	معامل ارتباط ماتيوز
CV	Cross Validation	التحقق المتقاطع
CA	Classification Accuracy	الدقة الكلية

مقدمة

مقدمة

- **ا. توطئة:**

يشـــهد قطاع التكنولوجيا مالية في الســـنوات الأخيرة تطورا متســـارعا وغير مســـبوق، مدفوعا بالتحول الرقمي الشامل الذي مس مختلف الأنشطة المالية والمصرفية، حيت أصبحت المعاملات الإلكترونية تمثل جزءا أساسيا من حياتنا اليومية للأفراد والمؤسسات على حد سواء. وقد ساهم هدا التحول في توسيع نطاق الخدمات المالية، سواء عبر البنوك التقليدية، أو منصـــات التجارة الإلكترونية أو أنظمة الدفع الرقمية الحديثة، مما أدى إلى ارتفاع كبير في حجم المعاملات وسرعتها وتنوعها.

غير ان هدا التحول بالرغم ما يحمله من مزايا، افرز في المقابل تحديات جديدة، أبرزها ظاهرة الاحتيال المالي الالكتروني التي أصـبحت اكتر تعقيدا وتنظيما، حيت يعتمد المحتالون على أسـاليب متطورة تسـتغل الثغرات التقنية والســـلوكية في ان واحد. ولم تعد الطرق التقليدية المعتمدة على القواعد الثابتة او المراقبة اليدوية كافية لمواجهة هدا النوع من الجرائم نظرا لسرعتها وقدرتها على التكيف مع أنظمة الحماية.

وعلى المسـتوى النظري، يتنوع الاحتيال المالي الالكتروني ليشـمل عدة مجالات، متل الاحتيال البنكي، احتيال في التامين، بطاقات الدفع، احتيال في التجارة الإلكترونية، والتمويل الجماعي والعملات المشـفرة. غير ان هدا التنوع لا يعكس بالضرورة نفس درجة الانتشار في جميع البيئات، حيت تختلف طبيعة الاحتيال السائد من دولة لأخري تبعا لمســتور التطور الرقمي، وســلوك المســتخدمين، والبنية التحتية المالية. وفي هدا الإطار، تشـير المعطيات الواقعية وانطلاقا من الشـــكاوى والحالات المتداولة في المجتمع أن الاحتيال المرتبط بالمعاملات المالية اليومية والتحويلات الإلكترونية يعد النوع الأكثر انتشـــارا في البيئة الجزائرية مقارنة ببعض أنواع الاحتيال الأخرى التي تزال محدودة الانتشـــار كالاحتيال المالي الالكتروني في العملات المشـــفرة مثلا, لذلك برزت الحاجة إلى دراســـة هدا النوع من الاحتيال بشكل معمق والتركيز عليه في الجانب التطبيقي باعتباره الأكثر حضورا في الواقع الجزائري مقارنة بغيره من الأنواع الأخرى من الاحتيال المالي الالكتروني.

وأمام هدا التحدي المتنامي باســـتمرار برزت خوارزميات التعلم الألي كأحد اهم الحلول المتقدمة القادرة على تحليل الكميات الضخمة من البيانات في وقت قصير، واكتشاف الأنماط الغير طبيعية التي قد تشير الى وجود نشاط احتيالي، بالإضـافة إلى قدرتها على التعلم المسـتمر وتحسـين أداءها بمرور الوقت والتكيف مع الأسـاليب الاحتيالية الجديدة، وقد اثبت هده الخوارزميات فعاليتها في الكثير من التطبيقات المالية خاصـــة في كشـــف الاحتيال المالي الالكتروني، حيت تمكنت من تحقيق مســـتويات عالية من الدقة وفي الوقت الفعلي ســـواءا من حيت الكشـــف عن العمليات الاحتيالية (Fraud detection) أو تقليل الإنذارات الكاذبة (False postive) مقارنة بالأساليب التقليدية القائمة على القواعد.

وانطلاقا من دلك تعتمد هده الدراســـة على مقاربة مزدوجة تجمع بين الجانب النظري والجانب التطبيقي، حيت يتم في الجانب النظري اسـتعراض مختلف أنواع الاحتيال المالي الالكتروني واهم خصـائصـه واسـاليبه ومفاهيم

أساسية حول خوارزميات تعلم الالة وأنواعها وألية عملها، بينما في الجانب التطبيقي يتم التركيز على نوع محدد من الاحتيال المرتبط بالمعاملات المالية، ودلك باستخدام بيانات (Fraud Detection Transactions Dataset) التي تحاكي هدا النوع من العمليات وتوفر بيئة مناسبة لبناء واختبار النماذج الذكية. وذلك من خلال بناءا نموذج يعتمد على خوارزمية الغابة العشوائية (Random Forest) باستخدام برنامج (Orange Data mining) بهدف الكشف عن العمليات الاحتيالية وتقييم فعالية النموذج في بيئة اصطناعية تحاكي الواقع العملي.

- **ب. طرح الإشكالية:**

في ظل التوسع السريع للمعاملات المالية الإلكترونية ،لم يعد الاحتيال المالي الالكتروني مجرد خطر محتمل، بل اصبح واقعا متزايد الحدوث يفرض نفسه بقوة داخل الأنظمة المالية الحديثة، حيت تواجه المؤسسات المالية صعوبات حقيقية في تتبع العمليات المشبوهة ويمتد ليؤثر بشكل مباشر على تقه المستخدمين في الخدمات المالية الرقمية ويزيد من حجم الخسائر التي قد تتكبدا المؤسسات والأفراد على حد سواء ومع تطور أساليب المحتالين، أصبحت الطرق التقليدية عاجزة عن مواكبة هدا النوع من التعقيد وهو ما يعكس بوضوح ان مشكلة الاحتيال المالي الالكتروني لم تعد مسالة نظرية بل أصبحت إشكالية واقعية تتطلب حلول فعالة وعملية ..ورغم تنوع مجالات الاحتيال المالي الالكتروني إلا أن الواقع الجزائري يبرز هيمنة الاحتيال المرتبط بالمعاملات اليومية باعتباره الأكثر انتشارا وسهولة للاستهداف مما يجعل دراستها بشكل معمق ضرورة ملحة لبناء نموذج قادر على التصدي لهدا النوع من التهديدات وفي هدا السياق تبرز خوارزميات تعلم الالة كأدوات واعدة قادرة على تحليل البيانات وكشف الاحتيال المالي الالكتروني بشكل مناسب وفي الوقت الفعلي بما يساهم من الحد من هده الظاهرة وتقليل أتارها السلبية .وبناءا على ما سبق، يمكن صياغة الإشكالية الرئيسة كمايلي:

كيف تساهم خوارزميات تعلم الألة في كشف الاحتيال المالي الالكتروني؟

وتتفرع تحت هده الإشكالية الأسئلة الفرعية التالية:

- ما هو الاحتيال المالي الالكتروني ومجالاتها وأساليبه؟
- ماهي خوارزميات تعلم الالة وخصائصها مقارنة بالطرق التقليدية القائمة على القواعد؟
- ماهي خصائص بيانات المعاملات المالية المستخدمة في الجانب التطبيقي؟
- ما الخطوات اللازمة لمعالجة البيانات وبناء نموذج لكشف الاحتيال المالي الالكتروني؟
- كيف يمكن بناء نموذج باستخدام خوارزمية الغابة العشوائية وتقييم أداءه في كشف الاحتيال المالي الالكتروني بواسطة برنامج (Orange Data mining)؟

- **ت. فرضيات الدراسة:**

بغية الإجابة على التساؤلات السابقة قمنا بصياغة الفرضيات التالية:

الفرضية الاولى :

- الفرضـــية الصـــفرية H0: لا يحقق انموذج خوارزمية الغابة العشـــوائية أداء كافيا في اكتشـــاف الاحتيال المالي الالكتروني بناءا على مقاييس تقييم الأداء.
- الفرضـــية البديلة H1: يحقق انموذج خوارزمية الغابة العشـــوائية أداء عاليا وفعالا في اكتشـــاف الاحتيال المالي الالكتروني وفق مقاييس تقييم الأداء.

الفرضية الثانية:

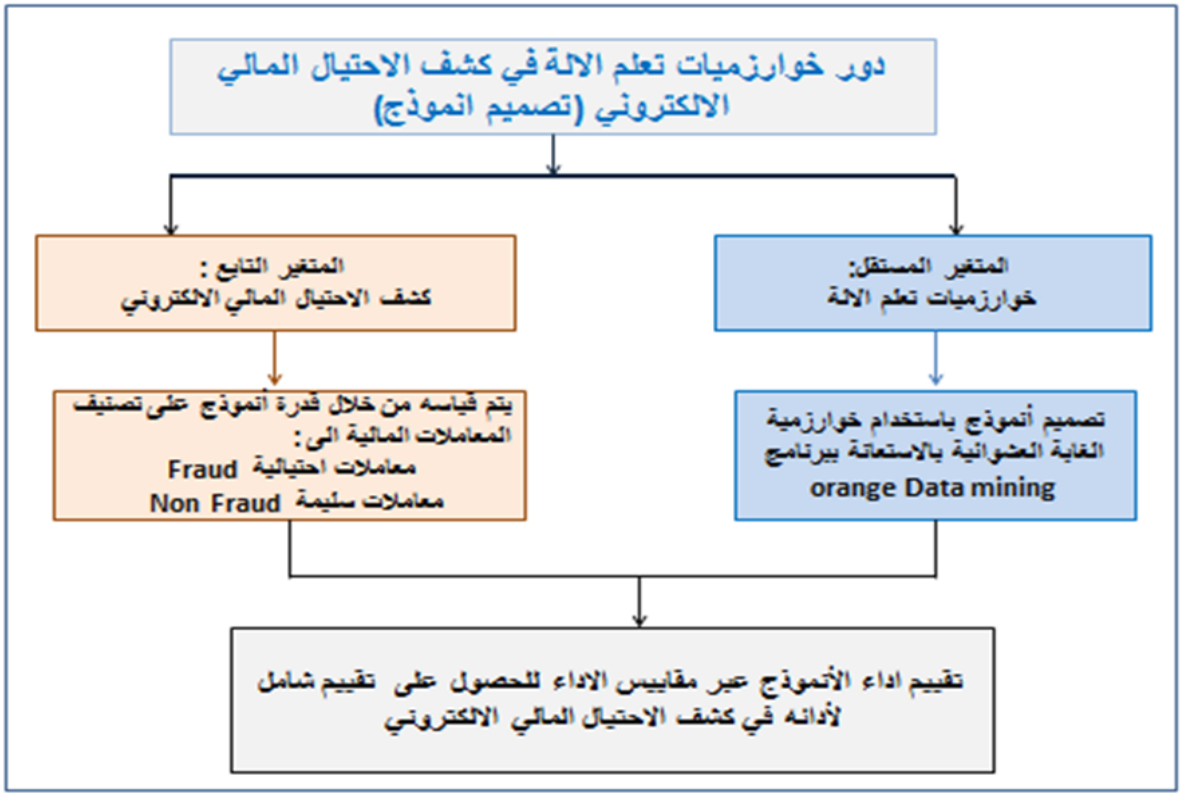
- الفرضية الصفرية H0: لا يظهر تحليل أهمية المتغيرات لا نموذج الغابة العشوائية ان بعض خصائص المعاملات المالية، تؤدي دورا مهما في كشف الاحتيال المالي الالكتروني.
- الفرضـــية البديلة H1: يظهر تحليل أهمية المتغيرات لا نموذج الغابة العشـــوائية ان بعض خصـــائص المعاملات المالية، تؤدي دورا مهما في كشف الاحتيال المالي الالكتروني.

- **ث. نموذج الدراسة:** يتمثل أنموذج الدراسة في العلاقة بين المتغيرات التالية:

المتغير المستقل: خوارزميات تعلم الالة، وفي درستنا شملت تصميم انموذج باستخدام خوارزمية الغابة العشوائية (Random Forest)، والتي تم تنفيذها بالاستعانة ببرنامج (Orange Data Mining).

المتغير التابع: كشـف الاحتيال المالي الالكتروني، ويتم قياسـه من خلال قدرة أنموذج المصـمم على تصـنيف المعاملات المالية: إلى سليمة (Non-Fraud)احتيالية (Fraud).

ويتم تقييم هده القدرة عبر مقاييس الأداء والمتمثلة في: الدقة الكلية (Classification Accuracy)، الدقة الإيجابية (Precision)، الاســـتذكار (Recall)، معامل F1Score ، النوعية (Specificity)، معامل ارتباط ما تيوس(Mcc)، منحنى خصـائص التشـغيل (Roc analysis)، المسـاحة تحت المنحنى (Auc-ROC)، مخطط المعايرة (Calibration Plot)، منحنى الأداء (Performance Curve). وذلك من أجل الحصول على تقييم اكتر شمولية.



الشكل 1: نموذج الدراسة، من اعداد الطالبة

- **ج. أهداف الدراسة:**

تهدف دراسة موضوع دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني الى:

- دراسة مختلف أنواع وأساليب الاحتيال المالي الالكتروني نظريا.
- معرفة أنواع خوارزميات تعلم الالة والية عملها وتحليل دورها في كشف الاحتيال المالي الالكتروني.
- التركيز تطبيقيا على الاحتيال المرتبط بالمعاملات المالية الأكثر انتشـــارا في البيئة الجزائرية المرتبط بالمعاملات المالية.
- تصـميم أنموذج لخوارزميات تعلم ألة باستخدام خوارزمية الغابة العشوائية بواسطة بيانات محاكاة اصـطناعية من منصة (Kaggle) عبر برنامج (Orange Data Mining).
- تقييم أداء أنموذج الغابة العشوائية في كشف الاحتيال المالي الالكتروني باستخدام مؤشرات تقييم الأداء
- تقديم أنموذج قابل للتكييف على البيئة الجزائرية والبيانات الحقيقية.

- **ح. أهمية الدراسة:**

تبرز أهمية هده الدراســـة كونها تعتبر من اكتر التحديات تعقيدا في قطاع التكنولوجيا مالية ، إذ أن التوســـع الكبير في الخدمات المالية الرقمية و اســـتخدامها اليومي ادى بشـــكل حتمي الى تزايد ممارســـات الاحتيال المالي الالكتروني وتطور أساليبه المعتمدة على الثغرات التقنية والسلوكية للأفراد بالإضـافة إلى ربط الجانب النظري الشـامل

لأنواع الاحتيال المالي الالكتروني وأســـبابه ومفهوم خوارزميات تعلم الالة وألية عملها والجانب التطبيقي الذي يركز على النوع الأكثر انتشـارا في البيئة الجزائرية باسـتخدام بيانات اصـطناعية محاكاة كما تسـهم الدراسـة في توسـيع المعرفة الأكاديمية المتعلقة بتطبيق خوارزمية الغابة العشـــوائية في مجال كشـــف الاحتيال المالي الالكتروني وتدعم الجهود الرامية إلى تطوير أنظمة دفع اكتر أمانا مما يوفر نموذجا يحاكي البيئة الحقيقة الجزائرية يمكن تســـتفيد منه البنوك والمؤسسات المالية محليا ودوليا.

- **خ. مبررات ودوافع اختيار موضوع الدراسة:**

– الرغبة الشخصية والميول لتعلم تقنيات تعلم الالة وألية عملها.

– الانتشار الواسع للاحتيال المالي الالكتروني عالميا وارتفاع خسائره.

– ظهور خوارزميات تعلم الالة كأدوات فعالة لكشـــف الاحتيال المالي الالكتروني وقدرتها على معالجة كميات كبيرة من البيانات.

– أهمية تعزيز الأمن المالي الرقمي وزيادة ثقة الأفراد في الخدمات المالية الرقمية.

– حاجة السوق إلى حلول مالية سريعة وأمنة في نفس الوقت.

- **د. حدود الدراسة:** وتمثلت حدود الدراسة في:

- الحدود الموضـــوعية: لتركيز في الجانب النظري على مختلف أنواع الاحتيال المالي الالكتروني وفي الجانب التطبيقي على النوع الأكثر انتشـــار في الجزائر الاحتيال في المعاملات المالية الإلكترونية وذلك من خلال الاعتماد على بيانات محاكاة اصـــطناعية عالية المخاطر من منصـــة (kaggle) (Fraud Détection Transactions Dataset).

- الحدود الزمانية: حدد الفترة الزمنية وفق مايلي:

– الحدود الزمنية لعينة الدراسة: تم اختيار بيانات اصطناعية محاكاة تخص المعاملات المالية لسنة 2023

- الحدود المكانية: لا ترتبط الدراسـة بمكان جغرافي محدد باعتبار أنها تعتمد على بيانات محاكاة اصـطناعية مأخوذة من منصـة (Kaggle) مع محاولة إسقاط النتائج على البيئة الجزائرية من خلال التركيز على النمط الأكثر انتشارا.

- **ذ. منهجية الدراسة والأدوات المستخدمة:**

- **منهجية الدراسة:**

من اجل تحقيق أهداف الدراسة، تم اتباع المنهج الوصفي في الدراسة النظرية، حيت تم إجراء مسح نظري في الأدبيات المتعلقة بالاحتيال المالي الالكتروني وخوارزميات تعلم الالة، وعرض اهم الدراسات السابقة العربية والأجنبية، وذلك من اجل تحقيق نوع من الربط بين التراكم المعرفي (النظري) والعمل التطبيقي. اما في الدراســة التطبيقية فقد تم

اعتماد المنهج التجريبي من خلال تصميم أنموذج عملي باستخدام خوارزمية الغابة العشوائية، وتقييمه وذلك بالاعتماد على بيئة برنامج (Orange Data mining).

- **الأدوات المستخدمة:**

- البيانات (عينة الدراسة): قاعدة بيانات اصطناعية محاكاة متوفرة في منصة (kaggle) بعنوان: (Fraud Detection Transactions Dataset) تخص المعاملات المالية لسنة 2023.
- البيئة البرمجية العملية: برنامج (Orange Data mining).
- خوارزمية الغابة العشوائية.
- مؤشرات تقييم أداء النموذج.

ر. صعوبات الدراسة:

خلال إنجازنا لهذا البحث الأكاديمي اعترضتنا بعض الصعوبات من أهمها ما يلي:

- عدم إمكانيات الحصول على بيانات حقيقية من المؤسسات المالية الجزائرية لاختبار الدراسة عليها نظرا لسرية المعلومات.
- محدودية الدراسات العربية التي تجمع بين الاحتيال المالي الالكتروني وتطبيقات تعلم الالة.
- نقص البيانات المتوازنة والبيانات القابلة للتفسير النتائج.
- تحديات معالجة البيانات الكبيرة.
- الاعتماد على بيانات اصطناعية محاكاة بدل البيانات الواقعية، قد يحد من تعميم النتائج بشكل كامل على الواقع الجزائري.

ز. تقسيمات الدراسة

لتحقيق الإحاطة الشاملة بجوانب الموضوع تم تقسيم هده الدراسة إلى فصلين:

- **الفصل الأول:** يشمل الإطار النظري للموضوع قمنا بتقسيمه إلى ثلاثة مباحث في المبحث الأول: قمنا بعرض مفهوم الاحتيال المالي الالكتروني وخصائصه وأركانه بالإضافة إلى أساليبه وأتاره، وقصور الطرق التقليدية في الكشف عنه ،تم في المبحث التأني قمنا بتسليط الضوء على الأسس النظرية للذكاء الاصطناعي وتعلم الالة تم خوارزميات تعلم الالة وألية عملها وأنواعها ، بأسلوب متدرج ومنطقي بالإضافة إلى استظهار دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني، أما المبحث الثالثة خصص للدراسات السابقة الأجنبية والعربية التي لها علاقة بموضوع دراستنا والمقارنة بينها وبين الدراسة الحالية.
- **الفصل الثاني:** يخص الجانب التطبيقي للدراسة حيت قمنا بتقسيمه لمبحثين: في المبحث الأول، تم عرض منهجية الدراسة التطبيقية والبيئة البرمجية المستخدمة، تطرقنا فيه إلى تحديد عينة الدراسة (البيانات المستخدمة) ومتغيراتها وأسباب اختيارها وتعريف بيئة العمل المستخدمة (Orange Data mining) بالإضافة إلى عرض خطوات

العمل نظريا. أما في المبحث الثاني قمنا بالبناء والتصـــميم الفعلي لأنموذج دراســـتنا التطبيقية بالاعتماد على خطوات العمل المحددة سابقا باستخدام خوارزمية الغابة العشوائية وعرض نتائجه مرئيا وتقييم أداءه عبر مؤشرات التقييم إضافة إلى تحديد المتغيرات المستقلة الأكثر تأثيرا في كشف الاحتيال.

وفي الأخير نختم موضوعنا هذا بتلخيص واختبار الفرضيات التي طرحت في مقدمة البحث، تم عرض للنتائج المتواصل إليها، وأخيرا قمنا بتقديم اقتراحات بناءاً على هده النتائج، إضافة إلى أفاق الدراسة.

الفصل الأول:

الأدبيات النظرية

للاحتيال المالي الالكتروني

وخوارزميات تعلم الالة

تمهيد:

أصبحت المعاملات المالية الإلكترونية جزءا أساسيا من الحياة اليومية للأفراد والمؤسسات، الأمر الذي ساهم في تسهيل العمليات المالية وزيادة سرعتها وفعاليتها، غير أن هدا التطور صاحبه تزايد ملحوظ في مخاطر الاحتيال المالي الالكتروني، نتيجة اعتماد المحتالين على أساليب رقمية متطورة يصعب كشفها بالطرق التقليدية، مما فرض على المؤسسات المالية ضرورة البحث عن حلول حديثة واكتر كفاءة لمواجهة هده التهديدات المتزايدة.

وفي ظل هذا التطور التكنولوجي، برزت خوارزميات تعلم الالة كأحد تطبيقات الذكاء الاصطناعي المستخدمة في المجال المالي، لما تتميز به من قدرة على تحليل كميات ضخمة من البيانات واكتشاف الأنماط الغير طبيعية والتنبؤ بالمعاملات الاحتيالية بدقة وسرعة عالية، الأمر الذي جعلها أداة فعالة في دعم أنظمة الحماية وتعزيز آليات الكشف المبكر عن الاحتيال المالي الالكتروني.

ومن هدا المنطلق، يهدف هدا الفصل إلى الإحاطة بالجوانب النظرية المتعلقة بموضوع الدراسة، من خلال التطرق لمختلف المفاهيم المرتبطة بالاحتيال المالي الالكتروني وخوارزميات تعلم الالة، إضافة إلى إبراز دور هده الخوارزميات في كشف الاحتيال المالي الالكتروني، مع مراجعة مجموعة من الدراسات السابقة ذات الصلة بموضوع الدراسة الحالية وعليه تم تقسيم هدا الفصل إلى ثلاثة مباحث رئيسية كمايلي:

المبحث الأول: الإطار المفاهيمي للاحتيال المالي الالكتروني.

المبحث الثاني: الإطار المفاهيمي لخوارزميات تعلم الالة ودورها في كشف الاحتيال المالي الالكتروني.

المبحث الثالث: الدراسات السابقة المتعلقة بموضوع الدراسة الحالية.

المبحث الأول: الإطار المفاهيمي للاحتيال المالي الالكتروني

في ظل التطور التكنولوجي يشهد المجال المالي تزايدا ملحوظا في استخدام الوسائل الإلكترونية، مما أدى الى ظهور أنماط جديدة من الجرائم وعلى راسها الاحتيال المالي الالكتروني، ونظرا لتعدد أشكاله سيتم في هدا المبحث التطرق إلى مفهومه وخصائصه وأهم مجالاته وأساليب تنفيذه ومدى تأثيره على الأفراد والمؤسسات المالية وعجز الطرق التقليدية في كشفه، وكل هدا بهدف تقديم رؤية شاملة تساعد على فهم الظاهرة كتمهيد لطرق كشفها.

المطلب الأول: مفاهيم الاحتيال المالي الالكتروني.

يعد الاحتيال المالي الالكتروني، من أبرز الجرائم المستجدة في عصر التحول الرقمي، حيت يستغل التقنيات الحديثة لخداع الضحايا وتحويل الأموال بطريقة غير قانونية. ولان نجاح آلية كشفه يتطلب فهما دقيقا لطبيعته، يتناول هدا المطلب تعريفه، ويستعرض الأدبيات النظريات المفسرة لدوافعه، تم يسلط الضوء على خصائصه وأركانه وأسبابه، تمهيدا لتحليل مجالاته وأساليبه في المطالب اللاحقة.

الفرع الأول: تعريف الاحتيال المالي الالكتروني ودوافعه النظرية.

يعتبر الاحتيال المالي الالكتروني من أخطر الجرائم التي أفرزتها التكنولوجيا الحديثة خاصة وانه يجمع بين أساليب الخداع التقليدي والوسائل التقنية المتطورة وقد حظي هدا السلوك الإجرامي باهتمام واسع اتمر عنه جملة من التعاريف التي حاولت الإحاطة بمختلف جوانبه وعكست زاوية رؤيتها لهده الظاهرة ونستعرض أبرزها ما يلي:

- **تعريف (01):** عرفته منظمة الإنتربول (Interpol) في تقرير تقييم الاحتيال المالي لسنة 2024 على انه :فئة شاملة تضم مجموعة واسعة من الأنشطة غير القانونية التي تهدف إلى تحقيق مكاسب مالية من خلال أفعال مخادعة ومتعمدة ضد الأفراد أو الكيانات وإلحاق الضرر بهم ويقوم هذا الاحتيال جوهريا على التفاعل بين عنصرين أساسيين هما الدافع الحصول على ربح مالي الخداع بأشكال متنوعة، وما يصبغه بالصفة الإلكترونية هو اعتماده على تقنيات المعلومات والاتصالات، مما يجعله جريمة عابرة للحدود والقارات بطبيعتها، ويسمح للمجرمين بالعمل بهويات مجهولة لتنفيذ عملياتهم على نطاق واسع[1]
- **تعريف (02):** تعريفه وفقا للتقرير المشترك بين مجموعة العمل المالي (FTFA) بالتعاون مع مجموعة ايغمونت: على انه التمويل الغير مشروع الناجم عن الاحتيال الذي يتم تمكينه من خلال البيئة الإلكترونية أو تنفيذه فيها والذي ينطوي على جرائم عابرة للحدود متل الجهات الفاعلة العابرة للحدود وتدفقات الأموال وأساليب الهندسة الاجتماعية الخادعة للتلاعب بالضحايا والصول لمعلوماتهم السرية [2]

[1] INTERPOL, INTERPOL GLOBAL FINANCIAL FRAUD ASSESSMENT, MAY 2024, P5-7
[2] FATF, EGMONT GROUP, INTERPOL, ILLICITE FINANCIAL FLOWS FROM CYBER -ENABLED FRAUD, PARIS, NOVEMBER 2023, P5

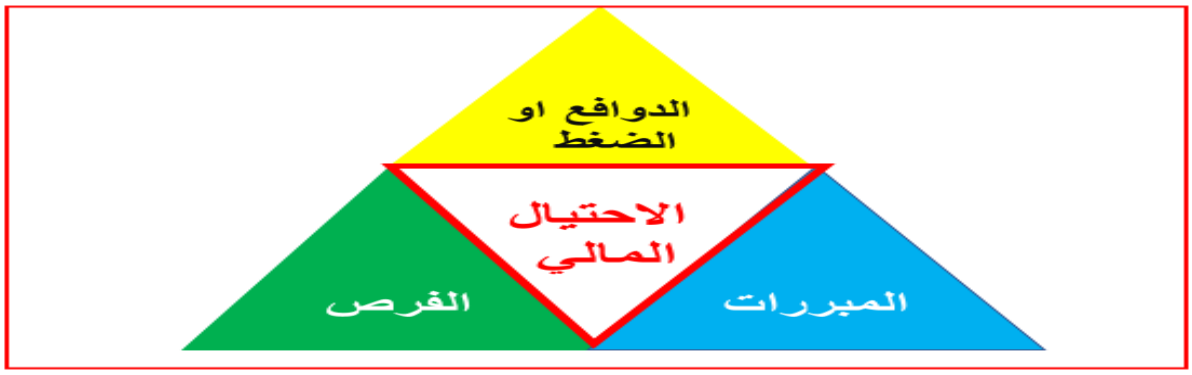
- **تعريف (03):** عرفته وزارة العدل الأمريكية بأنه مخطط احتيالي يستخدم مكونًا واحدًا أو أكثر من مكونات الإنترنت، مثل غرف الدردشة أو رسائل البريد الإلكتروني أو لوحات الرسائل أو مواقع الويب، لعرض طلبات احتيالية على الضحايا المحتملين، أو لإجراء معاملات احتيالية، أو لتحويل عائدات الاحتيال إلى مؤسسة مالية أو إلى جهات أخرى مرتبطة بالمخطط[3]
- **تعريف (04):** هو عمل مخادع متعمد مصمم لتزويد الجاني بمكاسب غير قانونية وغير مشروعة او حرمان الضحية من حقها وفي سياق البيانات الضخمة الاحتيال المالي الالكتروني يظهر على انه شذوذ يختلف عن السجلات المعتادة وهي جريمة متطورة تستدعي استخدام تقنيات ومناهج ذكية من مجال التعلم الآلي للكشف عن الأنماط الاحتيالية المشبوهة والمتغيرة حيت تمثل تحديا تقنيا كبيرا لصناعة التكنولوجيا المالية لأنها بيئة معرضة للاستغلال المستمر.[4]
- **ومن خلال ما سبق نعرف الاحتيال المالي الالكتروني على انه :** هو نشاط غير قانوني عابر للحدود يعتمد على الخداع المعتمد واستغلال الفضاء الرقمي والثغرات التقنية وأساليب التلاعب النفسي من أجل التلاعب بالضحايا وسلب أموالهم بطريقة غير مشروعة مما يجعله تحديا تقنيا يتطلب حلولا ذكية للكشف عنه والحد من أضراره.
- **الخلفية النظرية لدوافع الإحتيال المالي الالكتروني:** مع تسارع وتيرة الاحتيال المالي الالكتروني، برزت الحاجة لنماذج تفسيرية حديثة تواكب هذا التعقيد الرقمي، فالحماية الحقيقية من هده الجريمة لا يبدا من التحصينات التقنية فحسب، بل ينطلق من الفهم العميق للجوانب النفسية والظروف المحاطة بالمحتال المالي، لدلك سعى الفكر لتفكيك شيفرة دوافع المحتالين الماليين وراء ممارسة عملية الاحتيال المالي مهما كانت وسيلة تنفيذه عبر سلسلة من النظريات فهي ليست مجرد اطر نظرية بل أيضا تبين دوافع المحتالين لممارسة عملية الاحتيال مهما كانت طبيعته والظروف التي مكنتهم من ذلك وتفسير لسلوكهم حيت أن فهم الجوانب النفسية والهيكلية للمحتالين يعد خطوة محورية في الوقاية من الاحتيال حيت برزت كل نظرية على أنقاض سابقتها مكملة ومتممة لها ومن ابرزها:

[3] LINA FERNANDES, FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES, ASIA PACIFIC JOURNAL OF MARKETING & MANAGEMENT REVIEW. VOL2, NO 3, MARCH 2013, P24

[4] STOGANOVIC BRANKA, ET AL, "FOLLOW THE TRAIL: MACHINE LEARNING FOR FRAUD DETECTION IN FINTECH APPLICATIONS SENSORS ", VOL 21, NO.5, 02/2021, P2

أولا: نظرية مثلث الاحتيال لكريسي 1950:

الشكل رقم 01-01: مثلث الاحتيال المالي



المصدر: من إعداد الطالبة، بالاعتماد على: سامر هايل الصباغ، حسين احمد دحدوح، مدى التزام مدققي الحسابات بتقييم عوامل مخاطر الأخطاء الجوهرية الناجمة عن الاحتيال (دراسة ميدانية في هيئة الأوراق والأسواق المالية السورية)، 12 العدد 2، سنة 2016، ص 383

تعود جدور هده النظرية إلى سنة 1950، حين استهل عالم الجريمة دونالد كريسي دراسته لظاهرة الاحتيال المالي، منطلقا من تساؤلات بحتيه جوهرية حول الدوافع التي تجعل الأفراد يرتكبون هده الجرائم وما الذي يدفع الأشخاص الموثوق بهم إلى انتهاك هده الثقة، فاستند في دراسته على منهج ميداني على مدار 5 أشهر، شمل إجراء مقابلات مع 250 مجرم ممارس للاحتيال، وقد خلصت نتائج بحته إلى أن الفرد الذي يتمتع بمستوى من الثقة في بدايته قد يندفع لانتهاكها تحت تأثير ظروف معينة، مؤكدا أن وقوع فعل الاحتيال المالي لا يحدث إلا بتوفر ثلاثة عوامل رئيسية هي الدافع والفرصة والمبررات نشرحها كما يلي:

- **الضغط أو الدافع:** هو المحرك الذي يدفع الشخص للاحتيال المالي نتيجة ضغوط مالية أو غير مالية وهو المسؤول عن 95 بالمئة من حالات الاحتيال وتتنوع أشكاله بين ضغوط شخصية مهنية خارجية[5].
- **المبررات:** هي محاولة إقناع الجاني نفسه بان فعله مشروع وليس احتيال أو سرقة بوضع مصلحته فوق مصلحة العمل أو خلق اعدر متل هدا: حقي، الشركة مدينة لي، الجميع يفعل ذلك[6] .

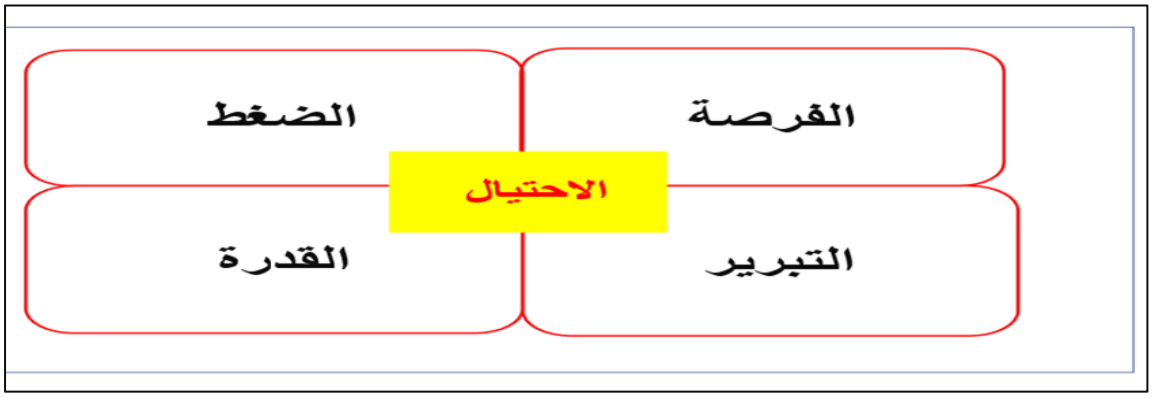
[5]ABDULLAHI RABI 'U, NOORHAYATI MANSOR. "FRAUD TRIANGLE THEORY AND FRAUD DIAMOND THEORY. UNDERSTANDING THE CONVERGENT AND DIVERGENT FOR FUTURE RESARCHE." INTERNATIONAL JOURNAL OF ACADEMIC RESARCH IN ACCOUNTING, FINANCE AND MANAGMENT SCIENCES, VOL5, NO4 ,2015. P39

[6]MANURUNG, DANIEL T.H, NIKI HADIAN. "DETECTION FRAUD OF FINANCIAL STATEMENT WITH FRAUD OF FINANCIAL STATEMENT WITH FRAUD TRIANGLE." PROCEEDINGS OF 23RD INTERNATIONAL. BUSINESS *RESARCH CONFERENCE*, MARRIOTT HOTEL, MELBOURNE, AUSTRlIA. 18-20 NOV. 2013, PP5.6

الفرص: هي اســـتغلال الثغرات ونقاط الضـــعف في الرقابة الداخلية والنظام ووفقا إلى معيار التدقيق SAS99، يمكن أن تحدث فرص الاحتيال المالي في تلات فئات من الظروف: طبيعة الصـــناعة، المراقبة الغير فعالة، الهيكل التنظيمي للمؤسسة.[7]

ثانيا: نظرية ماسة الاحتيال (معين الاحتيال) 2004

الشكل رقم 01-02: معين الاحتيال المالي



المصدر: من إعداد الطالبة , بالاعتماد على بشرى فاضل الطائي , حسين فخري سلمان، دور التخصص المهني لشركات التدقيق في الكشف عن الاحتيال في القوائم المالية، مجلة العلوم الاقتصادية والإدارية، المجلد 25، العدد 114، سنة 2019، ص 586

تعد هذه النظرية المطورة لنظرية مثلث الاحتيال الكلاسيكية حيت في سنة 2004 قام الباحثان دانا هيرمانسون وديفيد وولف بإضافة ركن رابعا حاسما وهو القدرة الشخصية وتفترض هذه النظرية ان وجود الدافع والفرصة والتبرير لا يكفي وحده لارتكاب الاحتيال المالي. ويقصد بالقدرة: امتلاك الجاني للمؤهلات والسمات الشخصية التي تمكنه من اســـتغلال الثغرات المتاحة، وتحويل فرص الاحتيال إلى واقع عملي، اذ لا يمكن لعملية الاحتيال ان تنجح دون وجود الشخص الذي يمتلك المهارة اللازمة لتنفيذها [8]

تالتا: نظرية خماسي الاحتيال (نظرية البنتاغون)2011:

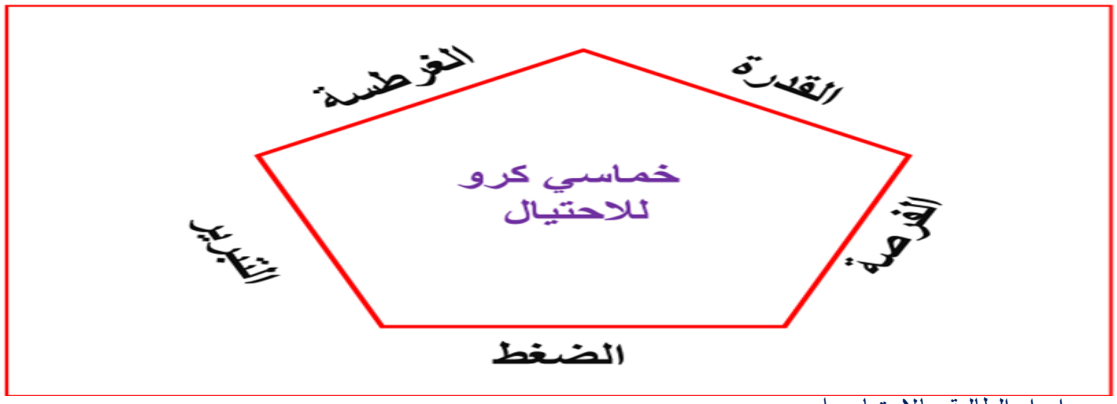
طرح هذه النظرية جوناثان ماركس في عام 2011، الشريك المسؤول عن ممارسات الاحتيال والأخلاقيات في شـركة كرو هورواث للمحاماة كتحسـين إضـافي وامتداد لنظرية مثلث الاحتيال ونظرية ماسـة الاحتيال حيث أضـاف عنصـر خامس للاحتيال وهو الغرطسـة، وتعرف هده الاخيرة على أنها: سـمة غير أخلاقية تتمثل في تضـخم الأنا والاسـتعلاء على حقوق الفرد والشـعور بأن الضـوابط أو سـياسـات الشـركة لا تطبق عليه، وغالبا ما يكون مصـحوبا

[7] د. نصـيف جاسـم الجبوري، ا. م. صـلاح هادي محمد الخالدي، **دور المحاسـبة القضـائية في اكتشـاف عمليات الاحتيال المالي**، مجلة العلوم الاقتصادية والإدارية، المجلد: 19، العدد 70، سنة 2013، ص 462.

[8] WOLFE DAVID. T, HERMANSON DANAR, THE FRAUD DIAMOND: CONSIDERING THE FOUR ELEMENTS OF FRAUD.THE CPA JOURNAL, NEW YORK STATE SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS. VOL 174.NO (12),2004, PP38-39

بالتقليل من شأن الآخرين فهدا الغرور يدفع بعض القيادين للتلاعب بالبيانات المالية للحفاظ على صورتهم المالية من خلال اساءة استخدام السلطة، وهو ما يمهد الطريق للاحتيال المالي[9].

الشكل رقم 01-03: خماسي الاحتيال المالي

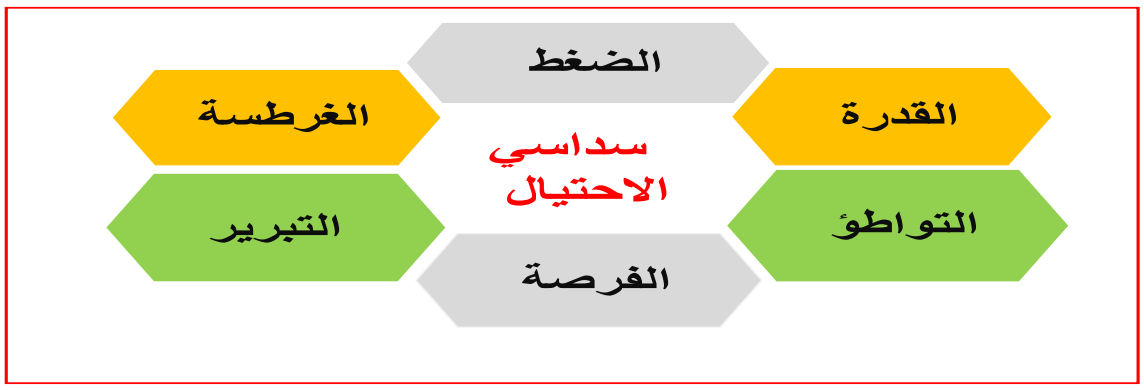


المصدر: من اعداد الطالبة, بالاعتماد على ,

TAUFIQUL AZIZ, RITA YUNIARTI, FRAUD PENTAGON THEORY FOR DETECTION OF FRAUDULENT FINANCIAL REPORTS: A PRELIMINARY STUDY IN MANUFACTURING ENTERPRISES IN INDONESIA, DINASTI INTERNATIONAL JOURNAL OF ECONOMICS, FINANCE & ACCOUNTING, VOL .4, No.1,2023, P5332

رابعا: نظرية سداسي الاحتيال 2019:

الشكل رقم 01_04: سداسي الاحتيال المالي لفوسيناس



المصدر: من اعداد الطالبة , بالاعتماد على :

FAIZ RAHMAN SIDDIQ, BAMBANG SUTOPO , THE FRAUD HEXAGON AS AN ANALYTICAL FRAMEWORK FOR PREDICTING FINANCIAL STATEMENT FRAUD : A SYSTEMATIC LITERATURE REVIEW , JOURNAL OF RESEARCH TRENDS IN SOCIAL SCIENCES AND HUMANITIES ,VOL 3,NO 2,2024,P160

[9] JASELLA SAKWI YANTI , YOSSI DIANTIMALA,NURAINI A TESTING THE CROWES PENTAGON THEORY OF FRAUD ON FINANCIAL STATEMENT FRAUD ,INTERNATIONAL JOURNAL OF MANAGEMENT ,ACCOUNTING AND ECONOMICS ,VOL 11,NO 3, 2024,P300

هي عبارة عن نظرية صـاغها جورجيوس فوسـيناس وهي متممة ومطورة للنظريات التي سـبقتها بإضـافتها عنصـر سـادس وهو التواطؤ وابرزت انه عنصـرا ضـروريا في العديد من عمليات الاحتيال المالي المعقدة وجرائم دو الياقات البيضاء.[10]

- **ويعرف التواطؤ:** بانه تحالف غير مشـروع بين شـخصـين أو اكتر لخداع طرف اخر، وغالباً ما يهدف لارتكاب عمليات احتيال تهدف لسـلب الحقوق حيت يتمكن الشـخص ذو الشـخصـية المقنعة للغاية من إقناع الآخرين بالتواطؤ في عملية احتيال او ببسـاطة غض الطرف عنها حيت يتم التواطؤ اما داخليا بين الموظفين او خارجيا عبر شبكات إجرامية او بين الموظفين وأطراف خارجية مما يجعل اكتشافه صعبا وايقافه تحديا كبيرا. [11]

الفرع الثاني: أسباب الاحتيال المالي الالكتروني:

لقد تعددت أسباب حدوث الاحتيال المالي الالكتروني من أبرزها.

- **ضـعف مسـتويات الوعي الرقمي:** حيت ان توسـع الوصـول إلى الإنترنت، مع غياب الثقافة الرقمية الكافية، جعل الكثير عرضة للوقوع في فخاخ المحتالين بسهولة
- **الاسـتدراج عبر وسـائل التواصـل الاجتماعي** المختلفة وتطبيقات المراسـلة ومنصـات لإغراء الضـحايا بوعود وهمية[12]
- **البرمجيات الاحتيالية كخدمة:** أصبح النظام البيئي للمجرمين السيبرانيين صناعيا ويشمل ما يسمى بالجريمة كخدمة حيث يمكن للمجرمين غير التقنيين الوصـول إلى أدوات سـيبرانية واسـتخدامها دون خبرة باسـتخدام أدوات جاهزة ومشتراة تمكنهم من تنفيذ هجمات احتيالية معقدة.
- **تطور التقنيات الاحتيالية:** اسـتخدام رموز برمجية خبيثة متطورة قادرة على تجاوز تدابير الأمان الحالية مثل المصادقة الثنائية (2FA) والبصمات الحيوية.
- **التحول الرقمي السريع واستغلال الثغرات الناتجة عن الازمات متل:** تأثير جائحة كورونا التي أدت الجائحة إلى تسـريع اعتماد العملاء على الخدمات المالية عن بعد، مما زاد من نطاق وطبيعة مخاطر الاحتيال وفتح فرص للمجرمين لاستغلالها[13].

[10] FAIZ RAHMAN SIDDIQ, BAMBANG SUTOPO, THE FRAUD HEXAGON AS AN ANALYTICAL FRAMEWORK FOR PREDICTING FINANCIAL STATEMENT FRAUD: A SYSTEMATIC LITERATURE REVIEW, OP. CIT, P160

[11] GEORGIOS L, VOUSINAS, ADVANCING THEORY OF FRAUD: THES.C.O.R.E. MODEL. JOURNAL OF FINANCIAL CRIME, VOL 26, NO 1,2019, P 378

[12] INTERPOL, INTERPOL GLOBAL FINANCIAL FRAUD ASSESSMENT, MAY 2024, OP CIT, P14-15

[13] BASEL COMMITTEE ON BANKING SUPERVISION, DIGITAL FRAUD AND BANKING: SUPERVISORY AND FINANCIAL STABILITY IMPLICATIONS, DISCUSSION PAPER, BANK OF INTERNATIONAL SETTLEMENTS, NOVEMBER 2023, P1, ISBAN 92-9197- 978-92-9259-709-2 (online)

- **الاعتماد على الشبكات المترابطة:** تتعرض المؤسسات المالية بشكل خاص لمخاطر الأمن السيبراني نظرًا لبنيتها التحتية الموثوقة واعتمادها على شبكات مترابطة للغاية.. تشمل البنى التحتية للسوق وأنظمة الدفع والتسوية، ومنصات التداول، ومستودعات الأوراق المالية حيث هجوم ناجح قد تكون له عواقب واسعة النطاق
- **انخفاض تكلفة الهجمات:** حيث يتمكن المحتالون من شن هجمات معقدة بتكلفة منخفضة.
- **الأنظمة القديمة الغير محدثة:** حيث تمتلك العديد من الانظمة القديمة الغير مرنة التي لا تملك القدرة على الصمود امام الهجمات الالكترونية الحديثة وبالتالي تكون مستهدفة اكتر للخطر وتحوي على العديد من الثغرات التي تفتح الأبواب لحدوث الاحتيال المالي الإلكتروني.[14]
- **ضعف امن الانترنت:** تعد حماية المستهلكين من القرصنة والسرقة والاحتيال مسألة معقدة. ويؤدي نقص أمن الإنترنت القوي إلى تقويض ثقة المستهلك في المعاملات الإلكترونية والحل الوحيد المتاح هو تحذير العملاء من المواقع الإلكترونية المشبوهة والمحتالين.[15]

الفرع الثالث: خصائص وأركان الاحتيال المالي الالكتروني

يتميز الاحتيال المالي الالكتروني بمجموعة كبيرة من الخصائص تميزه عن الاحتيال المالي التقليدي وهو ما نوجزه في الجدول التالي:

جدول رقم01-01: خصائص الاحتيال المالي الالكتروني

الخاصية	الشرح
البيئة الالكترونية	تتميز بحدوتها ضمن الفضاء الالكتروني، حيث تنفذ عبر نبضات الكترونية غير ملموسة تنتقل عبر الحواسيب وشبكات المعلومات، مستغلة أي ثغرات في انظمة التحكم التقني.
الخبرة التقنية والبساطة	تتطلب الجريمة قدرا من الخبرة الفنية لتتبع ثغرات الشبكات، الا انها تنفذ ببساطة، ومن قبل فردا واحد أحيانا، مما يجعل المستوى العلمي للمجرم مؤثر مباشر في نجاح الاحتيال المالي الالكتروني.
التخفي وسرعة التنفيذ	تتسم بكونها متسترة وغير مرئية للضحية، رغم أنها قد تقع أثناء وجوده على الشبكة وعلى مرأى من عينيه في اغلب الأحيان، حيث يتم إنجازها بسرعة مذهلة تتيح للجاني سرقة الأموال او اتلاف البيانات الخاصة والتجسس عليها.

[14] ANTONIE BOUVERET, CYBER RISK FOR THE FINANCIAL SECTOR: A FRAMEWORK FOR QUANTITATIVE ASSESSMENT, IMF WORKING PAPER, INTERNATIONAL MONETARY FUND, WP /18/143. JUNE 2018, P 10 -11

[15] BADIAA CHIFA, KERROM NESRINE, THE LEGAL REGULATION OF ELECTRONIC BANKING HOW DOES THE MONETARY AND BANKING LOW 09 23 ENHANCE TRUST IN DIGITAL TRANSACTIONS , JOURNAL OF LEGAL AND ECONOMIC RESEARCH, VOLUME 08,ISSUE: 02, 6/ 2025, P213

عابرة للحدود	بفضل الأنترنت تلاشت الحدود المكانية امام انتقال المعلومات، مما سمح بوقوع جرائم احتيالية عابرة للدول، حيت تتوزع اتار الجريمة في مواقع جغرافية متباعدة ومتعددة.
جريمة ناعمة	سميت بالجرائم الناعمة، لأنها لا تعتمد على العنف المادي او المجهود العضلي، بل تركز كليا على استغلال برامج الشبكة العنكبوتية.
صعوبة إثباتها	تكمن صعوبتها في غياب الأثر المادي الملموس للأفعال الاجرامية، مع إمكانية محو الأدلة الرقمية وتدميرها في مدة زمنية تقل عن الثانية الواحدة.
قابلة للتطوير والابتكار	هي جريمة متطورة بطبيعتها ومرتبطة طرديا بالتقدم التقني، فكلما ظهرت تكنولوجيا جديدة، واكبها ظهور أنماط إجرامية مستحدثة.
الاعتماد على الخداع والتضليل	يقوم الاحتيال المالي الالكتروني على تضليل الضحايا والتمويه عليهم لضمان تنفيذ المخطط الاجرامي بنجاح.
صعوبة الاكتشاف	غالبا ما يستغرق اكتشافها وقتا طويلا، وادا اكتشفت قد يمتنع الكثير من الضحايا عن التبليغ خوفا من عواقب الابتزاز والتشهير، مما يرفع نسبة الجرائم الغير مكتشفة مقابل الجرائم المكتشفة.
الهدف المادي الغير مشروع	المحرك الأساسي له، هو سعي الجاني لتحقيق أرباح مالية ضخمة وعوائد مالية بطرق غير مشروعة مخالفة للقانون.
صعوبة تحديد الهوية	نظرا لتعقيدها او تعدد الأطراف المشاركة فيها في الغالب، يصعب تحديد هوية الجاني، حيت وصفت من قبل جهات امنية كالمكتب الفيدرالي الأمريكي بالوباء لصعوبة حصر مرتكبيها.

المصدر , من اعداد الطالبة بالاعتماد على مراجعات سابقة [16] [17] [18]

الفرع الرابع: اركان الاحتيال المالي الالكتروني

الاحتيال المالي الالكتروني يقوم على تلاته اركان، ركن شرعي وركن مادي وركن معنوي من خلال هذه الجزئية سنحاول عرض هده الأركان في الجدول الموالي.

[16] وائل محمد نصيرات، غادة عبد الرحمن الطريف، " جريمة الاحتيال عبر شبكة المعلومات الدولية: دراسة مقارنة النظام السعودي والقانون الأردني، مجلة دفاتر السياسية والقانون ، العدد ،19 جوان ،2018 ص 98

[17] فرحاني رزيقة ,بالرايس زينب ,ضحايا النصب والاحتيال في ظل انتشار وتوسع التجارة الإلكترونية دراسة ميدانية على عينة من الوسط الجامعي -جامعة الشيخ 17العربي التبسي ,-مدكرة ماستر, تخصص انحراف وجريمة , كلية العلوم الإنسانية والاجتماعية ,جامعة الشيخ العربي التبسي تبسة ,سنة ,2025ص50

[18] حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري, مجلة الدارسات القانونية و السياسية, المجلد,6العدد ,20جوان ,2020ص172

الجدول رقم 01-02: اركان الاحتيال المالي الالكتروني

اركان الاحتيال المالي الالكتروني		
- الركن الشرعي: تستمد جريمة الاحتيال المالي الالكتروني صفتها الغير مشروعة من خلال نص المادة 372 من قانون العقوبات الجزائري ورغم غياب نص خاص يحدد بدقة ملامح الجريمة في فضاء الإنترنت الا ان القضاء يعتمد بدقة على عمومية هدا النص التشريعي لإسقاط العقوبة على كافة السلوكيات الاحتيالية، سواء نفدت بطريقة مادية ملموسة او عبر شبكات الأنترنت حيث تضمن نص المادة كل الأفعال المادية المشكلة لجريمة النصب وكان كمايلي : "فكل من توصل إلى استلام أو تلقي أموالا أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على أي منها، أو شرع في ذلك عن طريق الاحتيال بغية الاستلاء وسلب ثروة الغير أو بعضها، أو حتى الشروع في ذلك باستخدام أيا من هذه الأفعال سواء استعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي آو بإحداث	**ب- الركن المادي** تعد جريمة الاحتيال المالي من الجرائم المادية التي تحتاج إلى نتيجة، وبالتالي إلى علاقة سببية، وعليه فالركن المادي لجريمة الاحتيال المادي يقوم على تلاته عناصر وهي كمايلي: أولا: <u>السلوك المادي</u>: يتمحور حول توظيف الوسائل التقنية كالحاسوب والأنترنت كبديل للقوة المادية حيث يعتمد الجاني على الخداع الرقمي والمظاهر الوهمية لسلب أموال الضحية برضاه التام الناتج عن التضليل. تانيا: <u>العلاقة السببية</u>: العلاقة السببية في الاحتيال المالي الالكتروني تتمثل في الصلة المباشرة بين السلوك التدليسي المتمثل في الأساليب التقنية الاحتيالية التي استعملها الجاني وبين انخداع المجني عليه وتسليمه لأمواله، ويتحقق الشروع في الاحتيال المالي الالكتروني بمجرد شروع الفاعل في ممارسة هده المناورات للاحتيال على الضحية واقناعه بتقديم مبالغ مالية.	**الركن المعنوي:** لا يكفي لقيام الجريمة توفر الركنين الشرعي والمادي فقط بل يجب ان تربط الجاني بالفعل الاجرامي صلة هي الركن المعنوي وبما ان الاحتيال الالكتروني من الجرائم العمدية فان هدا الركن يقوم على عنصرين اساسين هما العلم والإرادة. أولا: <u>العلم بالسلوك الاحتيالي</u>: يشترط ان يكون الجاني مدركا تماما بانما يفعله ينطوي على كدب وخداع فمثلا ادا تصرف في منقول لا يملكه وهو يعلم بدلك يثبت الركن المعنوي اما إذا لم يكن على علم بمخالفة تصرفه للقانون ولم يستخدم وسائل تضليل فان الركن المعنوي ينتفي. تانيا: <u>الإرادة في الجرائم المعلوماتية</u>: نقصد بها انه لا يكفي بمجرد القيام بفعل ما في مجال تقنية المعلومات بل لابد من الإرادة الاجرامية حيت يشترط ان يعلم الجاني ان سلوكه مخالف للقانون وان يتعمد تنفيذه فادا دخل شخص نظاما معلوماتيا مسموحا ونتيجة جهله التقني ارتكب خطا غير مقصود الحق الضرر

الأمل بالفوز بأي شيء، أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع أي شيء منها" يعتبر فعل نصب واحتيال .	ثالثاً: النتيجة الاجرامية: تتحقق هذه النتيجة حين يقوم الضحية بتسليم أمواله سواء كانت نقدية أو منقولة للجاني بناءا على تصديقه للأكاذيب والمظاهر الخداعية المعروضة عليه.	بأحد فتكون هنا المسؤولية عن خطا غير متعمد ولا تعتبر جريمة

المصدر : من اعداد الطالبة بالاعتماد على مراجعات سابقة [19] [20]

المطلب الثاني: أنواع وأساليب الاحتيال المالي الالكتروني:

لا يقتصر الاحتيال المالي الالكتروني على نمط واحد، بل يتخذ اشكالا متعددة تتنوع بتنوع المجالات المالية المستهدفة، من بطاقات الدفع والتجارة الالكترونية الى البنوك والعملات المشفرة والتامين وغيرها. وكل نوع يطور اساليبه الخاصة التي تتراوح بين الهندسة الاجتماعية التقليدية والالية وصولا الى التزييف العميق المتطور. يهدف هذا المطلب الى تصنيف الأنواع مع تعريف كل منها وشرح الية حدوت الاحتيال داخلها تم ابراز الأساليب الاحتيال المالي الالكتروني المتبعة.

الفرع الأول: أنواع الاحتيال المالي الالكتروني

يشكل الاحتيال المالي الالكتروني جريمة اقتصادية خطيرة في ظل التحول الرقمي فهو يشمل عدة أنواع مختلفة حيت استفادت من التطورات التكنولوجية لخداع الضحايا بشكل اكتر فعالية فجميعها تخدم نفس الهدف وهو المكسب المالي الغير مشروع ومن بين اهم أنواع الاحتيال المالي الالكتروني ندكر ما يلي:

1. **الاحتيال ببطاقة الدفع الالكتروني: (Payment Card Fraud).**

جدول رقم 01-03: الاحتيال ببطاقة الدفع الالكتروني

تعريفه	الاستغلال الغير مشروع للبيانات الحساسة لبطاقة الدفع الالكتروني من قبل افراد غير مصرح لهم بهدف الاستيلاء على الأصول المالية والممتلكات باستخدام أساليب احتيالية او استغلال الثغرات الأمنية في منصات الدفع الالكتروني والمنصات الغير مؤمنة.[21]

[19] اسية بن بوعزيز ميلود بن عبد العزيز، جريمة الاحتيال المالي في ظل تكنولوجيا المعلومات، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد1،6/ 2024، ص 1368-1370.

[20] ابوبكر التواتي، الياس مالك قرادي، جرائم النصب والاحتيال الإلكتروني في التشريع الجزائري، مذكرة ماستر , تخصص القانون الجنائي والعلوم الجنائية , كلية الحقوق , المركز الجامعي المقاوم الشيخ آمود بن مختار-إيليزي,2025,-ص 16-13

[21] REJWAN BIN SULAIMAN, VITALY SCHETININ, PAUL SANT, REVIEW OF MACHINE LEARNING APPROACH ON CREDIT CARD FRAUD DETECTION, HUMAN -CENTRIC INTELLIGENT SYSTEMS, VOL 1, N 2 ,5/2022, P55

صوره واشكاله	**أولا: <u>الاحتيال من طرف صاحب البطاقة نفسه</u>:** قد تكون لصاحب البطاقة نية سيئة فيقوم باستخدام بطاقة الدفع بطريقة غير مشروعة بإحدى الاشكال التالية: • **استعمال البطاقة بعد انتهاء مدة صلاحيتها:** حيت يستمر العميل في استخدامها بنية التحايل والسرقة رغم علمه بانقضاء مدتها. • **استعمال البطاقة بعد الغاءها:** محاولة اجراء عمليات شرائية او سحب بعد الغاء البطاقة من قبل البنك نتيجة تعتر مالي او مخالفة إدارية. • **تخطي الحد الائتماني المقرر:** لكل بطاقة بنكية سقف معين يلتزم به العميل، ولا يجوز استخدام البطاقة الا في حدود الرصـــيد الســـموح به، الا انه أحيانا يتجاوز العميل هدا الســـقف بطرق احتيالية مخالفة للقانون. **ثانيا: <u>الاحتيال من طرف البنك مصـــــدر البطاقة</u>:** يحدث في الغالب من طرف موظفي البنك او نتيجة تواطؤهم مع الغير بإحدى المظاهر التالية: • **تواطؤ موظف البنك مع حامل البطاقة من خلال:** استصـدار بطاقات ائتمانية ببيانات زائفة، التغاضـي العمدي عن تجاوز سقف السحب واستخدام بطاقات منتهية الصـلاحية، افشـاء السر المهني وتسريب بيانات العملاء الحسـاسـة لاسـيما ذوي الأرصـدة المرتفعة لصـالح عصـابات إجرامية محترفة لغرض تزييفها ونســـخها، مســـتغلين في دلك صـــلاحياتهم التقنية لتعطيل رقابة البنك وتمرير هده العمليات الاحتيالية.[22] **ثالثا: <u>صور أخرى للاحتيال ببطاقة الدفع الالكتروني:</u>** • **الاحتيال من خلال سرقة البطاقة او فقدانها:** استغلال الغير للبطاقة ماديا بعد ضـياعها من صـاحبها او سرقتها لنفيد عمليات غير مشروعة بطرق الكترونية. • **التزييف والتقليد:** التصـنيع الكلي لبطاقات وهمية تحاكي الاصـلية تقنيا (التشفير والهولوغرام)، أو إعادة برمجة بطاقات ملغاة ببيانات حسابات نشطة. • **الطلبات التدليسية والاستيلاء على الحساب:** استخراج بطاقات قانونية من البنك بناءا على هوية مزورة او انتحال صـفة عميل لتغيير بيانات الاتصـال كالعنوان مثلا من اجل اسـتبدال البطاقة ببديل يصـل للمحتال مباشرة.

[22] بن خضرة حميدة، بضياف صالح، دور الذكاء الاصطناعي في الكشف والحد من الاحتيال على البطاقات الائتمانية البنكية على المستوى الدولي، مجلة الابداع، المجلد 14، العدد 2، 07\2024، ص 277.

	• **الاحتيال التقني دون الامتلاك المادي للبطاقة:** الاستيلاء الغير مشروع على بيانات البطاقة واستخدامها لتنفيذ معاملات عن بعد، بالإضـــافة الى تلاعب التجار عبر تكرار عمليات المســـح الالكتروني في معاملات شراء واحدة لتقييد مبالغ إضافية وهمية على حساب العميل.
الياته	• **انتحال الصـــفة (spoofing/phishing):** انشـــاء واجهات او مواقع مزيفة على الانترنت تحاكي الشركات والمؤسسات التجارية الكبرى لاستدراج المستخدمين وتسجيل بيانات بطاقاتهم عن طريق رسائل وروابط وهمية. • **التجســـس الرقمي (spyware/hacking):** اســـتخدام برمجيات خبيثة لاختراق أنظمة المعلوماتية للمؤسـسـات التجارية العاملة على الانترنت مما يتيح الوصـول المباشـر لقواعد بيانات العملاء وسـرقة ارقام حساباتهم. • **الكشط (skimming):** تركيب أجهزة قرصـنة دقيقة على منافذ الصـراف الالي لمسح بيانات الشـريط المغناطيسي للبطاقة ونسخها لاستخدامها في عمليات مشبوهة.[23]

المصدر :من اعداد الطالبة, بناءا على مراجعات سابقة

2. الاحتيال البنكي الالكتروني (Electronic Banking Fraud):

الجدول رقم 01-04: الاحتيال البنكي الالكتروني

تعريفه	وفقا لتقرير بازل للرقابة المصـرفية يقصـد بالاحتيال البنكي الالكتروني كافة الممارسـات الاحتيالية التي تنفذها أطراف خارجية باستخدام الوسائل الرقمية كالبريد الالكتروني، المواقع الوهمية، البرامج الخبيثة، بهدف الاستيلاء على اصول البنوك او بيانات عملاءها.[24]
صوره والياته	**أولا: اختراق البنية التحتية والبرمجيات:** تتمثل هده الصـــورة في الهجوم المباشـــر على الأنظمة المركزية للبنوك وقواعد بياناتها لإجراء تحويلات غير مشـــروعة، ويشـــمل دلك اختراق قنوات التحويل الدولية متل نظام (Swift) الذي سـجل في سـنوات ماضـية محاولات سـرقة بقيمة 336 مليون دولار الا ان الخسائر الفعلية انحصرت الى 07 مليون دولار أمريكي بفضل سرعة التدخل وتجميد العمليات المشبوهة وكدلك عمليات الاحتيال عبر نظام المقاصـة الالية (ACH) والسطو الرقمي العام كما يندرج تحت هدا العنوان الاختلاس التقني المعتمد على اســـتغلال الموظفين لصـلاحيتهم، بالإضـافة لتقنية احتيال السـلامي(salami) وهي تلاعب برمجي دقيق لسـرقة مبالغ

[23] عبد الكافي مريم، بوربابة صـــورية، جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية، مجلة القانون والعلوم السياسية، المجلد: 08، العدد01، 2022/02، ص 415.

[24]BASEL COMMITTEE ON BANKING SUPERVISION, DIGITAL FRAUD AND BANKING: SUPERVISORY AND FINANCIAL STABILITY IMPLICATIONS, OP.CIT, P3

	مجهرية تراكمية من الاف الحسابات على مدار فترات طويلة لضمان عدم اكتشافها من طرف أنظمة الرقابة. **ثانيا: تزوير الصفة الشخصية والاستيلاء على الأصول المالية:** تركز هده العمليات على تقمص شخصية الضحية للسيطرة على أصولها المالية، سواء عبر الاستيلاء الرقمي من خلال استنساخ شريحة الهاتف (Sim swapping) أو استغلال الهواتف المسروقة لتجاوز أنظمة المصادقة والوصول للتطبيقات البنكية. ولا يقتصر الامر على الحسابات القائمة بل يمتد الى الانتحال الائتماني عبر انشاء حسابات صورية او سحب قروض بأسماء الضحايا باستخدام وثائق مزورة تتم معالجتها رقميا. **ثالثا: تزوير أدوات الدفع والتوثيق الرقمي:** تعتمد هد الطريقة على ايهام الضحايا سوآء افراد او مؤسسات بتمام المعاملة المالية، من خلال تزييف مستندات الدفع ويشمل ذلك تزوير الشيكات الالكترونية باستخدام الماسحات الضوئية الحديثة، أو ارسال ايصالات مصرفية مزيفة ووهمية بما فيها التصيد عبر رموز (QR) و(NFC) لا تبات دفع غير حقيقي واتمام عمليات مشبوهة. **رابعا: الهندسة الإجتماعية والإحتيال الودي:** تقوم هده الصورة على التلاعب النفسي أو التضليل المتعمد، وتظهر بوضوح في احتيال الوعود والرسوم المسبقة متل اغراء الضحايا بجوائز يانصيب وهمية مقابل مبالغ مالية بسيطة. كما تشمل نوعا حديثا يعرف بالاحتيال الودي وفيه يقوم صاحب الحساب بممارسة التضليل المتعمد على البنك عبر ادعاء وقوع سرقة على حابه لاسترداد مبالغ مالية غير شرعية.

المصدر : من اعداد الطالبة بناءا على مراجعات سابقة [25] [26] [27] [28] [29] [30]

3. الاحتيال في التجارة الالكترونية (E-commerce Fraud):

جدول رقم 01-05: الاحتيال في التجارة الالكترونية

تعريفه	هو أحد أبرز الجرائم التي تعرقل سير المعاملات الالكترونية، ويتعرض لها الزبون عبر الحصول على معلومات مضلة عن المنتج او التعامل مع مواقع وهمية تستولي على الأموال

[25] MAMENE BESMA, IMAGES AND MANIFESTATIONS OF ELECTRONIC FRAUD ON PERSONS AND FUNDS THROUGH DIGITAL DATA, JOURNAL OF LAW, SOCIETY AND AUTHORITY, VOLUME 14, ISSUE 1, MARCH 2025, p 98

[26] MOZAN. "10 COMMON TYPES OF BANK ACCOUNT FRAUD +PROTECTION TIPS.NOVEMBER 23, 2023. ACCESSED11/ :2/2026.AVAIBLE AT: http://www.getfocal.ai/

[27] ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS (ASBA). DIGITAL FRAUD IN BANKING . TRENDS AND PRACTICES FOR MITIGATION. EXECUTIVE SUMMARY. PP 4-5

[28] LINA FERNANDES, FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES, OP.CIT, P2

[29] SHEWANGU DZOMIRA, ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, ZIMBABWE, RISK GOVERNANCE & CONTROL: FINANCIAL MARKETS & INSTITUTIONS, VOLUME 4, ISSUE 2, 2014, P17- 18

[30] ANTOINE BOUVERET, CYBER RISK FOR THE FINANCIAL SECTOR: A FRAMEWORK FOR QUANTITATIVE ASSESSMENT, OP.CIT, P13

	دون تسليم السلعة، أو عبر الدعاية المضللة وعرض مواد مغشوشة او منتهية الصلاحية. ويزداد خطر الاحتيال فيها عندما يكون المستهلك محدود الخبرة الالكترونية وحاجته للخدمات السريعة تدفعه للتعاقد مع مواقع غير موثوقة.[31]
صوره والياته [32]	• **المواقع الوهمية والعلامات التجارية الزائفة:** وذلك من خلال انشاء متاجر مزيفة تعرض تخفيضات وهمية لجذب الضحايا وسرقة أموالهم دون تسليم البضاعة او تقليد العلامات التجارية المشهورة من اجل تحقيق أرباح عن طريق الاحتيال والنصب • **استغلال بطاقة الائتمان المسروقة:** وتتم عبر شراء سلع فاخرة بطاقات مسروقة وشحنها عبر وسطاء الى دل بعيدة لتمويه مصدرها، تم إعادة بيعها بأسعار مرتفعة لتحويل قيمتها الى سيولة نقدية يتم تقاسمها بين افراد الشبكة. • **انتحال الهوية في المنصات التجارية:** يمكن تكييف مفهوم انتحال الهوية في مجال التجارة الإلكترونية من خلال استغلال المخترقون مهارتهم التقنية في انتحال صفة علامات تجارية موثوقة مستخدمين التمويه الرقمي لخداع المستهلكين يهدف هذا الاحتيال الى الاستيلاء على البيانات والأموال بالإضافة الى تدمير السمعة التجارية للمنافسين. • **التلاعب والتزوير المعلوماتي:** الدخول الغير مصرح به لقواعد بيانات المواقع التجارية لتعديل الأسعار، او جهات الشحن او إضافة طلبات ومعلومات مغلوطة لتحقيق مكاسب مالية غير مشروعة والاضرار بنزاهة التعاملات.

المصدر: من اعداد الطالبة بناءا على مراجعات سابقة

4. الاحتيال الالكتروني في السوق المالي (Electronic Fraud in Financial Markets):

جدول رقم 01-06: الاحتيال في السوق المالي والبورصات

تعريفه	**عرفته المنظمة الدولية لهيئات الأوراق المالية (IOSCO)**على أنه: احتيال مالي يُرتكب عبر الإنترنت، يستهدف بشكل أساسي مستثمري التجزئة في أسواق الأوراق المالية والمشتقات. يتم تنظيم هذا الاحتيال باستخدام افعال مخادعة أو محتوى مضلل عبر الإعلانات او الفيديوهات او المواقع المنتحلة او منشورات التواصل الاجتماعي، بما في ذلك المحتوى المضلل الذي ينشئه المستخدمون، لحثهم على شراء منتجات أو خدمات مالية.[33]
	• **الاحتيال القائم على المعلومات:** بث معلومات غير صحيحة او مضللة للتأثير على توقعات المستثمرين وسعر الأصل المالي.

[31] حياة هراكي، واقع جريمة الاحتيال الالكتروني في التجارة الالكترونية، مجلة التغير الاجتماعي، المجلد 8، العدد 02، 2023/02، ص 54.

[32] فرحاني رزيقة، بالرايس زينب، ضحايا النصب والاحتيال في ظل انتشار وتوسع التجارة الالكترونية دراسة ميدانية على عينة من الوسط الجامعي، جامعة الشيخ العربي التبسي، مرجع سبق ذكره، ص 51-52

[33] IOSCO, IOSCO STATEMENT ON ONLINE HARM,15 /12/ 2023. P1, FROM: https:// www.iosco.org /library/pubdocs /pdf / ioscopd 752.pdf

صوره	• **الاحتيال القائم على الفعل:** اتخاد قرارات مؤثرة متل الإعلان عن اندماج وهمي لتغيير قيمة السهم تم البيع بعد الارتفاع. • **الاحتيال القائم على التداول:** تنفيذ صفقات حقيقية او صورية تترك اترا مباشرا على الأسعار احجام التداول لتضليل المستثمرين. • **الاحتيال القائم على الطلب:** ارسال أوامر شراء او بيع بقصد عدم تنفيذها او تعديلها او الغاؤها كجزء من استراتيجية مخادعة. • الاحتيال القائم على التقديم: تقديم بيانات أو تقارير مالية خاطئة أو مضللة لحساب معيار مالي بشكل غير صحيح.[34]
الياته	• **استخدام لوحات المناقشة المالية (FDBs) والمنصات الرقمية لنشر معلومات كاذبة:** يستخدم المحتالون (FDBs) والمنصات الرقمية متل Yahoo! Financeو Ragin Bull بالإضافة الى وسائل التواصل الاجتماعي والبريد الالكتروني وسيلة لنشر معلومات كاذبة نظرا لامتلاكها مجموعة كبيرة من الجمهور عليها والتفاعل معها. • **التلاعب النفسي اللغوي:** استخدام عبارات تحفيزية لحت الاخرين على الشراء متل هدا هو الوقت المناسب فلنبدأ بضخ هذا السهم[35] ومن ضمن التقنيات المتعلقة بنشر الاشاعات نجد: – الضجيج والتفريغ (Hype and Dump): يعتمد على اخبار إيجابية كاذبة لرفع السعر تم البيع. – الافتراء والتفريغ (Slur and Dump): يعتمد على اخبار سلبية كاذبة لخفض السعر تم الشراء او تجنب الخسارة. • **استغلال تقة العملاء :** قيام السمسراء باستغلال جهل أو تقة العميل لدفعه لتنفيذ صفقات لا تخدم مصالحه بهدف الحصول على عمولة، سواء ربح العميل أو خسر. • **التأثير في سعر الاغلاق:** اصدار أوامر شراء قوية قبل الاغلاق مباشرة لرفع السعر وترك انطباع إيجابي مزيف بهدف رفع سعر الورقة المالية بشكل مصطنع. • **استغلال المعلومات الداخلية:** قيام شخص كمدير أو موظف مثلا يملك معلومات صحيحة وجوهرية ولكنها غير معلنة عن الشركة يتداول بها قبل الجمهور لتحقيق أرباح غير مشروعة او تجنب خسائر محققة. • البيع الصوري (wach sale): ويسمى كدلك بالبيع الوهمي وهي عبارة عن صفقات وهمية لا يترتب عنها انتقال الانتقال الفعلي لملكية الورقة المالية ولا ينجر عنها أي فائدة اقتصادية.

[34] جمال الدين عباس، اليات الحد من الانحرافات في الأسواق المالية دراسة تحليلية تقييمية لعدد من الأسواق المختارة، أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في علوم التسيير تخصص إدارة مالية، جامعة البشير الإبراهيمي برج بوعريريج، 2024، ص 123.122

[35] PEI SHYUAN LEE, MAJDI OWDA, KEELEY CROCKETT, THE DETECTION OF FRAUD ACTIVITIES ON THE STOCK MARKET THROUGH FORWARD ANALYSIS METHODOLOGY OF FINANCIAL DISCUSSION BOARDS, THE MANCHESTER METROPOLITAN UNIVERSITY, P1-2

	• اتفاقيات التلاعب (pools): اتفاق مجموعة من المحتالين فيما بينهم لتنفيذ عمليات بيع وشـــراء على ورقة مالية معينة بهدف التأثير على سعرها وفي هدا الصدد نجد نوعين من الاتفاقيات: • اتفاقيات التداول (trading pools): قيام مجموعة من المحتالين بشـــراء وبيع ســـهم معين فيما بينهم لتضـــخيم حجم التداول ،مما يخلق انطباعا زائفا بنشـاط السـهم و يجدب مسـتثمرين جدد تم يبيعون اسهم بعد ارتفاع السعر. – اتفاقيات الخيار (pools option): شراء مجموعة من المحتالين لخيارات الشراء على سهم معين تم التلاعب بسعره الفعلي ليرتفع بشكل حاد، مما يمكنهم من تنفيد الخيارات وتحقيق أرباح سريعة. • **الشـراء بنية الاحتكار (Corner the market)**: شـراء مجموعة من المحتالين لكمية ضـخمة من سهم معين مما يمنحهم السيطرة الشبه كاملة على العرض والسعر ويجبر البائعين على الشراء منهم السعر الدي يحددونه. • **ربط التعليقات على المنصـــات وحركة الســـوق:** اســـتغلال العلاقة بين التعليقات الإيجابية في المنتديات وزيادة حجم التداول والتقلبات السعرية لتحقيق عوائد غير مشروعة[36]

المصدر : من اعداد الطالبة بالاعتماد على ,مراجعات سابقة

5- الإحتيال الالكتروني في التامين (Electronic Insurance Fraud):

جدول رقم01-07 : الاحتيال الالكتروني في التامين

تعريفه	سـعي فرد أو مجموعة من الافراد الى الحصـول على مقابل مالي عن طريق الفضـاء الرقمي سـواء كان في شـــكل أموال أو ســـلع أو خدمات من خلال وثيقة تامين عن طريق الخداع وبطريقة غير مشـروعة ويمكن ان يحدث الاحتيال في أي وقت خلال عمر الوثيقة بدءا من مرحلة الاكتتاب وصـولا الى مرحلة المطالبات
صوره واشكاله	حيت ان أي تلاعب يتم عبر الوسائل الرقمية او أي أسلوب من أساليب الاحتيال الالكتروني من اجل تنفيذ هده الصور من الاحتيال يعد جزءا من منظومة الاحتيال الالكتروني في قطاع التامين. **1. الاحتيال في مرحلة الاكتتاب:** ويحدث باي شكل من الاشكال التالية: – **الواجهة:** ويحدث غالبا في تامين الســـيارات حيت يؤمن الوالدان على مركبة باســـمهما نيابة عن ابنهما للحصول على سعر تفضيلي. – **التضـــليل:** عندما يتعمد الفرد اغفال حقائق تؤثر على تقييم المخاطر او يقدم معلومات كاذبة للحصول على تامين بسعر اقل – **التامين الزائف:** السعي للحصول على تامين لخطر غير موجود أصلا لتقديم مطالبة لاحقا.

[36] جمال الدين عباس، اليات الحد من الانحرافات في الأسواق المالية دراسة تحليلية تقييمية لعدد من الأسواق المختارة، مرجع سابق، ص 124- 125.

	– **تعدد الوثائق:** استخراج عدة وثائق لنفس الخطر لتقديم مطالبات متعددة عن خسارة واحدة **2. الاحتيال في مرحلة المطالبات:** نجد فيها: • **المبالغة:** ولها ثلاثة اشكال: – **تضخيم القيمة:** المطالبة بمبلغ أكبر من قيمة العنصر. – **إضافة عناصر إضافية:** إضافة عناصر لم تكن ضمن الخسارة الفعلية. – **طراز محسن:** المطالبة بتعويض عن طراز احدث وأغلى تمنا. • **تعدد المطالبات:** المطالبة بالخسارة نفسها من عند اكتر من شركة تامين بشكل غير قانوني. • **المطالبة الزائفة:** اختلاق مطالبة وهمية بالكامل او التخطيط المسبق لحادث مفتعل

المصدر : من اعداد الطالبة بالاعتماد على مراجعة سابقة [37]

6- الاحتيال في العملات المشفرة (Cryptocurrency Fraud)

الجدول رقم01-08: الاحتيال في العملات المشفرة

تعريفه	هو نشاط غير قانوني يستغل التكنولوجيا الرقمية لأغراض احتيالية يتضمن ذلك إطلاق مشاريع استثمارية وهمية وجمع أموال الضحايا عبر عروض أولية للعملات المزيفة (ICOs) كما يعتمد على تقنيات متطورة متل اقتحام المحافظ الرقمية وسرقتها والتلاعب الاصطناعي بأسعار العملات المشفرة في السوق. [38]
صوره والياته	لقد تعددت صور الاحتيال العملات المشفرة ومن أبرزها نحصرها في الموالي: • **مخططات بونزي وعروض العملات الوهمية (ICOs):** حيث يتم استدراج المستثمرين بوعود أرباح مرتفعة ي مشاريع غير حقيقية وتمول الأرباح من أموال مستثمرين جدد الى ان ينهار النظام.[39] • **التعدين الخفي (Cryptojacking):** يتم من خلاله استغلال أجهزة الضحايا سرا لتعدين العملات المشفرة دون علمهم مما يؤدي بالنهاية الى منفعة مالية غير مشروعة على حساب الضحية [40]

[37] KAREN ANN GILL, INSURANCE FRAUD: CAUSES CHARACTERISTICS AND PREVENTION THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY AT THE UNIVERSITY OF LEICESTER, ,9/2001, P 27-30

[38] مناصرة يوسف، الاحتيال المالي السيبراني باستخدام الأصول المشفرة، مجلة صوت القانون، المجلد 10، العدد1، 2024/1/24، ص 354- 355

[39] تامر السيد احمد السيد قناوي، **اتر** استخدام العملات المشفرة على جريمة الاحتيال الالكتروني، المجلة القانونية الاقتصادية، المجلد 37، العدد53، ديسمبر2025، ص 61-62

[40] FARAH AICHA, FINANCIAL FRAUD IN THE ERA OF DIGITAL TRANSFORMATION, JOURNAL OF LEGAL AND POLICITICAL SCIENCE, VOL 62, N2, 07 /2025, P179

	• **الانفاق المزدوج (Double spending):** يحدث عندما يتم استخدام نفس الرصيد فالشخص قد يستخدم عملة مشفرة معينة لشراء سلعة، تم يستخدم العملة نفسها لشراء سلعة أخرى، مع أن العملة لم تعد ملكا له بسبب الشراء الأول مستغلا ثغرات بعض الأنظمة والتأخر في التحقق [41] • **التلاعب بأسعار العملات المشفرة:** يتم من خلال نشر اخبار او معلومات مضللة او استخدام منصات وهمية للتأثير على العرض والطلب، بهدف رفع او خفض الأسعار بشكل اصطناعي وتحقيق أرباح غير مشروعة.[42] • **احتيال البلوكشين وهجمات الاجماع:** [43] رغم امان البلوكشين، الا انها قد تتعرض لهجمات متل هجوم 51% وهجوم غولد فينغر وهجوم ريشة الشوكة (Feather-Forking) وتستغل هذه الهجمات لتنفيذ أنشطة احتيالية وحصول غير مشروع للأصول المالية.[44] • **تبيض الاموال بالعملات المشفرة:** يتم استخدام العملات المشفرة لإخفاء مصدر الأموال الغير قانونية وتحويلها بين عدة محافظ أو منصات غير خاضعة للرقابة. • **البرمجيات الخبيثة:** تشمل برامج ضارة تستهدف مستخدمي العملات المشفرة متل برمجيات تسجيل المفاتيح وسرقة البيانات، بهدف الوصول الى المحافظ الرقمية والاستيلاء على الأصول.[45] **المنصات وتطبيقات التداول المزيفة:** يتم انشاء مواقع أو محافظ تبدو شرعية لكنها صممت لسرقة المفاتيح الخاصة أو تحويل الأموال مباشرة للمحتالين.[46] **الهجمات على منصات التداول والمحافظ الرقمية:** تستهدف البورصات الرقمية والمحافظ الالكترونية عبر الاختراق وسرقة الأصول المالية مع صعوبة استرجاع الأموال بسبب غياب جهة مركزية.[47]

المصدر : من اعداد الطالبة بالاعتماد على مراجعات سابقة

7- الاحتيال الالكتروني التمويل الجماعي (Online Crowdfunding Fraud)

جدول رقم 01- 09: الاحتيال في التمويل الجماعي من اعداد الطالبة بناءا على مراجعات سابقة

---

[41] مرزوق آمال، العملات المشفرة: فرص وتحديات استخدامها، مجلة البشائر الاقتصادية، المجلد 6، العدد 2، ديسمبر 2020 ص119

[42] الموقع الالكتروني لشركة (kaspersky) للأمن السيبراني وحماية البيانات، الاحتيال في العملات المشفرة، على الرابط:
– https://support.kaspersky.com/kisa/android_11.98/ar-ae/248822.htm
تاريخ الاطلاع عليه في: 2026/2/1 على الساعة 15:00

[43] قاسمي زهيرة، موقف القانون الجزائري من التعامل بالعملات الرقمية بين الضرورة والمخاطر، مجلة افاق علمية، المجلد 16، العدد 2، 2024/10، ص 522

[44] STOGANOVIC BRANKA, ET AL,"FOLLOW THE TRAIL: MACHINE LEARNING FOR FRAUD DETECTION IN FINTECH APPLICATIONS SENSORS ", OP.CIT , PP5 -7

[45] مناصرة يوسف، الاحتيال المالي السيبراني باستخدام الأصول المشفرة، مرجع سابق، ص 355.

[46] تامر السيد احمد السيد قناوي، اتر استخدام العملات المشفرة على جريمة الاحتيال الإلكتروني، مرجع سابق، ص 66-68.

[47] عون الله سعاد، عامري رضوان، مخاطر وتداعيات تداول العملات المشفرة على استقرار القطاع المالي خلال الفترة 2017-2021، مجلة اقتصاديات شمال افريقيا، المجلد 19، العدد 31, 2023/3، ص217

تعريفه	هو التلاعب المتعمد بمنصات التمويل الجماعي الخيرية من قبل وكلاء يقومون بإنشاء مشاريع وهمية متعددة لخداع المتبرعين والحصول على الأموال بطريقة غير مشروعة.[48]
اشكاله وصوره	لقد تعددت اشكال الاحتيال في التمويل الجماعي ومن بينها ما يلي: • **الاحتيال في المنصـــات الالكترونية لتمويل الجماعي القائم على التبرع:** ويتمثل في تحريف الغرض منه حيت تجمع الأموال لقضايا إنسانية او اجتماعية تم توجه لتغطية مصاريف شخصية او أغراض مغايرة. • **الاحتيال في المنصـــات الالكترونية لتمويل الجماعي القائم على المكافأة:** يتخذ صـــورتين، اما اهمالا ناتجا عن ســـوء الإدارة وعدم القدرة على الوفاء بالوعود، او احتيالا صـــريحا عندما يطلق صـاحب المشـروع حملة وهمية غير قابلة للتنفيذ بقصـد الاسـتيلاء على الأموال دون نية تسـليم مكافئات او عدم وجود أي نية للوفاء بالوعود التي قدمها. • الاحتيال في المنصات الالكترونية الجماعي لتمويل الجماعي القائم على الأسهم: يظهر من خلال إساءة استخدام الأصـول كاستغلال أموال المستثمرين في سداد رواتب ضـخمة للمديرين بدلا من تطوير المشـروع مسـتغلين ضـعف الرقابة من قبل المسـتثمرين فقد لا يكون للأفراد المسـتثمرين بأموالهم القدرة والحافز على ممارسة الرقابة على الأنشطة التي تم تمويلها. • **الاحتيال في المنصات الالكترونية الجماعي لتمويل الجماعي القائم على الإقراض:** حيت يتم بنية احتيالية متمثلة في جمع الأموال من المقرضـين ومن تم اغلاق المنصـة فعلى سـبيل المتال يمكن ان يحدث الاحتيال عن طريق المنصـــات التي تشـــغل مخططات بونزي حيث حيت لا يتم توليد الدخل انطلاقا من نشـاط اقتصـادي انما يتم دفع فوائد المسـتثمرين الأوائل باسـتخدام اسـتثمارات المستثمرين اللاحقين.[49]
الياته:	يعتمد نجاح الاحتيال بالتمويل الجماعي على أليات احتيالية محورية من بينها: – اطالة فترة التمويل: يهدف المحتالون إلى إطالة فترة التمويل لزيادة كمية رأس المال المجموع من الضحايا – تعدد فئات التعهد: إنشاء فئات تعهد متعددة بحدود استثمار منخفضة لضمان جذب عدد كبير من المساهمين

[48]MARCOS R. MACHADO, IOANA FLORINA COITA,ET AL , 3D SYSTEMATIC LITERATURE REVIEW : AI,NETWORKS AND HUMANS TO DETECT CROWDFUNDING FRAUD ,10/2024,p10

[49] MARCOS R. MACHADO, IOANA FLORINA COITA, ET AL, 3D SYSTEMATIC LITERATURE REVIEW : AI,NETWORKS AND HUMANS TO DETECT CROWDFUNDING FRAUD,IBID ,P 4-5

	– تفاصيل المشروع الغامضة: استخدام أوصاف حملة غامضة أو مضللة تجعل من الصعب على المساهمين تقييم جدوى وشرعية المشروع – الاستهداف الانتقائي للفئات الأقل تعليما: يستهدف المحتالون الجماهير الأقل تعليما ووعيا بالثقافة المالية والرقمية، مستغلين نقص وعيهم بمؤشرات الاحتيال الالكتروني [50]

المصدر : من اعداد الطالبة بالاعتماد على مراجعات سابقة

الفرع الثاني: أساليب الاحتيال المالي الالكتروني:

يشهد الاحتيال المالي الالكتروني تطورا متسارعا من حيت الأساليب والتقنيات المستخدمة، فلم يعد يقتصر على الطرق التقليدية بل أصبح يجمع بين التلاعب البشري والأدوات التقنية المتقدمة، وتتنوع هده الأساليب بين العامل النفسي للهجوم كالهندسة الاجتماعية والتصعيد الاحتيالي واستغلال الثغرات التقنية وصولا الى توظيف الذكاء الاصطناعي في الاحتيال المالي الالكتروني مما يزيد تعقيد اكتشافها وهوما نبرزه بالتفصيل في الاتي:

1- الهندسة الاجتماعية (Social Engineering):

الاحتيال عبر الهندسة الاجتماعية هو مصطلح عام يعني الحيل التي يلجأ إليها المجرمون لاستغلال ثقة الشخص والتلاعب النفسي بالبشر بغية الحصول على المال بشكل مباشر أو على معلومات سرية تمكنهم من ارتكاب جريمة لاحقة، وتشكل وسائل التواصل الاجتماعي القناة المفضلة لديهم ولكن يتواصلون أحيانا مع الضحايا المحتملين عبر الهاتف أو الايميل أو رسائل (SMS) وتستهدف الهندسة الاجتماعية اما جمهورا كبير وعشواءي الايقاع اكبر عدد من الضحايا أو قد تستهدف اشخاص محددين فهي تعتمد على علم النفس البشري بدلا من الاعتماد على الثغرات التكنولوجية ودلك باستخدام اساليب مختلفة للإيقاع بالضحية من بينها ما يلي:[51]

- **التذرع (Pretexting):** يقوم المهاجم بإنشاء سيناريو مفبرك للحصول على معلومات أو الوصول إلى الهدف.
- **الإغراء (Baiting):** إغراء الهدف بعرض جذاب (مثل برامج مجانية) لاختراق امنه.
- **التعقب (Tailgating):** خداع موظفي الأمن او الموظفين للحصول على وصول مادي إلى منطقة محظورة.

[50] MARCOS R. MACHADO, IOANA FLORINA COITA, ET AL, CROWDFUNDING FRAUD DETECTION: A SYSTEMATIC REVIEW HIGHLIGHTS AI AND BLOCKCHAIN USING TOPIC MODELING, 9/2024, P9

[51] المنظمة الدولية للشرطة الجنائية الانتربول، الاحتيال عبر الهندسة الاجتماعية، الموقع على الأنترنت:
https://www.interpol.int / تم الاطلاع عليه في 2026/1/20، على الساعة 09:17

- **الاختبارات الاستبيانات (Quizzing):** خداع الضحية للكشف عن معلوماته تحت غطاء إجراء مسح أو استبيان.
- **برمجيات التخويف (Scareware):** خداع الهدف لشراء مضاد فيروسات مزيف بدعوى ان جهازه مصاب.

1-1- التصيد الاحتيالي (Phishing): وهو الشكل الأكثر شهرة وانتشارا ضمن أساليب الهندسة الاجتماعية لذلك سنقوم بشرحه بشكل تفصيلي اكتر حيت يشكل التصيد الاحتيالي، أسلوبا موثقا جيدا للجرائم الإلكترونية، مصمما للحصول على بيانات سرية بطريقة غير مشروعة عن طريق انتحال صفة كيان شرعي. تستغل هذه الممارسة الغير مشروعة للتلاعب بالضحايا لدفعهم على الكشف عن بيانات اعتماد حساسة بدون قصد ومن بين انواعه:

- **التصيد بالبريد الإلكتروني (Email phishing):** رسائل بريد إلكتروني تظهر وكأنها من مصادر موثوقة بنوك، جهات حكومية لسرقة المعلومات.
- **التصيد الموجه (Spear phishing):** تخصيص رسالة البريد الإلكتروني المخادعة لشخص او منظمة محددة.
- **التصيد عبر الرسائل النصية (Smishing):** استخدام الرسائل النصية القصيرة (SMS) لخداع الضحايا للنقر على روابط خبيثة.
- **صيد الحيتان (Whaling):** شكل متخصص من التصيد الموجه يستهدف الشخصيات رفيعة المستوى مثل المديرين التنفيذيين (CEO) لإجبارهم على تحويل مبالغ مالية ضخمة.
- **التصيد الصوتي (Vishing):** استخدام المكالمات الهاتفية المخادعة لخداع الهدف للإفشاء عن معلومات الهاتفية المخادعة لخداع الافراد للإفشاء عن معلومات سرية.
- **التصيد عبر وسائل التواصل الاجتماعي(Social-Media):** استخدام منصات مثل فيسبوك أو إنستغرام لخداع الضحايا.[52]

كما نلخص في الجدول الموالي مراحل التصيد الاحتيالي وتقنياته:

جدول رقم 01-10: مراحل وتقنيات التصيد الاحتيالي

مراحل التصيد الاحتيالي	• **المرحلة الأولى الهجوم الأولي:** تبدأ بالخداع عبر رسائل (بريد الكتروني او نصية) تنتحل صفة جهات رسمية او مالية موثوقة، يصمم هذا الاتصال بدقة لاستغلال الدوافع النفسية للضحية متل

[52] MARC SCHMITT, IVAN FLECHAIS, DIGITAL DECEPTION: GENERATIVE ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING AND PHISHING, JOURNAL ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING AND PHISHING, JOURNAL ARTIFICIAL INTELLIGENCE REVIEW, VOL.57, NO 324 ,12. OCTOBER2024, PP 5-6

	الخوف او الالحاح، لدفعها نحو كشـــف بياناتها. كما يعتمد المحتالون هذا على تزييف العلامات التجارية والشعارات الرسمية لضمان استجابة الضحية دون ارتياب • **المرحلة الثانية إعادة التوجيه:** يتم توجيه الضـحية إلى منصـة رقمية مزيفة تحاكي واجهات مستخدم المواقع الرسمية عبر روابط مضمنة في الرسالة الاحتيالية. • **المرحلة الثالثة جمع البيانات:** تتضمن المرحلة الأخيرة استخراج بيانات الضحية بشكل غير مصرح به بمجرد إرسـالها يتم نقل بيانات الاعتماد المخترقة على الفور إلى شـبكات المجرمين الإلكترونيين، حيث يمكن استخدامها في عمليات احتيال مالي مباشرة، بما في ذلك الاحتيال على بطاقات الائتمان، وحتى الاحتيال القائم على العملات المشفرة.
تقنياته	**انتحال (DNS) وعرض شـــريط عنوان مزيف** تجمع بين انتحال نظام أســـماء النطاقات (DNS) وتزييف شريط العنوان حيت يتم تغيير اعدادات النطاقات لتوجيه المستخدم لمواقع وهمية مع التلاعب بواجهة المتصـفح لإظهار روابط (URLs) تبدو شـرعية وتوجيههم لمواقع احتيالية لخداع الضـحايا حيث يجمع مجرمو الإنترنت بيانات الاعتماد الشخصية. – **اختراق واجهات المســـتخدم:** تعتمد على دمج نصـــوص برمجية خبيثة داخل المواقع الموثوقة او إظهار نوافذ منبثقة فجائية والهدف هو اســـتحداث واجهات دخول مزيفة تطلب بيانات مزيفة تحت دريعة تحديثات البرامج او الفحوصات الأمنية. – **هجمات الوسـيط (MITM):** تحدث هذه الهجمات عندما يعترض المهاجمون البيانات المنقولة بين طرفين ويتلاعبون بها دون علمهما، وغالبا في الوقت الفعلي. – **تقنيات التمويه:** باســـتخدام ترميز معقد لإخفاء عناوين (URL) الضـــارة، يجعل المهاجمون هذه العناوين تبدو غير ضارة للمستخدمين غير المشتبه بهم وحتى لأنظمة الأمان المتطورة. – **التصيد الاحتيالي بالبرمجيات الخبيثة:** من خلال تثبيت برامج التجسس أو برامج تسجيل ضـغطات المفاتيح سزا، يحصل المهاجمون على وصول مطول إلى المعلومات الشخصية والمالية للضحية. – **تضـــليل محركات البحث:** يتلاعب المحتالون بخوارزميات محركات البحث لتعزيز ترتيب مواقع التصيد الاحتيالي، مما يضل المستخدمين ويجعلهم يعتقدون انها مواقع شرعية.

المصدر : من اعداد الطالبة بالاعتماد على مراجعة سابقة [53]

2-1- الهندسة الإجتماعية الالية (Automated Social Engineering):

حيت من خلال الذكاء الاصطناعي يمكن فحص البيانات العامة والمسروقة التي تم جمعها لصياغة رسائل لا يمكن تمييزها عن تلك التي يكتبها المعارف المقربون ومن بين أبرز اشكالها:

[53] FARAH AICHA, FINANCIAL FRAUD IN THE ERA OF DIGITAL TRANSFORMATION, OP.CIT, P 176-177

- **التصيد الاحتيال السياقي:** رسائل مقنعة جدا وتبدو طبيعية ومنطقية للضحية في لحظة معينة لأنها تعتمد على استغلال أحداث أخيرة متل موسم ضرائب أو تحديثات لنظام الشركة أو جائحة عالمية أو تشير الى جهات اتصال مشتركة لجعل الطلب يبدو مشروعاً وطبيعياً أو منطقياً في لحظة معينة.
- **التصيد الاحتيالي المدعوم بالذكاء الاصطناعي:** يعتمد على نماذج لغوية متطورة وحصاد البيانات والتعلم التكيفي لصياغة اتصالات مخادعة مخصصة للغاية ومقنعة.[54]

حيت ان الهندسة الاجتماعية الالية تستخدم الذكاء الاصطناعي التوليدي من اجل الخداع الرقمي الغير مشروع وتعتمد على تلاته ركائز أساسية وهي:

جدول رقم 01-11: ركائز التصيد الاحتيالي المدعوم بالذكاء الاصطناعي

الركيزة الأولى: انشاء محتوى واقعي	يعتمد الاحتيال الحديث على قدرات الذكاء الاصطناعي التوليدي مثل (NLP)، و (Computer Vision)، و(Processing Audio and Speech)، (Multimodal Génération) لإنتاج محتوى تضليلي فائق الواقعية. حيث يتم استغلال هذه التقنيات لإنشاء هويات مزيفة، واستنساخ المواقع، لتجاوز الأنظمة الأمنية وانتحال الشخصيات. كما تُستخدم نماذج (LLMs) لأتمته هجمات التصيد وتخصيصها وتطويرها ديناميكياً مع الضحايا في الوقت الفعلي.
الركيزة الثانية الاستهداف المتقدم والتخصيص	وذلك من خلال ما يلي: 1. **الاستطلاع(Reconnaissance):** بفضل إتقانه للغة وقدراته التحليلية للبيانات، يمكن للذكاء الاصطناعي التوليدي فحص البصمات الرقمية للأفراد المستهدفة وهذا يوفر رؤى حول اهتمامات الهدف المحددة، أو انتماءاته، أو سلوكياته. 2. **التذرع (Pretexting):** يمكن استخدام هذه المعلومات الاستخباراتية التي تم جمعها لاحقا لتطوير استراتيجية الهجوم المشار إليها باسم التذرع وهي مرحلة واسعة تشمل إنشاء قصة، أو سيناريو، أو هوية. 3. **التصيد المدرك للسياق (Context-awarephishing):** هذا يمكن من التصيد المدرك للسياق، حيث يصيغ الذكاء الاصطناعي محتوى خبيثا يتوافق مع أنماط اتصالات الفرد المستهدف، مما يجعل القصة أو السيناريو قابلا للتصديق للغاية. 4. **اختبار تورينج:** أظهرت البوتات الذكية، مثل نماذج اللغات الكبيرة مكسورة الحماية (مثل ChatGPT) و(Gemini)، قدرات فائقة في اجتياز اختبار تورينج، والظهور كبشر حقيقيين بشكل عام.

[54] ABAS KADAR, AI-POWERED PHISHING DEEPFAKE AND THE NEW DATA GOVERNANCE IMPERATIVE,21/01/2026,pp1-2,RETRIED AT:18/02/2026 FROM [https://www.researchgate.net/publication/399984480_aipowered_phishing_ deepfakes_ and_the_new_data_governance_imperative]

الركيزة الثالثة: بنية تحتية مؤتمتة للهجوم	وذلك من خلال: 1. **حلقات التغذية الراجعة:** من خلال إدخال حلقات تغذية راجعة للاستطلاع في مرحلتي التذرع والتنفيذ، يصبح الذكاء الاصطناعي نظاما ديناميكيا قادرا على تطوير أساليبه بناءا على النتائج الواقعية فمثلا إذا لاحظ بوت الدردشة ترددا أو شكا في استجابات الضحية، يمكنه تغيير أسلوبه، نبرته، أو المعلومات التي يقدمها. 2. **بوت المستقل:** التهديد النهائي هو بوت هندسة اجتماعية ذكي ومستقل تماما. 3. **شبكات البوت (Botnets):** عبر شبكات البوت المدعومة بالذكاء الاصطناعي، يمكن للمهاجمين صياغة ونشر رسائل تصيد مخصصة لجمهور هائل بسرعته وتكييف المحتوى في الوقت الفعلي بناة على تفاعلات المستخدم. 4. **التهرب والتمويه:** يمكن للذكاء الاصطناعي استخدام أنماط هجوم متعددة الأشكال (مثل رسائل البريد الإلكتروني التي تتغير باستمرار، ومواقع الويب الخبيثة المتغيرة ديناميكيا، إلخ) تقنيات التهرب والتمويه هذه التي ينشئها الذكاء الاصطناعي قد تجعل من الصعب جدا تصفية المحتوى الخبيث. 5. **السرعة والمقياس:** باستخدام الأتمتة، يمكن للمهاجمين تنفيذ حملات هندسة اجتماعية وتصيد بمقياس وسرعة يستحيل على الفاعلين البشر تحقيقها

من اعداد الطالبة بالاعتماد على مراجعات سابقة.[55]

2.التزييف العميق (Deepfake):

جدول رقم 01- 12: التزييف العميق واليته من اعداد الطالبة بالاعتماد على مراجعات سابقة.

تعريفه	هي مزيج بين كلمتي التعلم العميق الدي هو فرع من فروع التعلم الالي والتزييف وتعرف على انها عملية استخدام الذكاء الاصطناعي لإنشاء وسائط تركيبية يتم فيها استبدال صورة شخص ما بالصورة او الفيديو الأصلي التي تنتحل شخصية اشخاص حقيقيين بشكل مقنع وبواقعية مذهلة تبدو انها اصلية للغاية.
اشكاله	– **تزييف الصوت والسلوك:** "يمكنه توليف الكلام والفيديو وتكرار الأصوات والسلوكيات بدقة غريبة. – **تزييف تعبيرات الوجه والفيديو:** "يمكن للتزييف العميق تكرار أنماط الكلام وتعبيرات الوجه والسلوكيات بدقة مثيرة للقلق.

[55] MARC SCHMITT,IVAN FLECHAIS,DIGITAL DECEPTION:GENERATIVE ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING AND PHISHING,OP.CIT,P 11-12

	– **انتحال الشخصية التنفيذية:** قد يتم محاكاة المسؤولين التنفيذين لتفويض معاملات احتيالية او تضليل المساهمين أو التلاعب بالسوق. – **تزييف الشخصيات العامة:** "تصوير القادة وهمم يدلون بتصريحات أو فبركة أحداث للإثارة.
مراحله	– **الاستطلاع الآلي:** تقوم انظمة الذكاء الاصطناعي بتجميع البيانات من وسائل التواصل الاجتماعي، والسجلات العامة، وإفصاحات الشركات، وخرق البيانات السابقة – **المحاكاة السلوكية:** تحليل الأنماط اللغوية من المنشورات العامة لمحاكاة عادات الكتابة الشخصية. – **الاستغلال النفسي:** تعتمد هذه الهجمات على التحيزات المعرفية البشرية، حيث يميل الأفراد إلى الثقة في الأسماء المألوفة والأصوات المعترف بها. – **التكيف في الوقت الفعلي:** "عندما تفشل رسالة أولية في الخداع، يمكن لنظام أبناء متابعات تضبط النبرة والإلحاح بناء على الردود.
تقنياته	• **شبكات الخصومة التوليدية(GANs):** تعتمد على نظام تنافسي بين شبكتين عصبيتين: **المولد** الذي يصنع بيانات مزيفة (صور أو فيديو)، و**المميز** الذي يحاول كشف زيفها. من خلال هذا التفاعل المستمر، يتعلم المولد تحسين مخرجاته بناءً على ملاحظات المميز، مما يؤدي في النهاية إلى إنتاج محتوى اصطناعي فائق الواقعية يصعب تمييزه عن الحقيقة، وهو ما يسهل إساءة استخدامه في عمليات التزييف. • **المشفرات التلقائية:** هي شبكات عصبية تأخذ بيانات الادخال الاصلية وتضغطها الى رمز أصغر تعيد تعيين الرمز الى بيانات الادخال الاصلية تستخدم لتشفير ملامح الوجه وتعبيراته، ثم تحويلها إلى فيديوهات مزيفة. • **الشبكات العصبية المتكررة (RNNs) متل شبكات الذاكرة طويلة المدى (LSTM):** لإنتاج تسلسلات متابعة ذات صلة صوتية ودلالية مما يجعل استخدام الصوت المزيف في حد ذاته يبدو واقعيا. • **الشبكات، العصبية الالتفافية (CNNs):** تستخدم لاستخراج ملامح الصور والتعرف عليها وهي مناسبة جدا لتشكيل تعبيرات الوجه في فيديوهات التزييف العميق.

المصدر :من اعداد الطالبة بالاعتماد على مراجعات سابقة [56] [57]

[56] POOGA KAUSHIK, ET AL," FINANCIAL FRAUD AND MANIPULATION: THE MALICIOUS USE OF DEEPFAKE IN BUSINESS, "DEEPFAKES AND THEIR IMPACT ON BUSINESS, EDITED BY GAURAV GUPTA ET AL, IGA GLOBAL, 2025, P174

[57] POOGA KAUSHIK, ET AL," FINANCIAL FRAUD AND MANIPULATION: THE MALICIOUS USE OF DEEPFAKE IN BUSINESS, "DEEPFAKES AND THEIR IMPACT ON BUSINESS,IBID ,P178-179

3.الاحتيال عبر الإنترنت الأشياء (Electronic Fraud via the Internet of Things):

الجدول رقم01-13: الاحتيال عبر انترنت الأشياء

تعريف الاحتيال عبر انترنت الاشياء	استغلال الثغرات في الأجهزة المترابطة رقميا للوصول للبيانات المالية الحساسة وسرقتها أو التلاعب بها سواء اعبر خداع العنصر البشري سلوكيا (الهندسة الاجتماعية) أو عبر الكود الخبيث تقنيا
تقنياته	**البرمجيات الخبيثة:** هي ديدان دكية تستخدم انترنت الأشياء كبيئة خصبة للهجوم والانتشار تمسح الشبكة وتصيب الأجهزة المجاورة ولان الأجهزة مترابطة مع بعضها البعض في بيئة (LoT) فدودة دكية واحدة يمكن ان تصـــيب العديد من الأجهزة في وقت قياســـي دون الاضطرار لاختراق كل جهاز على حدى، وتتكون من خمس وحدات: – **الوحدة الرئيســـية (الحمولة):** وهي الجزء الخبيث من الدودة الذي يهدف إلى تدمير والتلاعب بالبيانات. – **وحدة التحكم والسيطرة:** وهي جزء من الدودة يستخدمه المتسللون للتواصل مع الأجهزة المصابة وإدارة الأنشطة والعمليات. – **وحدة مكافحة الكشـــف:** وهي الجزء الذي يخفي ويموه الهوية الخبيثة للحمولة الخبيثة لتجنب اكتشافها بواسطة برامج مكافحة الفيروسات وجدران الحماية. – **وحدة الانتشـــار:** وهو الجزء الذي يعمل على مســح الأجهزة المجاورة في الشـبكة التي يوجد بها الجهاز المصاب لنشر العدوى وإصابة الشبكة. – **وحدة التحديث:** وهو جزء من التعليمات البرمجية المســـؤول عن تغيير الدودة إذا تم العثور على أي توقيع وتم الإبلاغ عنه. وتتجلى خطورة متل هده الأدوات في قدرتها على شن هجمات ضد البنية هجمات ضد البنية التحتية المالية العالمية، مثل هجوم (Mirai) الذي اسـتهدف العمود الفقري للأنترنت، وكان بإمكانه استهداف مؤسسات مالية كبرى

المصدر :من اعداد الطالبة بالاعتماد على مراجعة سابقة [58]

[58] MUSTAPHA M. HOBALLAH, ZAHRAA L. HAMMOUDA ,HABIB M , AWADA ,ELECTRONIC FINANCIAL FRAUD:ABSTRACT ,DEFINATIONS,VULNERABILITIES, ISSUSES AND CAUSES,PROCEEDINGS OF POM BEIRUT 2019 ,06/2019, p11 -13, doi : http://dx.doi.org/10.14236/ewic/pom19.2

4.الاحتيال عبر الهوية الاصطناعية (Synthetic Identity:): هو استخدام بيانات حقيقية مسروقة مع بيانات أخرى مزيفة لإنشاء هوية جديدة تبدو حقيقية و قانونية فمثلا في البنوك تستخدم لإنشاء سجلات مالية وهمية متل طلبات القروض وفتح الحسابات حيت ان الاحتيال بالهوية الاصطناعية يهدد بشكل مباشر دقة البيانات، مما قد يؤدي إلى خسائر مالية، ومسؤوليات قانونية، وأضرار بالسمعة حيت إن اعتماد القطاع المصرفي على سجلات العملاء الدقيقة لتقييم الائتمان، والتحقق من الهوية، وكشف الاحتيال يجعله عرضة بشكل كبير لهذا الخطر حيت انه في واقعة احتيالية حقيقية :استخدم المحتالون الماليون في هونغ كونغ ثماني بطاقات هوية مسروقة لتقديم 90طلب قرض و54تسجيلاً لحساب مصرفي عن طريق الاحتيال في غضون ثلاثة اشهر[59]

الفرع الثالث: مؤشرات الاحتيال المالي الالكتروني:

تتنوع مؤشرات الاحتيال المالي الالكتروني، والتي تعد بمثابة عناصر مساعدة في اتخاد القرار بشأن موثوقية المعاملات ومن أبرزها ندكر ما يلي:

- **قيمة المعاملة:** وتتمثل في تنفيذ عمليات بمبالغ ضخمة لا تتماشى مع النمط الاستهلاكي المعتاد لصاحب الحساب.
- **الانحراف الجغرافي:** رصد حركات مالية صادرة من مواقع مكانية بعيدة عن النطاق الذي ينشط فيه العميل عادة حيت تشير المعاملات التي تتم من أماكن غير مألوفة او بلدان غير معتادة لنشاط صاحب الحساب الى احتمال احتيال.
- **وقت المعاملة المشبوه:** تنفيذ العمليات في أوقات غير مألوفة، كالساعات المتأخرة من الليل.
- **عدد المعاملات في اخر 24 ساعة:** يشير التكرار الغير طبيعي للتحويلات المالية خلال فترة زمنية وجيزة الى احتمال هجوم او احتيال.
- **نوع المعاملة:** زيادة الحدر اتجاه عمليات السحب النقدي او التحويلات الفورية لسهولة استغلالها من طرف المحتالين.
- **هوية الجهاز:** التنبيه عند استخدام جهاز جديد او غير معرف مسبقا للنظام.[60]

المطلب الثالث: اثار الاحتيال المالي الالكتروني وقصور الطرق التقليدية في كشفه.

يعد الاحتيال المالي الالكتروني من أخطر الجرائم الرقمية، لما يخلفه من اثار مالية ونفسية ومجتمعية، وتزداد صعوبة كشفه بتعقيد اساليبه وضخامة البيانات، بينما تفشل الطرق التقليدية في مجاراته. لذلك في هذا المطلب

[59] GIUSEPPE VECCHIETTI, GAJENDRA LIYANAARACHCHI, GIAMPAOLO VIGLIA ,MANAGING DEEPFAKE WITH ARTIFICIAL INTELLIGENCE :INTRODUCING THE BUSINESS PRIVACY CALCULES ,JOURNALOFBUSINESS RESARCHE,14/08/2024,pp1-2,doi .org : https://doi.org/10.1016/j.jbusres.2024.115010

[60] فراحي فضيلة، نموذج تعلم الي لكشف الاحتيال في بطاقة الائتمان– تطبيق عملي على منصة تفاعلية، مجلة دفاتر اقتصادية، المجلد 16، العدد1، 2025 ,ص 518

سـنعرض اثار الاحتيال المالي الالكتروني وتحديات كشـفه تم قصـور الطرق التقليدية، مما يبرز الحاجة لتقنية اكثر فعالية في كشفه مثل خوارزميات تعلم الالة.

الفرع الأول: اثار الاحتيال المالي الالكتروني:

تتجاوز اثار الاحتيال المالي الالكتروني الخسـائر المادية المباشـرة لتمتد الى زعزعة اسـتقرار النظام المالي وتهديد امن المجتمع وتتجلى أبرز هده الأثار فيما يلي:

- **تعطل الخدمات الحيوية:** يؤدي تعطل مؤسـسـة كبرى تقدم خدمات مثل المقاصـة أو التسـوية إلى شـلل في القطاع المالي بالكامل وتوقف في معالجة المعاملات، لعدم وجود بديل سريع يقوم بنفس الدور
- **التشكيك في سلسلة المعاملات المالية:** تؤدي المخاوف بشأن سلامة البيانات الى تشكيك صحة سلسلة كاملة من المعاملات المالية، مما يتسبب في وقف النشاط المالي لفترات طويلة للتحقق.
- **أزمات السـيولة:** تتأثر السـيولة بسـرعة نتيجة فقدان الثقة، مما يؤدي الى انقطاعات في النظام وقطع روابط الاتصـال تمنع المؤسـسـات السـليمة مالياً من الوصـول إلى التمويل، مما يضـعف قدرتها على إدارة المخاطر والإقراض[61]
- **تهديد على الاسـتقرار المالي:** يسـاهم الاحتيال المالي الالكتروني في تشـويه أسـعار السـلع والخدمات واضـطراب في الأسـواق، مما يؤدي الى انخفاض كفاءة تخصـيص الأصـول وصـعوبة اتخاد قرارات مالية فعالة.
- **المنافسـة الغير عادلة:** تواجه الشـركات المشـروعة منافسـة غير متكافئة مع جهات تسـتخدم أموالا غير مشروعة، وهو ما قد ينعكس سلبا على سوق العمل ويزيد معدلات البطالة.
- **التهديد على امن ورفاهية المجتمع:** يمتد اتر الاحتيال ليمس اسـتقرار الافراد المادي والنفسـي، مما يهدم السلم الاجتماعي والرفاهية العامة.[62]
- **تآكل الثقة والولاء :** يزعزع الاحتيال ثقة جميع أصـحاب المصـلحة، بمن في ذلك المسـتثمرون، الدائنون، البنوك، الحكومة، المستهلكون، مما يضعف الولاء للمنظمة المالية.
- **الخسائر اقتصادية وضرر السمعة:** يتسبب الاحتيال في خسائر مالية مباشرة بالإضافة الى احاق اضرار بالغة بسمعة الحكومات والقطاعات المؤسسية والمساهمين.

[61] FRANK ADELMAANN, ET AL, CYBER RISK AND FINANCIAL STABILITY:IT S A SMALL WORLD AFTER ALL, IMF STAFF DISCUSSION NOTE, SDN /20/07, DECEMBER 2020, P 11, FROM: https://www.imf.org/-/media/files/publications/sdn/2020/english/sdnea2020007.pdf

[62] LUDIVIA HERNANDEZ AROS,LUISA XIMENA BUSTAMANTE MOLANO,ET AL ,FINANCIAL FRAUD DETECTION THROUGH THE APPLICATION OF MACHINE LEARNING TECHNIQUES: A LITERATURE REVIEW,JOURNAL HUMANITIES & SOCIAL SCIENCES COMMUNICATIONS, 3/09/2024, VOL11, ARTICLE NUMBRE 1130, P13,DOI : https://doi.org/10.1057/s41599-024-03606-0

- **انخفاض قيمة الأسهم واستبعاد الشركات:** تؤدي فضائح الاحتيال الى انخفاض قيم المساهمين واستبعاد الشركات من البوصات العالمية وتضرر سمعة الأسواق المدرجة فيها، حيث تشير الدراسات إلى أن قيم المساهمين في الشركات الألمانية انخفضت بمعدل 81 مليون يورو بسبب الإعلان عن الاحتيال، كما أدت فضيحة (Luckin Coffee) إلى استبعاد شركات من البورصة الصينية وتضرر سمعة شركات أخرى مدرجة.
- التأثير على جاذبية الاستثمار: يعتبر انتشار الاحتيال المالي من اهم العوامل المنفرة للمستثمرين، حيث يقلل من موثوقية الشركات وجدوى الاستثمار فيها.
- **تحفيز البحث والتطوير لإيجاد الحلول:** يمتل تزايد الاحتيال الدافع الرئيسي والمنطلق العلمي الذي يحفز الباحثين والخبراء لتطوير خوارزميات ومناهج تقنية جديدة لكشف الاحتيال والتصدي لها.[63]
- **البيع الغير قانوني للبيانات الشخصية:** يؤدي الاحتيال الى وصول المهاجمين للبيانات الشخصية مما قد يتم إساءة استخدامها او بيعها في الأسواق السوداء بشكل غير قانوني.[64]

الفرع الثاني: تحديات كشف الاحتيال المالي الإلكتروني:

تواجه عملية كشف الاحتيال المالي الالكتروني جملة من التحديات الواقعية والتقنية أهمها:

- **عزوف الضحايا عن الإبلاغ:** يمتنع الكثير من الضحايا عن التبليغ نتيجة ضغوط عاطفية: كالشعور بالإحراج أو الخوف من نظرة المجتمع مما يؤدي الى صعوبة حصر حجم الظاهرة.[65]
- **صعوبة تحديد الموقع:** يقع الاحتيال في بيئة عابرة للحدود مما يصعب ملاحقة الجناة دوليا وتحديد موقعهم الفعلي وملاحقتهم قضائيا.
- **توظيف الذكاء الاصطناعي في الأنشطة الاجرامية:** يساهم تطور الذكاء الاصطناعي واستخدامه في الاحتيال في مضاعفة حجم الأنشطة الضارة وتأثيراتها على الضحايا.
- **سهولة الوصول والانتشار:** يؤدي الاحتيال الى الوصول لعدد لا يحصى من المستثمرين حول العالم وبسرعة فائقة مما يجعل ملاحقة كل حالة احتيال أمراً معقدا.
- **تعقيد المنتجات المالية:** تزايد المنتجات الرقمية المعقدة التي يصعب على المستثمر العادي فهم مخاطرها، مما يسهل استغلاله.

---

[63]HESHAN GUAN, SIYING LI, QIAN WANG, OLEKSII LYULYOV, TETYANA PIMONENKO, « FINANCIAL FRAUD IDENTIFICTION OF THE COMPANIES BASED ON THE LOGISTIC REGRESSION MODEL." JOURNAL OF COMPETITIVENESS, VOL 14, NO 4,04/ 2022, p156

[64]MERYEM TOUIL, LEGAL PROTECTION OF ELECTRONIC PAYMENT METHODES, JOURNAL OF LAW AND POLICITICAL SCIENCE, KHENCHELA UNIVERSITY, VOLUME 12, ISSUE 02,07/2025,P578

[65]FATF, EGMONT GROUP, INTERPOL, ILLICITE FINANCIAL FLOWS FROM CYBER -ENABLED FRAUD, OP.CIT, P33

- **قصـــور الأطر الرقابية والقانونية:** الحاجة الملحة للتحديث المســتمر للقوانين ومرونة الصـــلاحيات الرقابية لتواكب التغيرات المتسارعة في البيئة الرقمية[66]
- **ضخامة وتعقيد البيانات:** أصبحت البيانات المرتبطة بالكشف عن الاحتيال ضخمة ومعقدة، وهو ما يتجاوز قدرات الأساليب التقليدية.
- **محدودية المعرفة التخصصية:** رغم اهتمام المنظمات والهيئات والباحثين بكشف الاحتيال المالي الالكتروني لكن لاتزال المعرفة الحالية في هذا المجال محدودة.
- **إشـــكالية انذارات الاحتيال الكاذبة:** أحد التحديات الرئيســـية هو الحاجة إلى تقليل إنذارات الاحتيال الكاذبة لضمان استجابة دقيقة ومنع التأثير السلبي على المنظمات.
- **ديناميكية الجرائم الســـيبرانية:** حيت ان التحدي الكبير يكمن في بناء أليات قادرة على اكتشـــاف المعاملات غير العادية ومنع الجرائم السيبرانية التي تطور باستمرار.[67]
- **غياب، المعايير الموحدة:** يمتل غياب لغة مشـتركة او قاعدة بيانات عالمية موحدة للإحصـائيات عائقا امام اجراء تحليلات مقارنة دقيقة او تشخيص عميق لحجم المشكلة عالميا.
- **صـــــعوبة القياس مقارنة بالمخاطر الأخرى:** على عكس المخاطر المالية التقليدية (مثل مخاطر الائتمان) التي لها مؤشرات واضحة ويسهل التنبؤ بها، يتسم الاحتيال بـــــ "الندرة والتشتت." مما يحول دون "مؤشرات قياسية" ثابتة تساعد المؤسسات في استشراف الهجمات قبل وقوعها.[68]

الفرع الثالث: قصور الطرق التقليدية في كشف الاحتيال المالي الالكتروني:

تكمن إشـــكالية مكافحة الاحتيال المالي الالكتروني في عجز الادوات الكلاســـيكية عن مواكبة الطبيعة التقنية والمعقدة لهده الجرائم، وهو ما يظهر من خلال القصور التالية:

- **مشـــــكلة الذيول الثقيلة:** حيت أن توز بعات خســـــائر الهجمات تتميز بالذيول الثقيلة، مما يجعل التحليل الإحصائي المبني على الطرق التقليدية معقدا وغير دقيق في التنبؤ بالخسائر المستقبلية الكارثية
- **شـح وتقادم البيانات:** محدودية البيانات المتاحة حول تكرار وشدة الهجمات، وأن الطبيعة المتطورة للهجمات تجعل البيانات التاريخية غير كافية لتقدير المخاطر

[66] IOSCO, IOSCO STATEMENT ON ONLINE HARM, OP.CIT, PP1-4

[67] LUDIVIA HERNANDEZ AROS, LUISA XIMENA BUSTAMANTE MOLANO, ET AL, FINANCIAL FRAUD DETECTION THROUGH THE APPLICATION OF MACHINE LEARNING TECHNIQUES: A LITERATURE REVIEW, OP.CIT, P2

[68] ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS (ASBA). DIGITAL FRAUD IN BANKING . TRENDS AND PRACTICES FOR MITIGATION. EXECUTIVE SUMMARY, OP.CIT, P2

- **الافراط في التقييم النوعي:** ان الأســـاليب التقليدية تعتمد بشـــكل مفرط على التقييم النوعي وأحكام الخبراء، وهي بحاجة للتطوير نحو نماذج كمية أكتر دقة[69]
- **عجز القوانين الإجرائيـة:** لا تتلاءم القوانين الإجرائيـة التقليـديـة مع طبيعـة الأدلـة الرقميـة القـابلـة للتغيير والاتلاف.
- **محدودية أسـاليب التحقيق التقليدية:** أسـاليب التحقيق الكلاسـيكية وحدها لم تعد كافية للوصـول إلى الأدلة والحصول عليها في الجرائم المعلوماتية العابرة للحدود التي تتم في فضاء سيبراني مفتوح.
- **ضـعف التعاون الدولي التقليدي:** يواجه صـعوبات فريدة بسـبب الطبيعة المتطايرة للأدلة الرقمية، مما يجعل الوسائل القديمة بطيئة وغير فعالة في ملاحقة الجناة،
- **إشكالية حجية الإثبات:** توجد حاجة ماسـة لإجراءات واحتياطات خاصـة لتوثيق وجمع وحفظ وفحص الأدلة الرقمية لضمان قبولها كمصادر إثبات رسمية في المحاكم.
- **الحاجة الى اليات تحقيق هجينة:** ودلك من خلال ضـــرورة الجمع بين التحقيق التقليدي وتقنيات حديثة تشـــمل: أوامر الحصـــول على بيانات الكمبيوتر، الجمع الفوري للبيانات أثناء انتقالها، أوامر الحفاظ على البيانات لمنع مسحها.[70]

المبحث الثاني: الإطار المفاهيمي لخوارزميات التعلم الالي ودورها في كشف الاحتيال المالي الالكتروني.

في ظل تعقيد ظاهرة الاحتيال المالي الالكتروني، برزت الحاجة الى اســتخدام تقنيات حديته قادرة على تحليل البيانات واكتشــاف الأنماط الغير عادية ومن أبرزها خوارزميات تعلم الالة. وعليه سـيتم في هذا المبحث التطرق الى من المفهوم العام للخاص لدلك لابد من الاحاطة بمفهوم الذكاء الاصــطناعي باعتباره الأســاس الدي تقوم عليه هده التقنيات تم تعلم الالة كفرع من فروعه وانواعها والية عملها تم اهم الخوارزميات المستخدمة في هذا المجال ودورها في اكتشاف الاحتيال المالي الالكتروني بهدف ابراز أهميتها كأساس علمي يعتمد عليه في الجانب التطبيقي.

المطلب الأول: مفاهيم حول الذكاء الاصطناعي

[69] FRANK ADELMAANN, ET AL, CYBER RISK AND FINANCIAL STABILITY:IT S A SMALL WORLD AFTER ALL, IMF STAFF DISCUSSION NOTE, OP.CIT, P14

[70] DIMOSTHENIS CHRYSIKOS ,INTERNATIONAL LEGAL FRAMEWORKS FOR COMBATING CYBERCRIME:THE UNODC PERSPECTIVE ,PRESENTATION NINTH MEETING OF OAS REMJA WORKING GROUP ON CYBERCRIME,WASHINGTON D.C,DECEMBER 2016 ,P12 -13,FROM : https://www.oas.org/juridico/pdfs/cyb9-unodc-dec16 -v1.pdf

لا يمكن فهم دور خوارزميات تعلم الالة في كشـــف الاحتيال المالي الالكتروني دون الإشـــارة الى الذكاء الاصـطناعي الذي تحتضـنه، فهو البيئة الاوسـع التي وفرت الأسـاس المنطقي والتقني لظهور هذه الخوارزميات، وهو ما يستوجب التوقف عند تعريفه واستخداماته قبل الانتقال الى فروعه.

الفرع الأول: تعريف الذكاء الاصطناعي(AI):

لقد تعددت المقاربات المفاهيمية للذكاء الاصـــطناعي بســـبب تعدد اســـتخداماته وطبيعته المتطورة وتقنياته المختلفة وتداخله مع مجالات معرفية شتى ومن أبرزها ما يلي:

- **تعريف (01):** عرفته منظمة التعاون والتنمية الاقتصـادية (OECD): انه عبارة عن أنظمة الية مصـممة لمعالجة البيانات والمدخلات بهدف صـياغة مخرجات متنوعة، تشـمل التنبؤ بالنتائج او تقديم مقترحات واتخاد قرارات ذات اتر ملموس في الواقع الفعلي او الرقمي وتتميز هده الأنظمة بقدرات متباينة على التكيف الذاتي والعمل باستقلالية وفقا للمهام المملوكة [71]
- **تعريف (02):** العلم الذي يطور أنظمة ذكية قادرة على تنفيذ مهام دهنية بشـرية معقدة وتوسـيعها وتسـريع سـرعة معالجتها تحاكي الوظائف التي يقوم بها الدماغ البشري متل الفهم والتذكر والادراك والتفكير مما يوفر حلولا مبتكرة وسريعة تعالج تحديات ومشكلات العصر في مختلف الميادين.[72]
- **تعريف 3:** يرى بروس بوشـان وادوارد شـورتليف ان الذكاء الاصـطناعي هو: انه ذلك المسـار التقني ضـمن علوم الحاسوب الذي يرتكز على تطوير تقنيات لمعالجة الرموز والبيانات بطرق غير تقليدية ودلك بغرض الوصـول الى حلول للمشكلات المعقدة
- **من خلال ما سـبق نعرف الذكاء الاصـطناعي انه:** فرع متطور من علوم الحاسـوب يسـعى لإنتاج برامج وأجهزة تمتلك قدرات تحليلية تشبه العقل البشري في الادراك والاستنتاج وحل القضايا ولا تقتصر على تنفيذ الأوامر فحسب بل تقوم بتطوير اداءها تلقائيا لإنتاج حلول ذكية ومخرجات دقيقة تسـاهم في تيسـير المهام المعقدة وتجاوز عوائق العصر الرقمي والواقعي بفعالية.

الفرع الثاني: أهمية الذكاء الاصطناعي

- **تطوير التفاعل بين الانســـان والالة:** حيت تبرز أهميته في جعل التكنولوجيا متاحة للجميع عبر التواصـــل باللغة البشرية ما أنهى حصر التعامل مع الآلات على المبرمجين

[71] خير الدين بوزرب، عبد الرؤف عباسـي، **الذكاء الاصطناعي كأداة استراتيجية في مكافحة غسيل الأموال في البنوك : عرض تجربة بنك (hsbc) وبنك (Danske)**، مجلة دراسات اقتصادية، المجلد 19، العدد 3، 2025، ص 553.

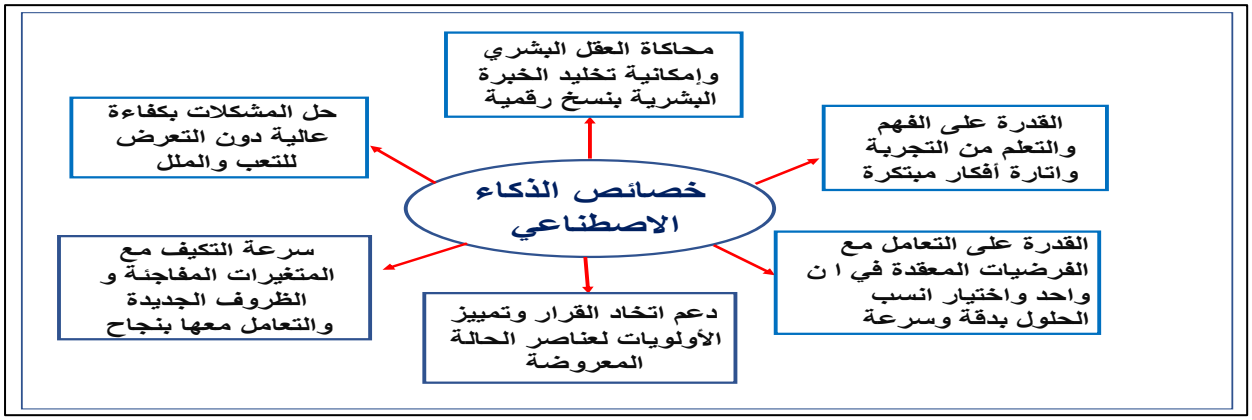
[72] خراز عبد الحق ,شـاربي بلقاسـم ,الذكاء الاصـطناعي وتطوير الأداء الرياضـي :من التحليل البدني والتكتيكي الى الاعداد الفني والذهني ,مجلة روافد للدراسات والابحات في علوم الرياضة ,المجلد 6, العدد 1, 2026 , ص195

- **دعم التخصـــصـــات الحيوية:** ودلك بتقديم حلول تطبيقية مرنة ودقيقة في مجالات متنوعة كالمجال المالي والطب والقانون والتعليم
- **نزاهة القرار وعدم تحيزه:** تكمن جدواه في تقديم قرارات منطقية ومســتقلة تضــمن تجاوز الأخطاء البشــرية والتحيزات الشخصية او العرقية
- **إدارة المهام الحرجة:** يحمي الانسان من المخاطر الجسدية والنفسية عبر انابة الالة في تنفيذ المهام الشاقة والخطرة والعمليات الاستكشافية المعقدة. [73]

الفرع الثالث: خصائص الذكاء الإصطناعي

يتميز الذكاء الاصطناعي بمجموعة من الخصائص نختصر أبرزها في الشكل الموالي:

الشكل رقم01 -05: خصائص الذكاء الاصطناعي



المصدر: من اعداد الطالبة, بالاعتماد على : زهواني مروة، تطبيقا ت نماذج الذكاء الاصطناعي للتنبؤ بمخاطر التعثر المالي في المؤسسة الاقتصادية -دراسة حالة -,أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في العلوم الاقتصادية تخصص نقدي وبنكي، جامعة غرداية، جوان 2022,ص 13

الفرع الرابع: تطور استخداماته في ظل البيانات الضخمة المالية

أصبح الذكاء الاصطناعي أداة أساسية في تطوير الخدمات المالية حيث ساهم في أتمته المهام وتحسين دقة القرارات الاستثمارية وكشف الأنماط المشبوهة والتصدي لعمليات الاحتيال الالكتروني بشكل الي انطلاقا من تحليل البيانات الضخمة لهاته المعاملات مما عزز من موثوقية المعاملات المالية الرقمية ومن أبرز استخداماته في القطاع المالي نجد ما يلي:

- **كشـــف الاحتيال المالي الالكتروني:** تحليل بيانات المعاملات المالية في الوقت الفعلي لكشـــف الأنماط المشبوهة والحالات الشاذة التي قد تشير الى نشاط احتيالي.

[73] خيرة حنش، احمد بن الشين، **الذكاء الاصطناعي بين الابتكار والمسؤولية الأخلاقية في البحث العلمي**، مجلة العلوم الإسلامية والحضارة، المجلد 10، العدد 2، 2025، ص 602-603

- **إدارة المحافظ الاستثمارية:** استخدام التحليلات المتقدمة لتحسين استراتيجيات الاستثمار، وتخصيص المحافظ حسب تفضيلات المستثمر وقدرته على تحمل المخاطر وإعادة توازن المحفظة اليا.
- **التداول الخوارزمي:** تحليل كميات هائلة من السوق بسرعة ودقة عالية مما يمكن المتداولين من تنفيذ استراتيجيات معقدة واستغلال لفرص العابرة في الوقت الفعلي.
- **إدارة المخاطر:** تحليل مصادر بيانات متنوعة كاتجاهات السوق والبيانات التاريخية والمؤشرات الاقتصادية الكلية لتوقع المخاطر المحتملة.
- **خدمة العملاء:** استخدام Chabots والمساعدين الافتراضيين للتفاعل مع العملاء بلغة طبيعية وتقديم توصيات مخصصة والإجابة عن الاستفسارات وتسهيل المعاملات على مدار الساعة.[74]
- **التنبؤ بالإفلاس**
- **تقييم الجدارة الائتمانية:** بناءا على نماذج التسجيل الائتماني او الموافقة على القروض
- **التحليلات السلوكية:** للمستثمرين عبر تحليل المشاعر
- **مراقبة الامتثال التنظيمي للمؤسسات المالية** [75]
- **زيادة امان المعاملات المالية:** ودلك عن طريق دمج البلوك تشين مع الذكاء الاصطناعي في زيادة امان المعاملات المالية وشفافيتها.
- **التمويل المستدام:** يمكن للذكاء الاصطناعي تقديم رؤى دقيقة وفورية حول مقاييس الاستدامة للاستمارات.
- **التمويل الأخضر:** يمكن للدكاء الاصطناعي المساعدة في التوجيه نحو الاستثمارات الخضراء وتمييز الأثر البيئي الناتج عن الاستثمار تم توجيه مديري المحافظ نحو اتجاه اكتر اخضرارا.
- **التنبؤ المالي والاقتصاد القياسي:** عن طريق دمج الذكاء الاصطناعي والاقتصاد القياسي من اجل ان يكون اكتر موضوعية في فهم ديناميكيات السوق وتقلباته بالتالي التنبؤ الأفضل بالأسعار.[76]

المطلب الثاني: التعلم الالي كفرع من فروع الدكاء الاصطناعي

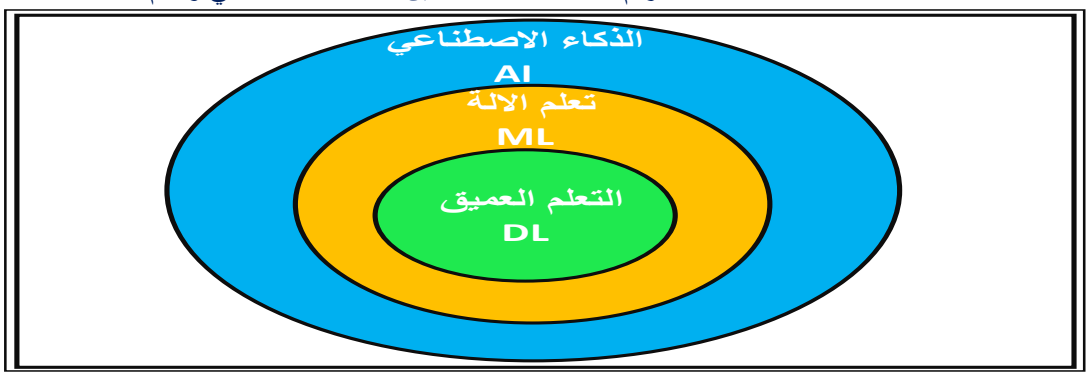
يعد الذكاء الاصطناعي مجالا واسعا يضم عدة فروع وتخصصات تهدف الى تمكين الآلات من محاكاة القدرات الذهنية للإنسان واكتشاف الأنماط الخفية والتعلم المستمر من أبرزها تعلم الالة التي تعد الأداة التنفيذية المباشرة والجسر الذي يصل بين مفاهيم الذكاء الاصطناعي وتطبيقات كشف الاحتيال كما يوضحه الشكل التالي:

[74] D.DIVAY, ET AL, ARTIFICIAL INTELLIGENCE IN FINANCE, CONFERENCE PAPER ON INNOVATION AND TRANSFORMATION: REVOLUTIONIZING THE BUSINESS WORLD WITH BREAKTHROUGH CREATIVITY, SRI RAMAKRISHNA COLLEGE OF ARTS AND SCIENCE, COIMBATORE, INDIA,2 /2024, P220 -221

[75] SALMAN BAHOO, ET AL, ARTIFICIAL INTELLIGENCE IN FINANCE: A COMPREHENSIVE REVIEW THROUGH BIBLIOMETRIC AND CONTENT ANALYSIS, SN BUSINESS AND ECONOMICS A SPRINGER NATURE JOURNAL, VOL 4, N23,2024, P23

[76] JYOTHI. G, PAVANKUMAR G KULKARNI, ARTIFICIAL INTELLIGENCE IN FINANCE ;A LITERATURE REVIEW ,REVISTA DE CIENCIAS DE GESTION ;360,N10,P8 -9

الشكل رقم 01 -06: العلاقة بين الذكاء الاصطناعي وتعلم الالة



المصدر: من اعداد الطالبة , بالاعتماد على , MATTHEW N .O.SADIKU,ET AL,MACHINE LEARNING :AN OVERVIEW,INTERNATIONAL JOURNAL OF TREND IN SCIENTIFIC RESARCHE AND DEVELOPMENT ,VOL 9,N 5, 9 /2025,P 1130

الفرع الأول: تعريف تعلم الالة والية عمله(ML):

لقد تعددت تعريفات لتعلم الالة بتعدد زاوية النظر اليه، سواءا كعلم قائم على التجربة او كأداة إحصائية متطورة ومن أبرز ما صيغ في هدا الإطار ما يلي:

- **تعريف 1:** هو مصطلح صاغه العالم (Arthur Sameul) عام 1959 يرتكز هذا على تطوير خوارزميات تمنح الحاسوب القدرة على الاكتساب الذاتي للمعرفة من خلال تحليل التجارب والبيانات السابقة مما يجعله مؤهلا لاستنباط التوقعات واتخاد القرارات الذكية دون الحاجة لبرمجة مباشرة لكل خطوة.[77]
- **تعريف 2:** يعد تعلم الالة أحد أبرز فروع الدكاء الاصطناعي المتخصصة في أتمته النمذجة التحليلية وتعتمد اليته على معالجة البيانات بشكل تكراري يكسب الأنظمة قدرة ذاتية على استنباط الأنماط وتطوير جراءتها على الملاحظات المستمرة ويتميز عن الإحصاء التقليدي بتركيزه على خوارزميات رياضية تستهدف تعظيم الكفاءة التنبؤية بدلا من الاكتفاء بالأطر الاحتمالية وتبرز تطبيقاته البحثية بوضوح في مجالات التصنيف، الانحدار الخطي، تحليل المجموعات.[78]
- **تعريف 3:** هو استخدام مزيج من الخوارزميات الحاسوبية والنماذج الإحصائية للسماح للكمبيوتر بإنجاز المهام دون الحاجة الى برمجة صريحة. [79]
- **من خلال ما سبق نعرف تعلم الالة انه:** أحد فروع الذكاء الاصطناعي الذي يركز على منح الأنظمة الحاسوبية قدرة ذاتية على تطوير اداءها والتنبؤ بالنتائج وذلك عبر معالجة البيانات واستخراج الأنماط الكامنة فيها، مما يلغي

[77] سامية بوضياف، فيصل بهلولي، استخدام الذكاء الاصطناعي لدراسة علاقة أسعار النفط، الصرف، الذهب، بالتضخم والتنبؤ به في الفترة الممتدة من جوان 2006 –أفريل 2020 ,مجلة (les cahiers du cread), المجلد 39 , العدد 1 ,2023 , ص 394

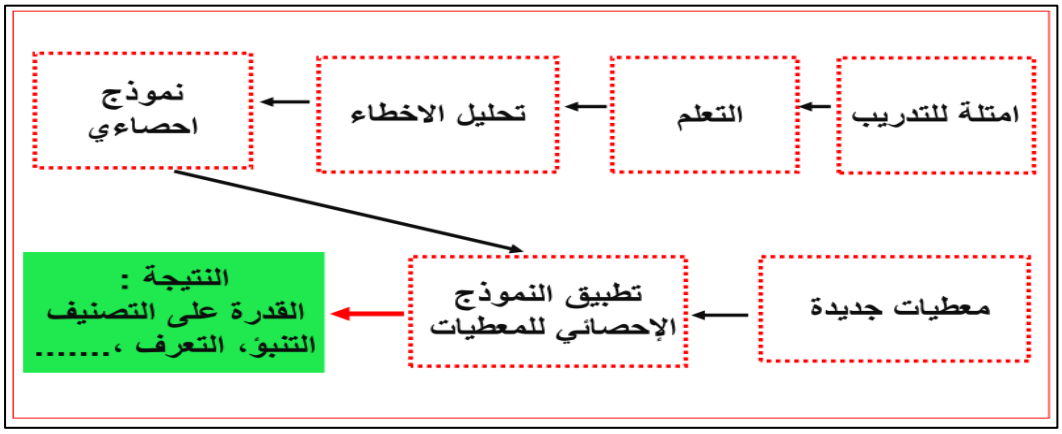
[78] كريم محمد محافظ حافظ توفيق القاضي، اتر تطبيق تقنيات التعلم الالي على مراحل عملية المراجعة الخارجية للكشف عن الاحتيال المحاسبي – دليل عملي من الشركات المقيدة بالبورصة المصرية – , المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد17 , العدد 1, 2025/3 , ص 92

[79] M.VALVAN ,S.RITA ,PREDIACTIVE -ANALYSIS -BASED MACHINE LERNING MODEL FOR FRAUD DETECTION WITH BOOSTING CLASSIFICATION ,JOURNAL COMPUTER SYSTEM SCIENCE AND ENGINEERING ,VOL 45,N 1,P 232

الحاجة للبرمجة التفصـــيلية لكل عملية، ويحول البيانات الخام الى قرارات ذكية بناءا على التجربة والنمذجة الرياضية.

- **ونبرز الية عمل تعلم الالة (Machine Learning Mechanism) من خلال الشكل ادناه:**

الشكل رقم01 -07: الية عمل تعلم الالة



المصـــدر: من اعداد الطالبة , بالاعتماد على , عبد الكريم حرز الله، التعلم الالي كجزء من الذكاء الاصـطناعي، مجلة العلوم والتكنولوجيا، العدد التجريبي، ماي 2019، ص 15

حيث تتمثل الديناميكية الإجرائية لعمل تعلم الالة من خلال تزويد الحاسوب ببيانات وأمتله ضخمة ليقوم ذاتيا ببرمجة خوارزميات تبني تمثيلا داخليا للمهام فعلى عكس الأســـاليب البرمجية التقليدية يظهر الشـــكل أعلاه الالية الديناميكية لتعلم الالة حيث لا يكتفي النظام باســـتقبال البيانات بل يدخل في دورة من تحليل الأخطاء والمقارنة بين النتائج الحقيقية والمتوقعة حيت يتم معالجة هذه البيانات حتى الوصـــول الى مرحلة الاســـتقلال في الأداء واتخاذ القرارات دون تدخل بشـري مباشـر حيت فنلاحظ انه من خلال امتله التدريب والتعلم المسـتمر وتحليل الأخطاء تعمل خوارزميات التعلم الالي على اســتخلاص نموذج احصـــاءي هدا النموذج هو المحرك الدي يعالج المعطيات الجديدة والحقيقية لتقديم مخرجات دقيقة على ارض الواقع سواء عبر التنبؤ او التصنيف او التعرف...الخ. [80]

الفرع الثاني: قدرات وامكانيات تعلم الالة

يتميز تعلم الالة بمجموعة من القدرات التي تمكنها من التعلم الذاتي والتطور المســـتمر مما يجعلها العمود الفقري لمختلف التطبيقات الذكية الحديثة ومن أبرز هده القدرات:

- **معالجة وتحليل البيانات الضـــخمة:** يتميز تعلم الالة بقدرته على فحص مجموعات هائلة من البيانات واستخلاص الانماط والمعلومات الكامنة فيها، وهي مهمة تتجاوز القدرات البشرية في التحليل.

[80] عبد الكريم حرز الله، **التعلم الالي كجزء من الذكاء الاصطناعي**، مرجع نفسه، ص 15

- **التعلم الذاتي المستند الى البيانات:** يمنح تعلم الالة الأنظمة القدرة على اكتساب المعرفة وتطوير قواعد منطقية ذاتيا من خلال تزويدها ببيانات التدريب، مما يساعد النماذج على صياغة أنماط تدعم اتخاذ القرارات بذكاء.
- **تعددية المجالات والتطبيقات:** تمتد استخدامات تعلم الالة لتشمل طيفا واسعا من القطاعات الحيوية متل: القطاع المالي، الروبوتات، معالجة اللغات الطبيعية، والتعرف الرقمي على الأصوات والصور.
- **القدرة التنبؤية:** تستطيع نماذج تعلم الالة تطبيق الأنماط التاريخية المكتشفة، لتوليد توقعات دقيقة حول الاتجاهات المستقبلية، مما يقلل عدم اليقين ويوجه عمليات اتخاذ القرارات بفعالية.
- **التطوير المستمر للأداء:** تعمل على تحسين كفاءة الأنظمة بشكل تراكمي مع مرور الوقت، حيت يتم تحديت النماذج وضبطها باستمرار بناءا على البيانات الجديدة التي ترد اليها.
- **كشف الأنماط والترتيبات الخفية:** تبرع نماذج تعلم الالة في تحديد العلاقات والروابط المعقدة وغير الظاهرة داخل البيانات، مما يساهم في تعميق الفهم وتوفير رؤى تحليلية اكتر دقة.[81]

الفرع الثالث: انماط تعلم الالة

تتنوع أنماط تعلم الالة تبعا لطبيعة البيانات المستخدمة والية تدريب الخوارزميات ويمكن تقسيمها الى 5 أنماط أساسية كما هو موضح في الجدول التالي:

جدول رقم :01-14: أنماط تعلم الالة

النمط	التعريف	الهدف الاساسي
التعلم الخاضع للإشراف Supervied Learning	يتم تدريب البرنامج على مجموعة من الأمثلة المعروفة من البيانات حيت يستخدم لتسهيل الوصول الى استنتاجات دقيقة، عند اعطاءه بيانات جديدة. في هده الحالة تأتي البيانات مع سمات إضافية نرغب في التنبؤ بها. ومن امتلته استخدام البيانات التاريخية لتوقع الأحداث المحتملة في المستقبل.	التنبؤ او التصنيف لبيانات جديدة بناءا على بيانات مصنفة مسبقا
التعلم الغير خاضع للإشراف Unsupervised Learning	يوصف بانه نوع من التعلم التحسيني الذاتي حيت لا يحتاج الى بيانات ذات نتائج محددة مسبقا. يعطى البرنامج مجموعة من البيانات، ويطلب منه اكتشاف الأنماط المخفية في البيانات والعلاقات داخلها مما يساعد في تنظيم البيانات بطريقة هادفة.	استخراج الأنماط الخفية والعلاقات دون الحاجة الى تصنيفات مسبقة

[81] كريم محمد حافظ توفيق القاضي، **أثر تطبيق تقنيات التعلم الالي على مراحل عملية المراجعة الخارجية للكشف عن الاحتيال المحاسبي – دليل عملي من الشركات المقيدة بالبورصة المصرية**–، مرجع سبق دكره, ص 94

التعلم شبه خاضع للإشراف Semi-Supervised Learning	مزيج من التعلم الخاضع للإشراف والغير خاضع للإشراف يستخدم كميات قليلة من البيانات المصنفة وكبيرة من البيانات الغير مصنفة	تحسين دقة النماذج استنتاج تصنيفات للبيانات الغير مصنفة تم تتعلم من الكل معا.
التعلم المعزز Reinforcemen Learning	يدرب هدا النوع بشكل تجريبي من خلال التجربة والخطأ، حيت يطارد النموذج تحقيق مكافئات، من خلال تخصيص قيمة للمراحل التي يمر بها. وكل هدا من اجل جمع أكبر عدد من النقاط أو المكافآت في النهاية.	اتخاد سلسلة من القرارات الصحيحة للوصول الى أفضل نتيجة ممكنة وتحسين الأداء بناءا على التفاعل مع البيئة
التعلم العميق Deep Learning	سمي بالتعلم العميق، لأنه يتكون من مستويات هرمية متعددة الخلايا العصبية حيت يستخدم الشبكات العصبية الاصطناعية لمحاكاة دماغ الانسان ويعد من التقنيات المتقدمة لمعالجة المهام المعقدة متل التعرف على الصوت والصورة.	حل مشكلات شديدة التعقيد والتميز والتصنيف بناءا على الأنماط المعقدة في البيانات الكبيرة.

المصدر من اعداد الطالبة ,بالاعتماد على مراجعات سابقة:[82] [83]

المطلب الثاني: خوارزميات تعلم الالة

تطرقنا في هدا المطلب الى تعريف خوارزميات تعلم الالة والية عملها , بالإضافة الى مختلف انواعها و معايير المقارنة بينها .

الفرع الأول: تعريف خوارزميات تعلم الالة واطارها العام:

لقد تنوعت تعريفات خوارزميات تعلم الالة ولكنها تلتقي في جوهر واحد يتمثل في تمكين الأنظمة من التعلم الذاتي من البيانات وتحسين اداءها بمرور الوقت ومن أبرز ما قدمه الباحتين من تعريفات نجد:

- **تعريف 1:** تعرف خوارزميات تعلم الالة بانها نظام من القواعد والعمليات الإحصائية التي تهدف الى تمكين الحواسيب من استخلاص الأنماط من البيانات وتطوير اداءها ذاتيا حيت تقوم ببناء استنتاجات وتنبؤات دقيقة بناءا على المعطيات المتوفرة مما يسمح باتخاذ قرارات ذكية اتجاه الحالات الجديدة والمستقبلية [84]

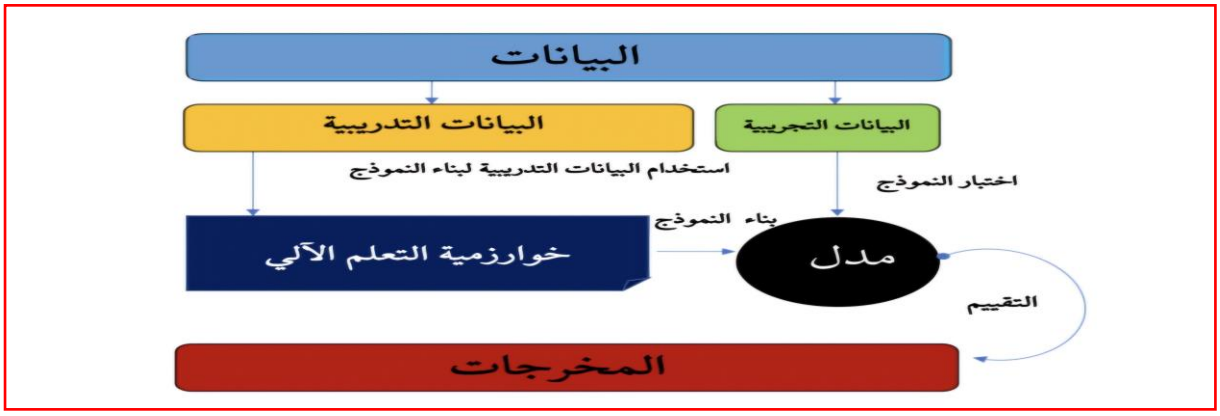
[82] ريم محمد محمود عبد المنعم واخرون، اتر التنبؤ بالأرباح المستقبلية باستخدام خوارزميات تعلم الالة كإحدى تقنيات الذكاء الاصطناعي على تعزيز ثقة المستثمرين –دراسة تطبيقية، مجلة الشروق للعلوم التجارية، العدد17، ماي 2025، ص 25-26

[83] MATTHEW N .O.SADIKU,ET AL,MACHINE LEARNING IN MEDIA AND ENTERTAINMENT ,INTERNATIONAL JOURNAL OF TREND IN SCIENTIFIC RESARCH AND DEVELOPMENT ,VOL 9,ISSUE 6, NOV -DEC 2025,P164

[84] مزاري نصر الدين، **دور خوارزميات التعلم الالي في استهداف الإعلانات: تهديد للخصوصية ام ضرورة تجارية؟ دراسة حالة (Facebook abs)**، مجلة التشريع الإعلامي، المجلد 3، العدد 1، 2024، ص9

- **تعريف2:** عملية تعتمد على تحليل البيانات واكتشاف أنماطها والتعلم منها من اجل بناء نماذج تعلم الي وتستخدم بشكل رئيسيي من اجل أداء 3 وظائف اساسية التصنيف والانحدار والتجميع [85]
- **تعريف 3:** هي نظام يعتمد على المنطق الرياضـــي لتحليل ســجلات البيانات، بهدف اكتشــاف الروابط المتكررة داخلها وتحويلها الى استنتاجات مفيدة[86]
- **من خلال ما ســـبق نعرف خوارزميات التعلم الالي:** هو أنظمة ذكية تمزج بين المنطق الرياضـــي والعمليات الإحصـــائية لتحليل البيانات واكتشـــاف انماطها العميقة، تهدف الى بناء نماذج تتعلم ذاتيا وتتطور مع الوقت، لتحويل البيانات الى تنبؤات دقيقة ووظائف عملية كالتصـــنيف والتجميع مما يمنح الحواســـيب القدرة على اتخاذ قرارات ذكية في مواقف جديدة دون الحاجة لبرمجة صريحة لكل خطوة.
- **الإطار العام لعملها:** يتمثل الإطار العام لعمل خوارزميات التعلم الالي بشكل أساسي على ابتكار نموذج رياضي قادر على التنبؤ بنتائج بيانات جديدة لم يسبق له التعامل معها وذلك بالاستناد الى أنماط المستخلصة ويتكون هدا النظام من ثلاثة اركان أساسية البيانات ساء المخصصة للتدريب او الاختبار وخوارزمية التعلم الالي التي تصيغ النموذج وعملية تقييم النموذج باســـتخدام بيانات التجريب حيث يتم قياس مدى دقة النتائج التي يتوقعها النموذج ومقارنتها بالنتائج الحقيقية وبمجرد التأكد من كفاءته يصبح النموذج جاهز لتوليد مخرجات نهائية.[87]

الشكل رقم01 -08: الاطار العام لعمل خوارزميات التعلم الالي



المصدر: ميلاد وزان، تعلم الالة وعلم البيانات - الأساسيات والمفاهيم والخوارزميات والأدوات، (ترجمة: علاء طعيمة)، مرجع سابق، ص 187

[85] ميلاد وزان، **تعلم الالة وعلم البيانات – الأساسيات والمفاهيم والخوارزميات والادوات**، (ترجمة علاء طعيمة)، عمان: دار المناهج للنشر والتوزيع، 2024، ص 185

[86] لمى عدنان عوكل، **دور استخدام خوارزميات الذكاء الصنعي في عمليات ضبط الجودة دراسة حالة** – مصنع الميسور للصـناعات البلاسـتكية– سـوريا– ريف دمشـق، بحث مقدم لنيل درجة الماجيسـتير في إدارة الجودة، الجامعة الافتراضـية السورية، 2021، ص 34

[87] ميلاد وزان، **تعلم الالة وعلم البيانات – الأساسيات والمفاهيم والخورزميات والادوات**، (ترجمة علاء طعيمة)، مرجع سابق ص 187

الفرع الثاني: أنواع خوارزميات تعلم الالة:

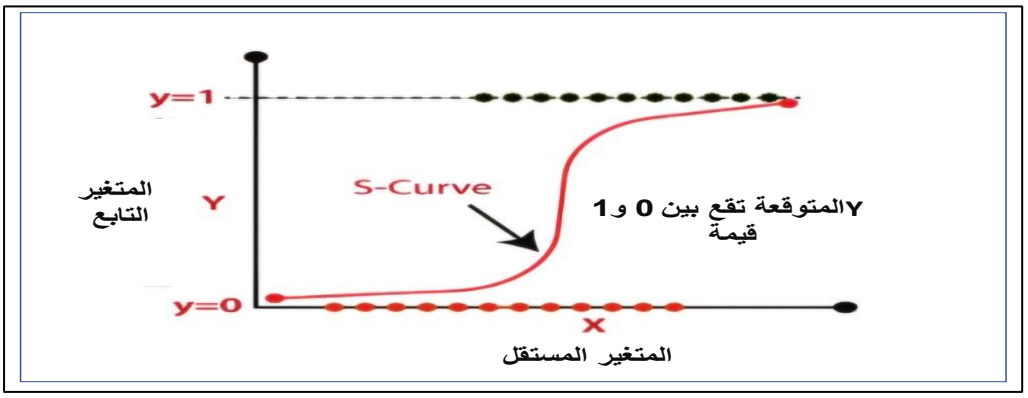
قمنا بتصنيف الخوارزميات بناءا على أنماط تعلم الالة الخمسة حيث قمنا باستعراض أبرزها كمايلي:

1- خوارزميات التعلم الخاضع للإشراف:

1-1- خوارزميات الانحدار: ومن أبرزها

- **خوارزمية الانحدار اللوجيستي (LogisticRégression):** هي خوارزمية تستخدم في مسائل التصنيف النتائج، حيث تقوم بتقدير احتمال انتماء العينة الى احدى الفئتين، يعتمد هدا النموذج على تطبيق دالة لوجستية على تركيب خطي للمدخلات، مما يحول القيم الناتجة الى احتمال يتراوح بين 0 و1. ويتم تصنيف العينة عادة الى الفئة 1 إذا كان الاحتمال أكبر أو يساوي 0،5 والى الفئة 0 إذا كان اقل من ذلك.[88]

الشكل رقم01 -09: الية عمل خوارزمية الانحدار اللوجستي



المصدر , بتصرف في الترجمة :

AMER F.A.H.ALNUAIMI ,ET AL ,AN OVERVIEW OF MACHINE LEARNING CLSSIFICATION TECHNIQUES ,JOURNAL BIO WEB OF CONFERENCES ,VOL 97,P12

- **خوارزمية الانحدار الخطي (Linear Regression)** : يعتمد على بناء علاقة خطية بين متغيرات الادخال والمتغير الهدف، فيقوم النموذج بتقدير القيمة المتوقعة من خلال جمع مدخلات البيانات مضروبة في اوزان معينة مع إضافة تابت الانحياز، ويتميز هدا النموذج ببساطته، وغالبا ما يعطي نتائج جيدة عندما تكون البيانات ذات علاقة خطية، بينما تقل دقته في حالة العلاقات الغير خطية، مما قد يستدعي نماذج اكثر تعقيدا او معالجة مسبقة للبيانات.[89]

1-2- خوارزميات الأشجار(Tree Algorithms):

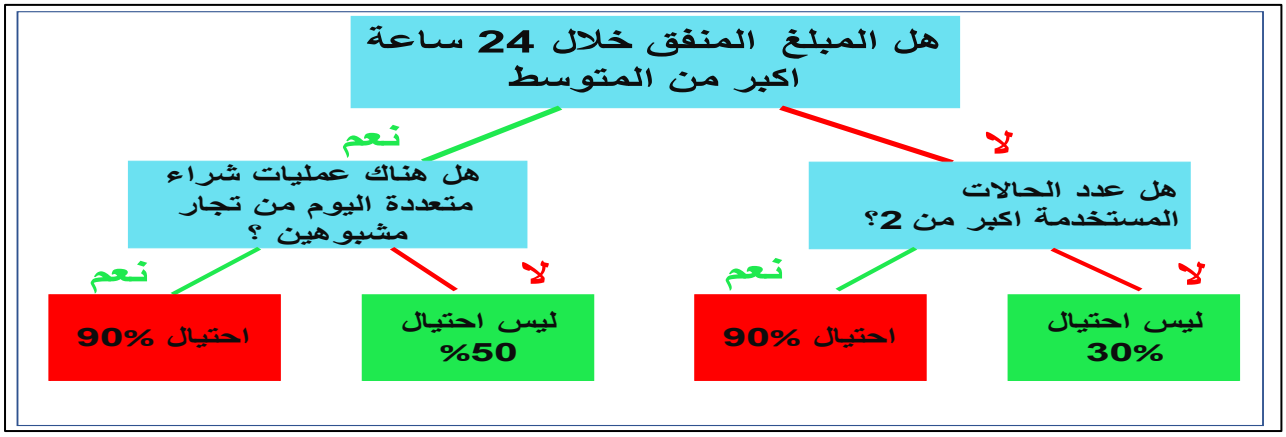
- **خوارزمية شجرة القرار(Decision Tree)(DT):** هي خوارزمية تستخدم في كل من التصنيف والانحدار، وتبنى على شكل هيكل شجري يتكون من عقد تمثل خصائص البيانات، وفروع تمثل قواعد اتخاد القرار، وعقد

[88] PRATYUSH SHARMA, ET AL, MACHINE LERNING MODEL FOR CREDIT CARD FRUD DETECTION -A COMPARATIVE ANALYSIS, THE INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY, VOL 18, NO 6,11/2021, P793

[89] XIN ZHANG, ET AL, A MACHINE LEARNING MODEL THE PREDICTION OF ATHLETE ENGAGEMENT BASED ON COHESION, PASSION AND MENTAL TOUGHNESS, VOL 15, N 3220,2025, P6

طرفية تمثل النتائج النهائية، وتوفر هده الشجرة طريقة رسومية لا تخاد القرارات بناءا على مجموعة من الشروط، حيث يتم الوصول الى النتيجة النهائية، عبر سلسلة من القواعد المنطقية المتتابعة.[90]

الشكل رقم 01 -10: الية عمل خوارزمية شجرة القرار



المصدر من اعداد الطالبة بالاعتماد على:

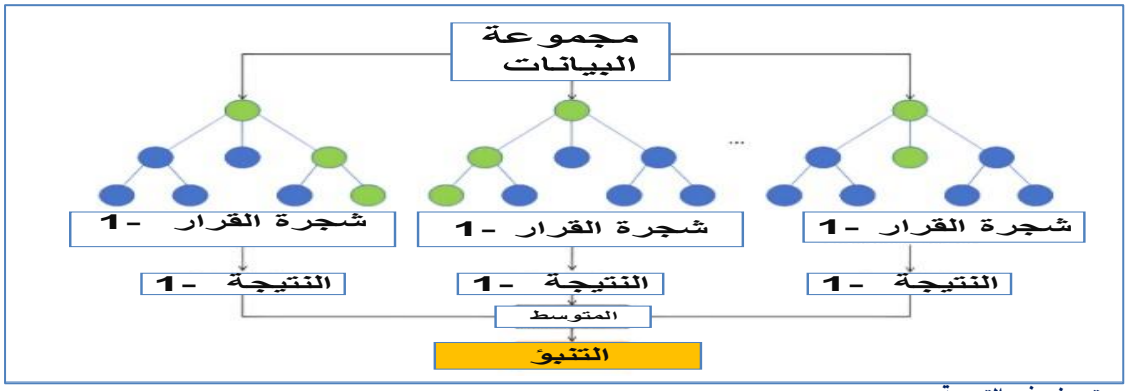
CHIE IKEDA, A NEW FEATURE ENGINEERING FRAMEWORK FOR FINANCIAL CYBER FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING, PHD DISSERTATION, SCHOOL OF COMPUTING AND DIGITAL MEDIA, LONDON METROPOLITAN UNIVERSITY, 9/2022، p39

- **خوارزمية الغابة العشوائية (Random Forest)(RF)**: تعتمد على هيكلية شجرية لاتخاذ القرارات بناءا على مدخلات الافراد، تتميز بسهولة ادراكها حيث لا تتطلب من المستخدم تعمقا في الرياضيات والاحصاء، كما انها تختصر الجهد بفضل بساطة اعداد البيانات، كما تمتاز بقدرة فائقة على معالجة البيانات الضخمة والسمات المعقدة في ان واحد، سواءا كانت الروابط بينها خطية او غير خطية، وذلك دون الحاجة لفرضيات مسبقة، مما يسرع من ظهور النتائج الفعالة وتعتمد في الية عملها على توزيع البيانات وتجميع الميزات المتشابهة ضمن عقد برمجية، تتفرع تدريجيا وفق شروط محددة حتى تكتمل العقد الفرعية التي تحتوي على الخصائص النهائية، وما يمنحها التميز عن بقية خوارزميات التعلم الموجه التصنيفي هو قدرتها على استخراج نتائج فعالة وسريعة عبر نظام التصويت الأغلبية، بالإضافة الى براعتها في معالجة البيانات الغير متوازنة وتقليل أخطاء الافراط في التكيف وهدا ما يزيد من دقتها[91]

[90] PALAK GUPTA, ET AL,UNBALANCED CREDIT CARD FRAUD DETECTION DATA :A MACHINE LEARNING -ORIENTED COMPARATIVE STUDY OF BALANCIG TECHNIQUES,PROCEDIA COMPUTER SCIENCE ,VOL 218,2023,P 2578

[91] فراحي فضيلة، **نموذج تعلم الي لكشف الاحتيال في بطاقة الائتمان – تطبيق عملي على منصة تفاعلية**، مرجع سابق، ص 511

الشكل رقم 01 -11 : الية عمل خوارزمية الغابة العشوائية



المصدر، بتصرف في الترجمة:

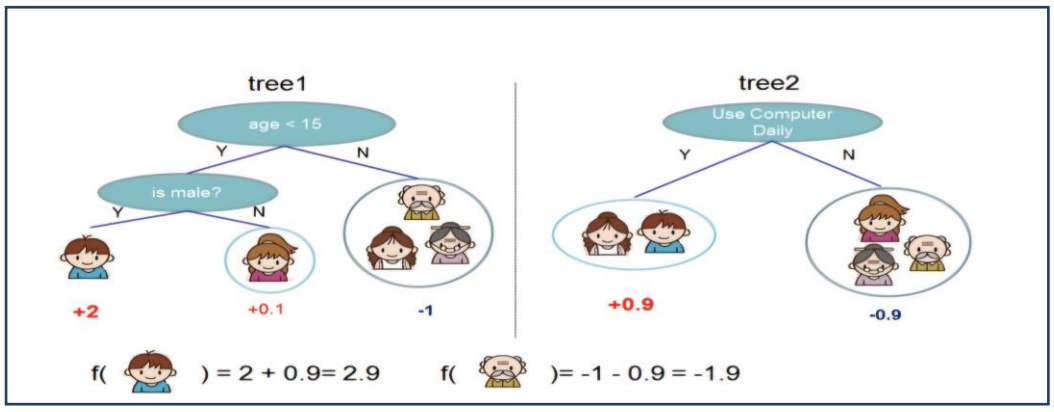
XIN ZHANG, ET AL, A MACHINE LEARNING MODEL THE PREDICTION OF ATHLETE ENGAGEMENT BASED ON COHESION, PASSION AND MENTAL TOUGHNESS, OP.CIT, P12

1-3- خوارزميات التعزيز:

- **خوارزمية (Gradient Boosting)(GB):** هو أسلوب من أساليب التعلم التجميعي، يعتمد على بناء نماذج بشكل متسلسل، حيث يتم تدريب كل نموذج جديد بهدف تصحيح الأخطاء التي ارتكبها النموذج السابق، ويتم ذلك من خلال تقليل قيمة الخطأ أو البواقي تدريجيا باستخدام الانحدار التدريجي، مما يسمح بتحسين دقة النموذج النهائي عبر مراحل متتابعة من التعلم.
- **خوارزمية (XGBoost):** هي خوارزمية متقدمة وفعالة وتعتبر أسلوب من أساليب النماذج التجميعية يعتمد على بناء نماذج تعلم الة بشكل متسلسل، وهي تطبيق محسن وسريع لفكرة التعزيز التدريجي (Gradient Boosting Machines) تعتمد على دمج مجموعة من أشجار القرار الضعيفة بشكل متسلسل، حيث يتم

تحسين كل شجرة لاحقة لتقليل أخطاء النماذج السابقة. كما تقوم بإرجاع احتمالات انتماء كل عينة الى الفئات المختلفة، ويتم اتخاذ القرار النهائي في التصنيف باستخدام عتبة احتمالية غالبا ما تكون 0،5.[92]

الشكل رقم 01-12 : الية عمل خوارزمية (XGBoost)



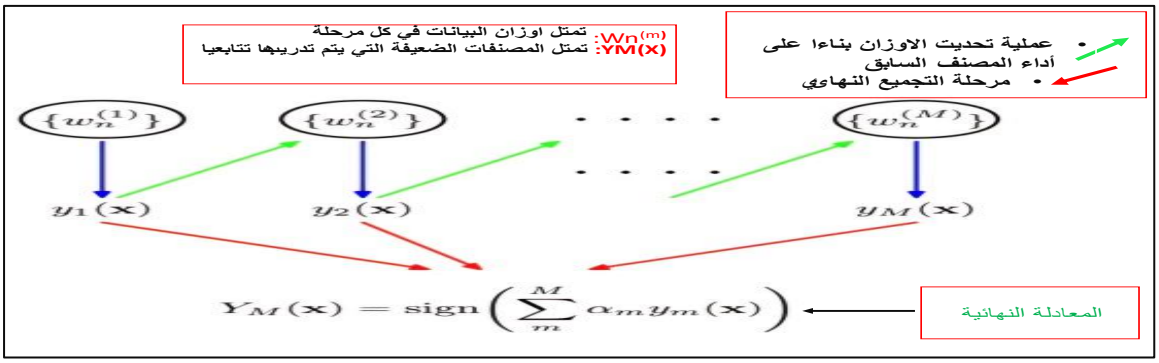
المصدر :

[92] RAMIRO DANIEL CAMINO,MACHINE LEARNING TECHNIQUES FOR SUSPICIOUS TRANSACTION DETECTION AND ANALYSIS ,PHD DISSERTION ,THE FACULTY OF SCIENCE ,TECHNOLOGY AND MEDICINE ,UNIVERSITE DU LUXEMBOURG EN INFORMATIQUE,10 /2020, P16

TIANQI CHEN ,CARLOS GUESTRIN ,XGBOOST : A SCALABLE TREE BOOSTING SYSTEM ,IN PROCEEDINGS CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING,2016،P786، https://doi.org/10.1145/2939672.2939785

- **خوارزمية (GBM)Gradient Boosting Machine)):** هي تقنية من تقنيات التعلم التجميعي التسلسلي تستخدم في مسائل التصنيف والانحدار، حيت تقوم ببناء نموذج قوي من خلال دمج مجموعة من النماذج الضعيفة، في الغالب أشجار القرار، بشكل تدريجي ومتسلسل، في كل خطوة، يتم تدريب نموذج جديد بهدف تصحيح أخطاء النماذج السابقة عبر تقليل دالة الخطأ، باستخدام الانحدار التدرجي، مما يؤدي الى تحسين دقة التنبؤ النهائية.[93]
- **خوارزمية (AdaBoost):** هي خوارزمية تعلم تجميعي تسلسلية تعتمد على مبدا التعزيز، حيت تقوم بدمج مجموعة من المتعلمين الضعفاء بشكل تدريجي للحصول على نموذج قوي. تعمل هده الخوارزمية على تدريب نفس المصنف بشكل متكرر، مع تعديل الاوزان في كل مرحلة، بحيث تعطي أهمية أكبر للعينات التي تم تصنيفها بشكل خاطئ في المراحل السابقة، واهمية اقل للعينات المصنفة بشكل صحيح، مما يؤدي في النهاية الى تحسين دقة التصنيف وبناء نموذج نهاءي اكتر قوة وفعالية.[94]

الشكل رقم 01 -13: الية عمل خوارزمية AdaBoost



المصدر :

CHRISTOPHER.M. BISHOP, PATTERN RECOGNITION AND MACHINE LEARNING, INFORMATIQUE SCIENCE AND STATISTICS, NEW YORK: SPRINGER -VERLAG ,2006,P658

- **خوارزمية (CatBoost):** هي خوارزمية تعتمد على تقنية التعلم التجميعي التسلسلي باستخدام التعزيز التدرجي، ويستخدم بشكل فعال في مهام التصنيف وكدا مسائل الترتيب. يعمل هدا النموذج على تحسين أداء أشجار القرار من خلال بناء نماذج متتالية تهدف الى تقليل الخطأ تدريجيا، مما يؤدي الى رفع دقة التنبؤ وتحسين الأداء العام للنموذج.[95]

[93] M.VALVAN, S. RITA, PREDIACTIVE -ANALYSIS -BASED MACHINE LERNING MODEL FOR FRAUD DETECTION WITH BOOSTING CLASSIFICATION, OP CIT, P 235 -236

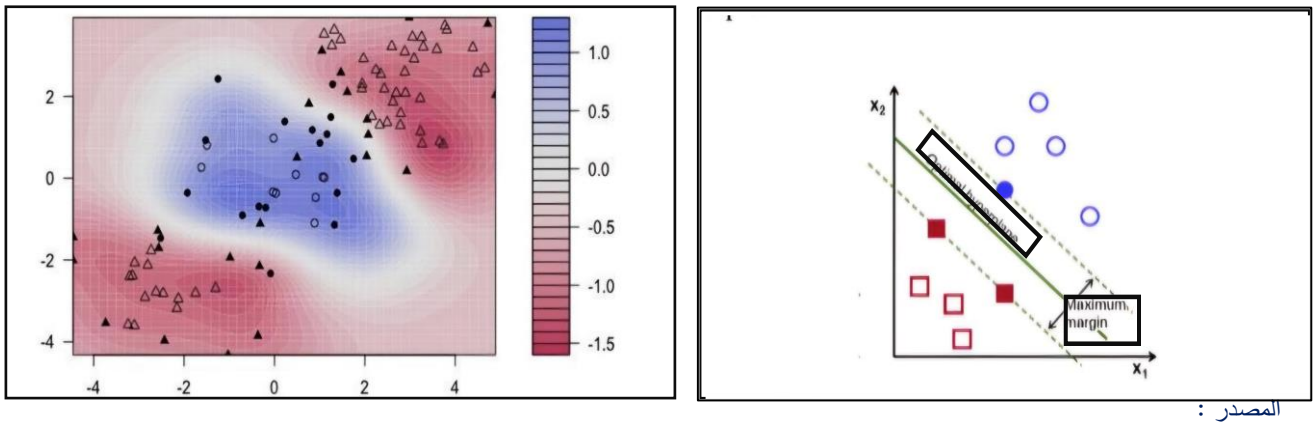
[94] A.C.Y. HONG, ET AL, PREDICTION OF US AIRLINE PASSENGER SATISFACTION USING MACHINE LEARNING ALGORITHMS, DATA ANALYTICS AND APPLIED MATHEMATICS (DAAM), VOL 4, N 1,2023,P 5

[95] KHALIFA ALSENAANI, FRAUD DETECTION IN FINANCIAL SERVICES USING MACHINE LEARNING, DEGREE OF MASTER OF SCIENCE IN PROFESSIONAL STUDIES: DATA ANALYTICS, DEPARTMENT OF GRADUATE PROGRAMS & RESEARCH, ROCHESTER INSTITUTE OF TECHNOLOGY, 2022, P 23 4

4.1 خوارزميات أخرى:

- **خوارزمية الة المتجهات الداعمة (Support Vector Machine)(SVM)** : هي خوارزمية تصنيف تعتمد على إيجاد مستوى فائق يفصل بين الفئات المختلفة في فضاء متعدد الابعاد، مع اختيار المستوى الذي يحقق الهامش الأقصى بين الفئات، وتستخدم بشكل فعال في التصنيف خاصة في الحالات التي يكون فيها عدد الخصائص كبيرا مقارنة بعدد العينات، مما يجعلها مناسبة لمعالجة البيانات عالية الابعاد .[96]

الشكل رقم 01 –14: الية عمل خوارزمية الة المتجهات الداعمة



المصدر :

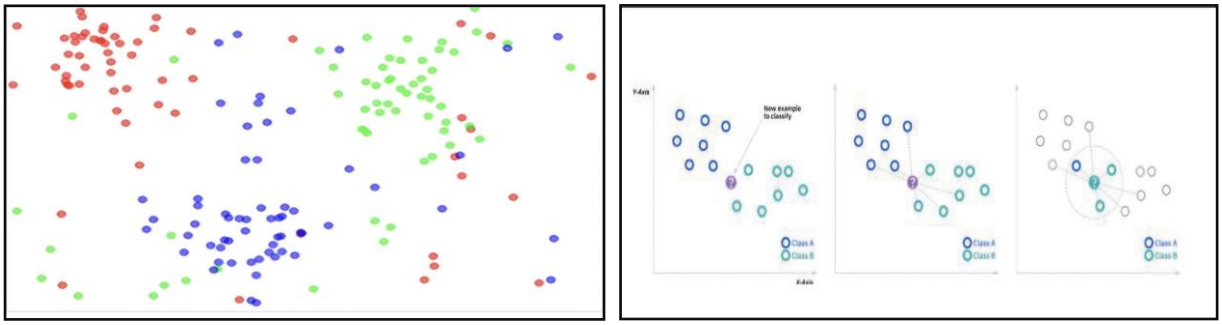
- . CHIE IKEDA, A NEW FEATURE ENGINEERING FRAMEWORK FOR FINANCIAL CYBER FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING, OP CIT, P 36
- SEBRI ABDERAHIM, COURS OF MACHINE LEARNING IA, UNIVERSITY OF SAVOIE -FRANCE, ،2022 - 2023،P13، FROM:https://cel.hal.science/hal-03906387

- **خوارزمية الجيران الأقرب (K−Nearest Neighbors)(KNN)**: هي خوارزمية من خوارزميات التعلم الخاضع للإشراف، تستخدم في مهام التصنيف والانحدار، حيث تعتمد على مبدا قياس المسافة والتشابه بين البيانات لتحديد الفئة المناسبة للعينة الجديدة بناءا على أقرب الجيران لها. تستخدم بشكل واسع في كشف الاحتيال اذ تساعد في تحسين دقة الكشف وتقليل الإنذارات الكاذبة من خلال تحليل ترابط المعاملات وتحديد الأنماط المشابهة. رغم انها قد تتأثر بزيادة حجم البيانات واستهلاك الذاكرة. [97]

الشكل رقم 01 -15 : الية عمل خوارزمية الجيران الأقرب

[96] ISRAT JAHAN, ET AL, COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR SENTIMENT CLASSIFICATION IN SOCIAL MEDIA TEXT, WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS, VOL 23, N3, P 2846

[97] REJWAN BIN SULAIMAN, ET AL, REVIEW OF MACHINE LEARNING APPROACH ON CREDIT CARD FRAUD DETECTION, HUMAN -CENTRIC INTELLIGENT SYSTEMS, VOL 2 , 5/2022,P 59



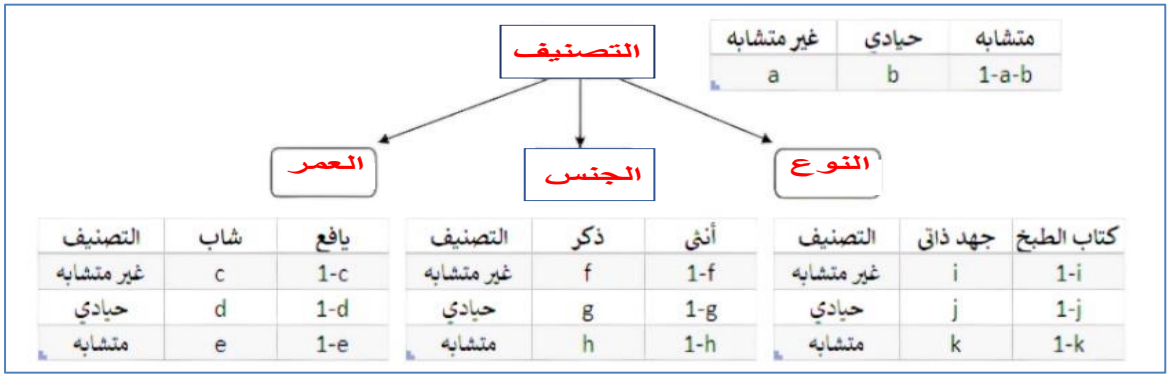
المصدر :

. SEBRI ABDERAHIM, COURS OF MACHINE LEARNING IA, OP CIT, P

. AMER F.A.H. ALNUAIMI, ET AL, AN OVERVIEW OF MACHINE LEARNING CLSSIFICATION TECHNIQUES, OP CIT, P14

- **خوارزمية ساذج بايز (Naïve Bayes):** هي خوارزمية تصنيف تعتمد على مبدا الاحتمالات، وتستخدم في الحالات التي تكون فيها الخصائص مستمرة ويفترض انها تتبع التوزيع الطبيعي، تقوم هده الخوارزمية بحساب احتمالية انتماء العينة الى فئة معينة بافتراض استقلالية الخصائص عند إعطاء الفئة، وتتميز ببساطتها وسرعتها في التنفيذ، الا ان اداءها قد يتأثر، إذا لم تتحقق الافتراضات الإحصائية الخاصة بها.[98]

الشكل رقم 01 –16: الية عمل خوارزمية ساذج بايز



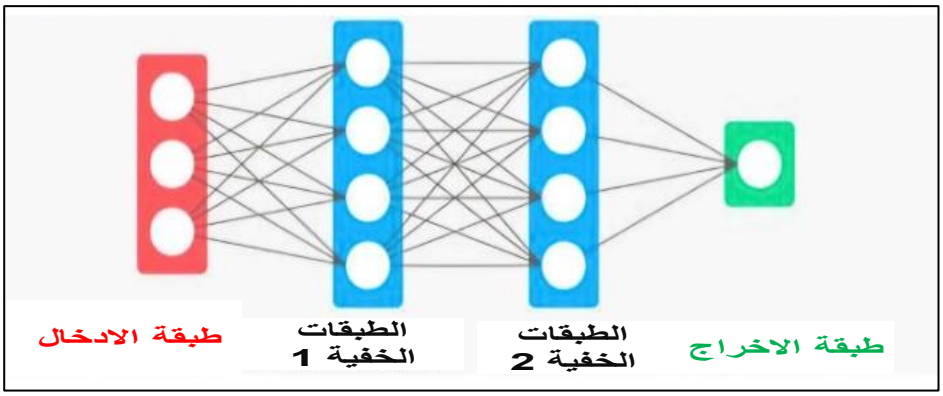
المصدر :لمى عدنان عوكل، دور استخدام خوارزميات الذكاء الصنعي في عمليات ضبط الجودة دراسة حالة، مصنع الميسور للصناعات البلاستكية، سوريا، ريف دمشق، مرجع سابق، ص 38

- **خوارزمية الشبكة العصبية الاصطناعية (Artificial Neural Network)(ANN):** هي احدى تقنيات التعلم الالي القوية التي تهدف الى محاكاة طريقة عمل الجهاز العصبي البشري، حيت تتكون من مجموعة من الوحدات الحسابية تسمى عصبونات، مترابطة فيما بينها عبر اوزان تمتل قوة الاتصال بينها، تعتمد هده الشبكات على معالجة المعلومات عبر طبقات متعددة، تشمل طبقة الادخال وطبقات خفية وطبقة الإخراج، حيت يتم تعلم

98 V.S.RAJ KUMAR, T. KUMARESAN, A COMPARATIVE STUDY ON MACHINE LEARNING APPROACHES FOR SENTIMENT ANALYSIS, INTERNATIONAL RESEARCH JOURNAL ON ADVANCED ENGINEERING HUB (IRJAEH), VOL 2, N 2,2/2024, P 173 -174

الأنماط من البيانات، كما تتميز بقدرتها العالية على معالجة المشـــكلات المعقدة في مجالات متعددة متل التصنيف، معالجة الصور، الترجمة الالية.[99]

الشكل رقم 01 -17: معمارية الشبكة العصبية الاصطناعية



المصدر بتصرف في الترجمة :

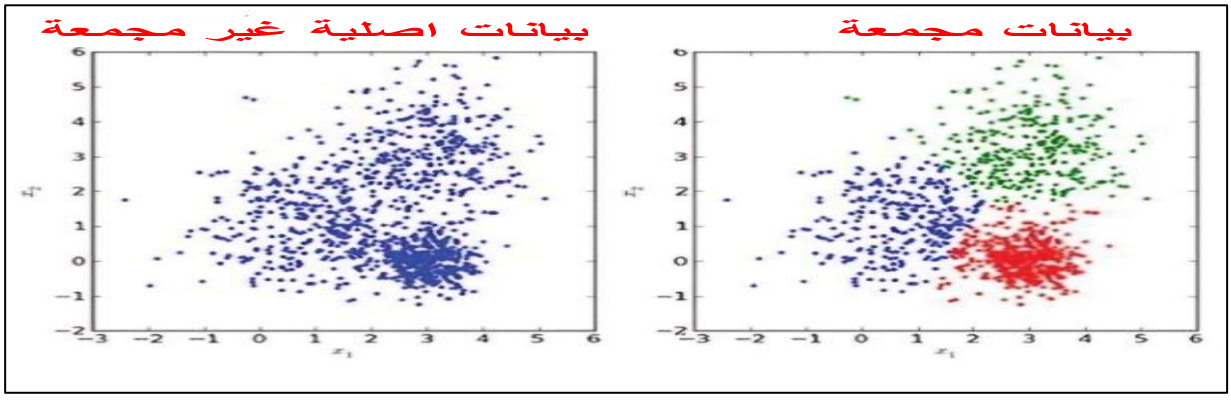
MATTHEW N.O. SADIKU, ET AL, MACHINE LEARNING :AN OVERVIEW,OP.CIT,P 1108

2- خوارزميات التعلم الغير خاضع للإشراف:

2-1- خوارزميات التجميع:

- **خوارزمية (k-Means):** تســـتخدم في مهام تجميع البيانات من خلال تقســـيم مجموعة من النقاط الى (K) مجموعات، بحيث تكون كل نقطة اكتر تشـــابها مع النقاط داخل نفس المجموعة مقارنة بالنقاط في المجموعات الأخرى، وذلك في الحالات التي لا تتوفر بيانات معنونة، مما يجعلها مناسـبة لا كتشـاف الأنماط والبنى المخفية داخل البيانات.[100]

الشكل رقم 01 -18: الية عمل خوارزمية (k-Means)



المصـدر: لمى عدنان عوكل، دور اسـتخدام خوارزميات الذكاء الصـنعي في عمليات ضـبط الجودة، دراسـة حالة - مصـنع الميسـور للصناعات البلاستكية -سوريا- ريف دمشق، مرجع سابق، ص 40

[99] SHAHNAWAZ KHAN, ET AL, DEVELOPING A CREDIT CARD FRAUD DETECTION MODEL USING MACHINE LEARNING APPROACHES, INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, VOL 13, N 3, 2022, P414

[100] ALEX SMOLA, S.V.N. VISHWANATHAN , INTRODUCTION TO MACHINE LEARNING, CAMBRIDGE UNIVERSITY PRESS,2008,P36

- **خوارزمية التجميع الهرمي (Hierarchical clustering)** :تعد أحد أســـاليب تحليل التجمعات التي تهدف الى ترتيب البيانات الغير مصنفة في شكل مجموعات مرتبة هرميا بحيث يتم تجميع العناصر المتشابهة تدريجيا بهدف الكشـف عن البنية الداخلية للبيانات والعلاقات فيما بينها، غير ان جودة هدا الأسـلوب تتأثر بقدرته المحدودة على تعديل القرارات بعد تنفيذها. حيت لا يمكن التراجع عن عمليات الدمج او التقســـيم او إعادة توزيع العناصـــر بين المجموعات، ممايجعل القرارات الغير مناسبة في المراحل المبكرة تؤدي الى انتاج مجموعات ذات جودة منخفضـة ولدلك يقترح دائما بتحســـين هده الطريقة من خلال دمجها مع تقنيات أخرى تعتمد على التجميع متعدد المراحل، بهدف تجاوز القيود الموجود في هذا الأسلوب.[101]
- **خوارزمية نموذج الخليط الغاوسـي (Gaussian Mixture Model):** هي نموذج يسـتخدم لتمثيل البيانات على انها مجموعة من الملاحظات متعددة الابعاد، بافتراض ان كل ملاحظة تتولد من أحد توزيعين طبيعيين مختلفين. ويتم تحديد انتماء كل ملاحظة الى هدين التوزيعين من خلال متغير كامن تناءى يأخذ القيم 0 أو1 باحتمال معين. فادا كانت القيمة 0 فان الملاحظة تتبع توزيعا طبيعيا بمعلمات خاصـــة، وإذا كانت القيمة 1 فإنها تتبع توزيعا طبيعيا اخر بمعلمات مختلفة. وبذلك يتم وصف البيانات على انها خليط من توزيعين طبيعيين مختلفين.[102]
- **خوارزمية التجميع القائم على الكثافة (DBSCAN):** خوارزمية تســـتخدم في مهام التجميع من خلال تقســـيم البيانـات الى مجموعـات اعتمـادا. على كتـافـه النقـاط. حيت تقوم بتجميع النقـاط المتقاربـة مكـانيـا وفقا لمقيـاس المسافة، مع اعتمار النقاط الواقعة في مناطق منخفضة الكثافة قيما شاذة يتم عزلها عن المجموعات الرئيسية.[103]

1.2 خوارزميات كشف الشدود:

- **خوارزمية الغابة المعزولة (Isolation Forest)(IF):** هي احدى تقنيات كشـف الشـدود المبنية على أشـجار القرار، وتعمل على تحديد القيم الغير طبيعية بشكل مباشر بدلا من نموذجة البيانات العادية تعتمد هده الخوارزمية على عزل الملاحظات بشكل عشواءي عبر اختيار الخصـائص وقيم التقسيم، حيت تعتبر العينات التي يتم عزلها بسرعة او عبر مسارات قصيرة داخل مجموعة الأشجار على انها شذوذات، وذلك لأنها تكون اقل تكرارا وتختلف عن البيانات الطبيعية في فضاء الخصائص.[104]
- **خوارزمية عامل الشدود المحلي (Local outlier Factor)(LOF):** هي تقنية لاكتشاف الشدود تعتمد على قياس مدى انحراف نقطة عن جيرانها المحليين داخل مجموعة البيانات. تقوم هده الخوارزمية بحســـاب كثافة كل

[101] YOGITA RANI, HARISH ROHIL, A STUDY OF HIERARCHICAL CLUSTERING ALGORITM, INTERNATIONAL JOURNAL OF INFORMATION AND COMPUTATION TECHNOLOGY, VOL 3, N11,2013, P1227

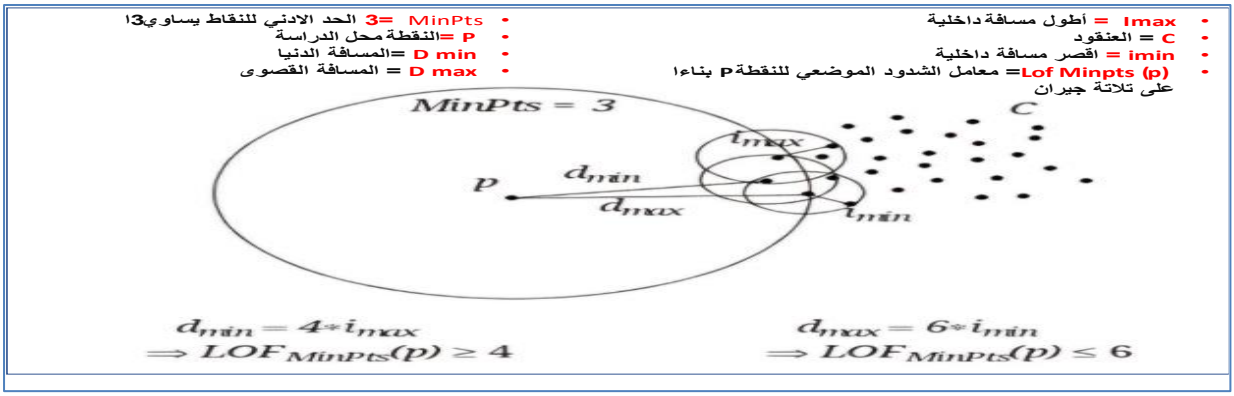
[102] XUETONG LI, ET AL, GAUSSIAN MIXTURE MODELS WITH RARE EVENTS, JOURNAL OF MACHINE LEARNING RESEARCH, VOL 25, 1245 ,2024, P 4 -5

[103] سامية بوضياف، فيصل بهلولي، **استخدام الذكاء الاصطناعي لدراسة علاقة أسعار النفط، الصرف**، الذهب، بالتضخم والتنبؤ به في الفترة الممتدة من جوان 2006، أفريل 2020، مرجع سبق دكره، ص 397

[104]VIKAS THAMMANNA GOWDA, CREDIT CARD FRAUD DETECTION USING SUPERVISED LEARNING, IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY, VOL 11, N1, P96

نقطة بيانات ومقارنتها بكتافه النقاط المجاورة لها، وبناءا على ذلك يتم تحديد ما إذا كانت هده النقطة شـاذة ام لا. وتعد هده الطريقة فعالة بشـكل خاص في الحالات التي لا تكون فيها كثافة البيانات متسـاوية عبر كامل مجموعة البيانات.[105]

الشكل رقم 01- 19: الية عمل خوارزمية عامل الخروج المحلي



المصدر بتصرف في عملية الترجمة :

MARKUS M. BREUNIG, ET AL, LOF: IDENTIFYING DENSITY -BASED LOCAL OUTLIERS, IN PROCEEDINGS OF THE 2000 ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGMENT OF DATA, DALLAS, TEXAS.USA,2000, P 97

- **خوارزمية احادي الفئه (one-class SVM):** هي طريقة تصـــنيف من فئة واحدة تعتمد على تحويل البيانات الى فضـــاء خصـــائص باســـتخدام دالة نواة (karnel)، تم اعتبار نقطة الأصـــل كفئة ثانية افتراضـــية، وبعد ذلك يتم إيجاد حد فاصـــل بأكبر هامش ممكن، يفصـــل معظم بيانات الفئة الواحدة عن الأصل، بحيث تعتبر النقاط القريبة من البيانات طبيعية والنقاط البعيدة خارج الفئة وشدود.[106]

2.2 خوارزميات تقليل الابعاد:

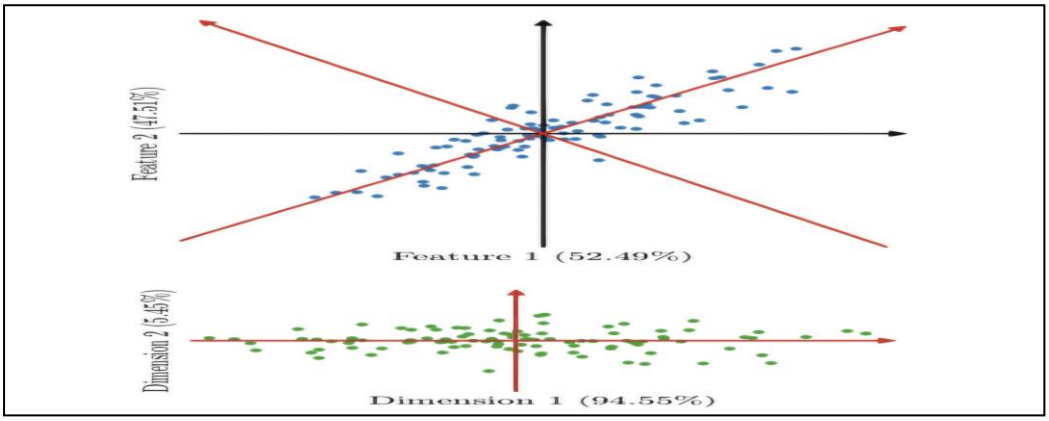
تحليل المكونات الرئيســـة (PCA)(Principal Component Analysis) : تقنية من تقنيات التعلم الغير خاضـع للإشـراف، تهدف الى تقليل ابعاد البيانات من مجموعة كبيرة الى مجموعة أصـغر، مع الحفاظ على معظم المعلومات التي تحتويها البيانات الاصـــلية. وتعتمد هده الخوارزمية على إزالة المتغيرات القدرة التفسيرية الضعيفة، والاحتفاظ بالعوامل الأكثر أهمية في تمثيل البيانات.[107]

[105] VIKAS THAMMANNA GOWDA, CREDIT CARD FRAUD DETECTION USING SUPERVISED LEARNING, OP CIT, P 95

[106] LARRY M. MANEVITZ, MALIK YOUSEF, ONE -CLASS SVMS FOR DOCUMENT CLASSIFICATION, JOURNAL OF MACHINE LEARNING RESARCH, VOL 2,12/2001, P142

[107] سامية بوضياف، فيصل بهلولي، **استخدام الذكاء الاصطناعي لدراسة علاقة أسعار النفط**، الصرف، الذهب، بالتضخم والتنبؤ به في الفترة الممتدة من جوان 2006 -أفريل 2020, مرجع سبق دكره، ص 396

الشكل رقم 01 –20: رسم بياني يوضح الية عمل تحليل المكونات الأساسية



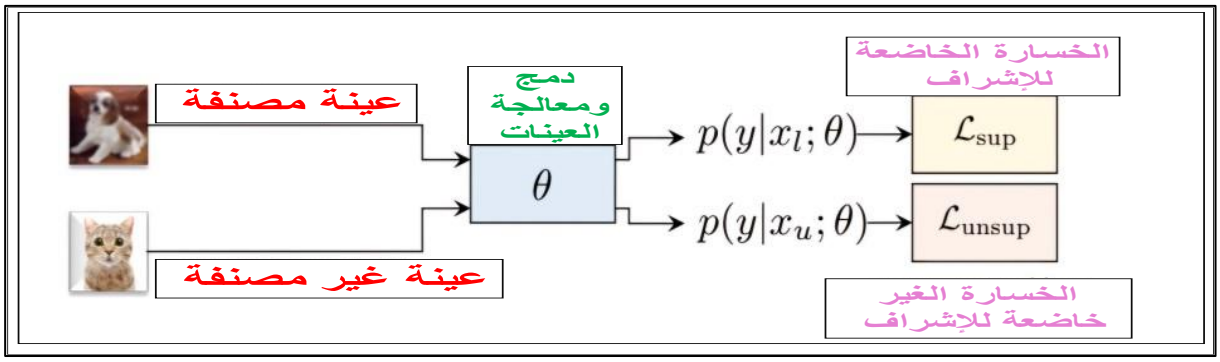
المصدر :

OLIVIER COLLIOT, MACHINE LEARNING FOR BRAIN DISORDERS, NEUROMETHODS, VOL 197, HUMAN PRESS, NEW YORK ,2023، P67

- **خوارزمية (t-SNE):** هي تقنية لتقليل الابعاد تستخدم خصوصا في تصور البيانات عالية الابعاد في فضاء تنائي او تلاتي الابعاد. تعتمد فكرتها على تحويل العلاقات بين النقاط في الفضـــاء الأصـــلي الى احتمالات تعبر عن التشـــابه، تم انشـــاء تمثيل منخفض الابعاد يحافظ على هده العلاقات قدر الإمكان، بحيث تبقى النقاط المتشـــابهة قريبة وغير المتشـــابهة بعيدة. ويتم ذلك عبر تقليل الفرق بين التوزيعين باســـتخدام تباعد كولباك –ليبر.[108]

3. خوارزميات التعلم الشبه خاضع للإشراف:

الشكل رقم 01 –21: الإطار العام لمبدأ عمل خوارزميات التعلم شبه خاضع للأشراف



المصدر, بتصرف في عملية الترجمة :

YANBEI CHEN, ET AL, SEMI -SUPERVISED AND UNSUPERVISED DEEP VISUAL LEARNING: A SURVEY, ARVIEX, ARVIEX :2208. 1 1296v1 [cs.CV]، P 2

[108]SANGWON JUNG, ET AL, A REVIEW OF T -SNE, IMAGE PROCESSING ON LINE, VOL 14,2024, P 251 - 252

- **خوارزمية التدريب الذاتي (Self-Training)** : يعتمد على استراتيجية تسمى الاسناد الافتراضي للتسميات، حيت تبدا الخوارزمية بتدريب مصنف على البيانات الموسومة تم يقوم هدا المصنف بإستاد تسميات افتراضية للبيانات الغير موسومة اعتمادا على تنبؤاته، بعد دلك تضاف العينات التي تم تصنيفها افتراضيا الى مجموعة التدريب ويتم إعادة تدريب النموذج من جديد، فتتكرر هده العملية بشـــكل دوري، حيت يتم تحديت النموذج وإعادة استخدامه لتوسيع مجموعة البيانات الموسومة تدريجيا، الى ان يتم استنفاد البيانات الغير موسومة أو عدم القدرة على إضافة تسميات جديدة غير موثوقة.[109]
- **خوارزمية نشر التسميات (Label Propagation)**: هي خوارزمية لاكتشاف العناقيد في الشبكات تعتمد على انتشـــار المعلومات داخلها. في البداية تمنح كل عقدة في الشـــبكة تســـمية فريدة، تم يتم تطبيق عملية تكرارية تقوم فيها كل عقدة بتحديث تســـميتها الى الأكثر تكرارا بين جيرانها. في حالة وجود اكتر من اختيار ممكن يتم كسر التعادل بشكل عشواءي. تستمر العملية الى غاية الوصول الى حالة استقرار لا تتغير فيها التسميات حيت تحدد العناقيد على انها مجموعات من العقد تشترك في نفس التسمية النهائية.[110]
- **خوارزمية نشر التسميات بأسلوب تدريجي (Label spreading)**: هي خوارزمية تعتمد على انشاء رسم بياني من البيانات، حيت تمثل العقد نقاط البيانات وتمتل الروابط درجة التشـابه بينها. تعمل الخوارزمية على نشـر معلومات التصـنيف من مجموعة صـغيرة من النقاط المصـنفة يدويا الى بقية النقاط الغير مصـنفة في الرسـم البياني. يتم التحكم في شـدة الانتشـار بواسـطة معاملات داخلية تحدد مدى انتشـار المعلومات عبر الرسم البياني، مع افتراض ان النقاط المتقاربة في فضاء الخصائص لها تسميات متشابهة.[111]
- **خوارزمية الة المتجهات الداعمة شـبة خاضـعة للإشـراف (Semi-Supervised SVM)**: تعد من اهم طرق التعلم شبه خاضـع للإشـراف وتهدف الى إيجاد فاصـل تصـنيفي يقع في مناطق منخفضـة الكثافة من البيانات ودلك من خلال تعظيم الهامش بالاعتماد على كل من البيانات المعلمة والبيانات الغير معلمة.[112]

4. خوارزميات التعلم المعزز

[109] MASSIH -REZA AMINI, ET AL, SELF -TRAINING: A SURVEY, NEUROCOMPUTING, VOL 616, N 128904,2025, P3

[110] GENNARO CORDASCO, LUISA GARGANO, COMMUNITY DETECTION VIA SEMI -SYNCHRONOUS LABEL PROPAGATION ALGORITHMS, IN 2010 IEEE INTERNATIONAL WORKSHOP ON BUSSINESS APPLICATION OF SOCIAL NETWORK ANALYSIS,2011, P2

[111] JONATHAN KLESS, ET AL, PROBABILISTIC LABEL SPREADING: EFFICIENT AND CONSISTENT ESTIMATION OF SOFT LABELS WITH EPISTEMIC UNCERTAINTY ON GRAPHS, ARIVEX PREPRINT: 2602.04574 ,2026, p2 -3

[112] BIN GU, ET AL, NEW INCREMENTAL LEARNING ALGORITHM FOR SEMI -SUPERVISED SUPPORT VECTOR MACHINE, KDD 2018, LONDON ,8 /2018, p1475

الشكل رقم 01 –22: مبدا عمل خوارزميات التعلم المعزز



المصدر: محمد سالم المصراتي، الذكاء الاصطناعي وتعلم الالة: الجزء الأول مفاهيم تقنية أساسية وتحديات أخلاقية ومجتمعية، مجلة البحوث التقنية، المجلد 1، العدد 1، 2023، ص 10

- **(Q-Learning)**: خوارزمية تقوم على التعلم خارج السياسة، حيث يتم فصل التعليم عن التنفيذ، أي ان النظام يتعلم كيف يختار افضل قرار دون ان يتأثر مباشرة بالفعل الذي قام به سابقا، تعتمد على تحديث قيمة تسمى (Q-value) لكل حالة وفعل، وذلك باستخدام المكافاة والحالة التي يصل اليها النظام بعد كل خطوة. يتم تكرار هذه العملية عدة مرات حتى تستقر القيم داخل جدول خاص يسمى (Q-table) والذي يستخدم لاحقا لاتخاذ القرارات المناسبة هده الخوارزمية فعالة وبسيطة لكنها تواجه صعوبة عندما يكون مساحات الحالات والافعال كبيرا لأنها تحتاج الى ذاكرة كبيرة وتجارب كثيرة.
- **(Deep Q Learning)(DQl)**: هي تطوير لخوارزمية (Q-Learning) حيث يتم استخدام شبكة عصبية (CNN) بدلا من تخزين كل القيم في جدول، خاصة عندما يكون عدد الحالات كبيرا، تعتمد هده الخوارزمية على فكرتين أساسيتين الأولى هي تخزين التجارب السابقة واختيارها بشكل عشواءي اثناء التعلم لتقليل الترابط بينها، والثانية هي استخدام شبكة منفصلة لحساب القيم المرجعية بهدف جعل التعلم اكتر استقرارا. هدا الأسلوب يساعد في تحسين الأداء لكنه قد يحتاج الى ذاكرة أكبر ويؤثر على سرعة التعلم.[113]
- **(SARSA)**: هي خوارزمية تقوم على التعلم داخل السياسة حيث تعتمد على التعلم الزمني (TD)، حيث تستخدم سياسة (ابسيلون جريدي) في كل من التعلم واتخاد القرار. تقوم هده الخوارزمية بتقدير دالة القيمة (Q) اعتمادا على معادلة بيلمان، ويتم تحديتها باستخدام المكافاة المباشرة والحالة التالية ،بالإضافة الى الفعل الذي يتم اختياره فعليا في تلك الحالة يعتمد التحديث على انتقال واحد فقط، حيث يتم تحسين القيم تدريجيا بالاعتماد على تقديرات سابقة، مما يقلل التعقيد الحسابي، وعلى عكس خوارزمية (Q-Learning) التي تعتمد على افضل فعل ممكن، فان خوارزمية (SARSA) تعتمد على الفعل الحقيقي المختار، لذلك فهي تتقارب

[113] BEAKCHEOL JANG,ET AL,Q-LEARNING ALGORITHMS: A COMPREHENSIVE CLASSIFICATION AND APPLICATIONS,IEEE ACCESS,VOL7,2019 ,P133657,DOI : 10.1109/access.2019.2941229

نحو سياسة جيدة قريبة من المثلى، ويمكنها الوصول الى السياسة المثلى عند تقليل احتمال الاستكشاف تدريجيا مع الزمن.[114]

- **(Policy Gradient):** هي خوارزمية تقوم عل التعلم داخل السياسة، وتمثل بديلا للطرق المعتمدة على دوال القيمة في التعلم المعزز مثل: (Q-Learning) و(SARSA)، اللدان يعتمدان على تعلم دوال قيمة تتقارب نحو القيمة المثلى والتي من خلالها يتم استنتاج السياسة لاحقا، في المقابل تقوم هده الخوارزمية على التعلم المباشر لسياسة معلمة، حيت يتم تحسينها عبر زيادة احتمال اختيار الأفعال التي تؤدي الى عوائد تدريجيا الى غاية الوصول الى سياسة متلى او تقريبية. ويتم هدا التعلم من خلال تحديت معاملات السياسة باستخدام أساليب تعتمد على التدرج في اتجاه تعظيم دالة الأداء.[115]
- **خوارزمية الممثل – الناقد (Actor-Critic):** تقوم على الجمع بين مزايا طرق الممثل فقط وطرق الناقد فقط، حيت تتكون من جزئين اساسين: جزء يتولى تعلم دالة القيمة بالاعتماد على التقريب والمحاكاة، وجزء يقوم بتحديث معاملات السياسة في اتجاه تحسين الأداء. تعتمد على استخدام تقدير دالة القيمة بتوجيه تحسين السياسة بشكل تدريجي. وتصنف ضمن الخوارزميات المعتمدة على التدرج، مما يسمح لها بتحقيق خصائص أفضل مقارنة بالناقد فقط، كما تساعد على تسريع التقارب وتقليل التباين مقارنة بطرق الممثل فقط. كما انها تقوم على فكرة ان تعلم دالة القيمة لا يتطلب حسابها بدقة كاملة، بل يكفي تقريبها داخل فضاء منخفض الابعاد مرتبط بتمثيل السياسة.[116]

5. خوارزميات التعلم العميق:

- **الشبكات العصبية العميقة (Deep Neural Networks)**(DNN): خوارزمية مستقاة من تركيب الدماغ البشري تتكون من طبقات متعددة من العقد المترابطة، تتمثل قوتها في قدرتها على تحليل كميات هائلة من البيانات واكتشاف الأنماط والعلاقات الغير واضحة،[117] حيت تعمل وفقًا لآلية علمية مستوحاة من الخلايا العصبية في العلوم البيولوجية أي طريقة نقل الإشارة بين العصبونات وتوظف هده الخوارزمية في دراسة

---

[114] HAO JIANG, ET AL, AN IMPROVED SARSA (λ) REINFORCEMENT LEARNING ALGORITHM FOR WIRELESS COMMUNICATION SYSTEMS, IEEE ACCESS, VOL7,2019, P115424, DOI: 10.1109/access.2019.2935255

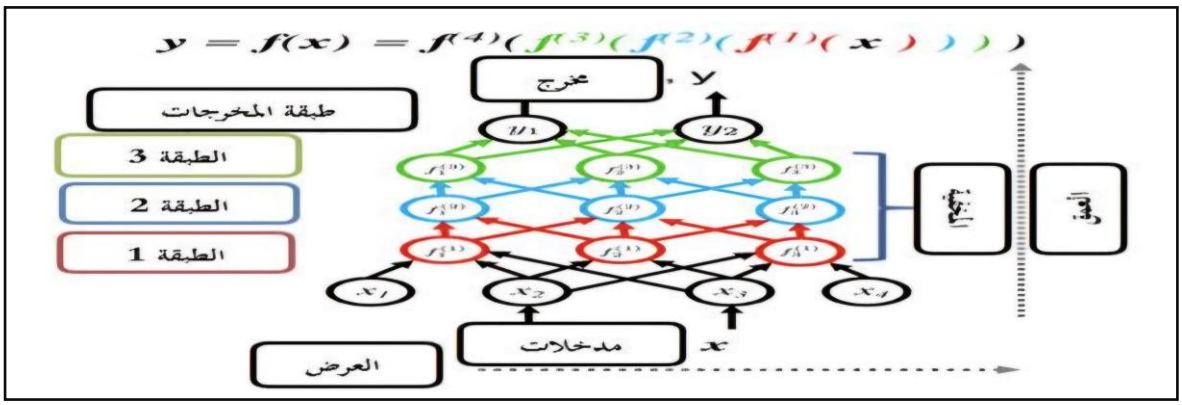
[115] MATTHIAS LEHMANN ,THE DEFINITIVE GUIDE TO POLICY GRADIENTS IN DEEP REINFORCEMENT LEARNING :THEORY ,ALGORITHMS AND IMPLEMENTATIONS ,ARIVEX PREPRINT ,ARIVEX: 2401.13662.,2024, P4 -5

[116] VIJAY R. KONDA,JOHN N. TSITSIKLIS ,ACTOR -CRITIC ALGORITHMS,ADVANCE IN NEURAL INFORMATION PROCESSING SYSTEMS, VOL 12, 1999,P 1008-1009

[117] ريم محمد محمود عبد المنعم واخرون، **أثر التنبؤ بالأرباح المستقبلية باستخدام خوارزميات تعلم الالة كإحدى تقنيات الذكاء الاصطناعي على تعزيز ثقة المستثمرين – دراسة تطبيقية**، مرجع سبق ذكره، ص 22

الجينات لاكتشاف الأمراض والتحقيق في الطفرات والظواهر الأخرى وقد صممت وطورت لتحسين الأداء في التصنيف والتنبؤ باي علاقات او أنماط مشبوهة.[118]

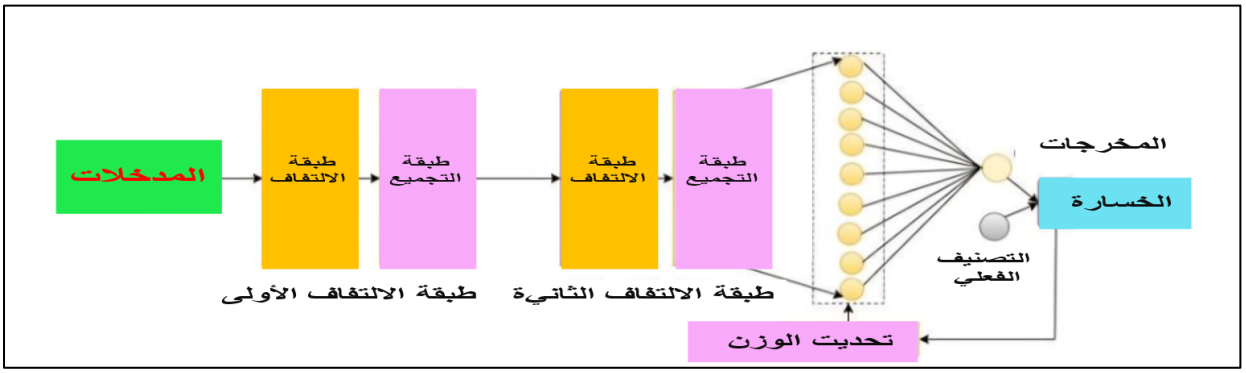
الشكل رقم 01-23: معمارية الشبكات العصبية العميقة



المصدر: زهواني مروة، تطبيقات نماذج الذكاء الاصطناعي للتنبؤ بمخاطر التعثر المالي في المؤسسة الاقتصادية- دراسة حالة-، مرجع سابق، ص 21

- **الشـــبكات العصـــبية الالتفافية (convolution Neural Networks)(CNN):** تعد نموذجا من نماذج التعلم العميق، صـممت خصـيصـا لاكتشـاف الأنماط والخصـائص داخل البيانات المرئية متل الصـور، من خلال عمليات الالتفاف لاسـتخراج خرائط الخصـائص، تم تقليل الابعاد تلقائيا عبر طبقات التجميع، وصـولا الى طبقات التصنيف التي تقوم بتحديد الفئات وانتاج احتمالاتها، مما يجعلها فعالة في مهام تصنيف الصور والتعرف على الاجسام.[119]

الشكل رقم 01 -24: معمارية الشبكات العصبية الالتفافية



المصدر, بتصرف في عملية الترجمة:

MOHAMMED NAJIM UDDIN, FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS, THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE

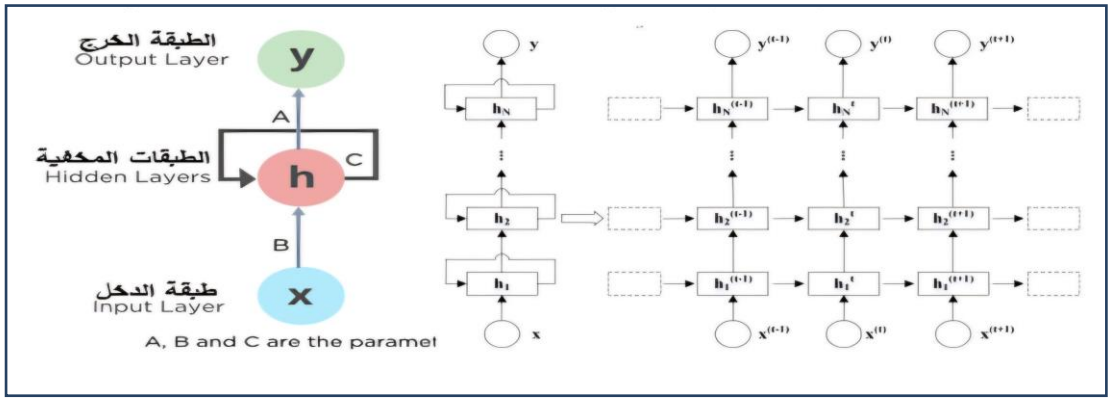
[118] BEKADDOUR FATIMA ZAHRA, STOCK PRICE CLASSIFICATION USING FINANCIAL INDICATORS FROM 10 -K REPORTS: A COMPARATIVE STUDY BETWEEN NEURAL NETWORKS (NN) AND LOGISTIC REGRESSION (LR), JOURNAL OF FINANCE, INVESTMENT AND SUSTAINABLE DEVELOPMENT, VOLUME :10, NEMBER :01, JUNE 2025, P 233-233

[119] CHIE IKEDA, NEW FEATURE ENGINEERING FRAMEWORK FOR FINANCIAL CYBER FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING, OP.CIT, P55 -56

DEGREE OF MASTER OF RESEARCH CENTRAL QUEENSLAND UNIVERSITY ,SCHOOL OF ENGINEERING AND TECHNOLOGY ,AUSTRALIA,، 2 /2024، p 46

- **الشبكات العصبية المتكررة (Recurrent Neural Networks:(RNN))**: هي نوع من الشبكات العصبية الاصطناعية المصممة لمعالجة البيانات المتسلسلة، حيت تعتمد على ربط المعلومات عبر الزمن من خلال استخدام الحالة السابقة مع المدخل الحالي، يتيح هدا البناء للشبكة القدرة على تعلم الأنماط، واستخراج العلاقات داخل البيانات متل: النصوص والصوت، إضافة الى إمكانية استخدامها في تحديد السلوكيات الغير طبيعية وكشف الاحتيال في البيانات المتتابعة. مما يجعلها مناسبة لمهام التحليل والتنبؤ في البيانات المتغيرة عبر الزمن.[120]

الشكل رقم 01-25: معمارية الشبكات العصبية المتكررة



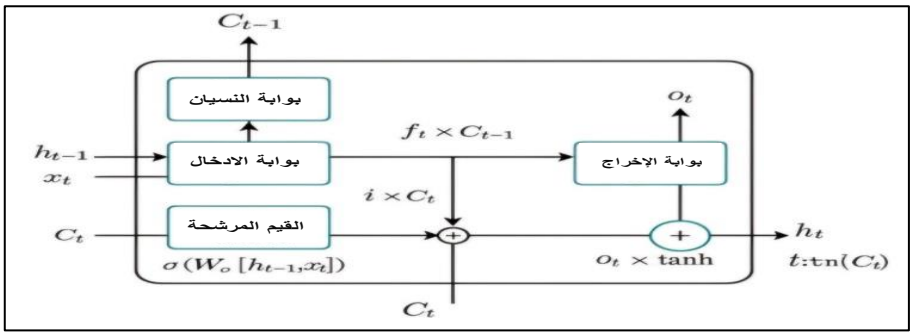
المصدر: زهواني مروة، تطبيقات نماذج الذكاء الاصطناعي للتنبؤ بمخاطر التعثر المالي في المؤسسة الاقتصادية –دراسة حالة، مرجع سابق، ص 23.

- **الذاكرة طويلة قصيرة المدى (Long short-term Memory)(LSTM)**: تعد نوعا متقدما من الشبكات العصبية المتكررة، صممت خصيصا لمعالجة البيانات التسلسلية من خلال التقاط الاعتماديات الزمنية طويلة المدى، وتمتاز بقدرتها على الاحتفاظ بالمعلومات لفترات زمنية طويلة، مما يسمح لها بنماذج العلاقات الزمنية المعقدة والتغلب على مشكلة تلاشي التدرج، وهو ما يجعلها فعالة في التطبيقات التي تتطلب فهم السلوك عبر الزمن متل كشف الاحتيال المالي.[121]

[120] ROBIN M. SCHMIDT ,RECURRENT NEURAL NETWORKS (RNNs):A GENTLE INTRODUCTION AND OVERVIEW,ARIVEX PREPRINT,ARIVEX : 1912. 05911v1 [cs. lg],11/2019, p1

[121] HONGFANG ZHOUA,ET AL , A DEEP LEARNING HYBRID RNN-LSTM MODEL FOR CREDIT CARD FRAUD DETECTION , GOOGLE SCHOLAR , 12/2025, p7,DOI:HTTPS://doi.org/10.21203/rs.3.rs-8327749/v1

الشكل رقم 01- 26 : معمارية الذاكرة طويلة قصيرة المدى

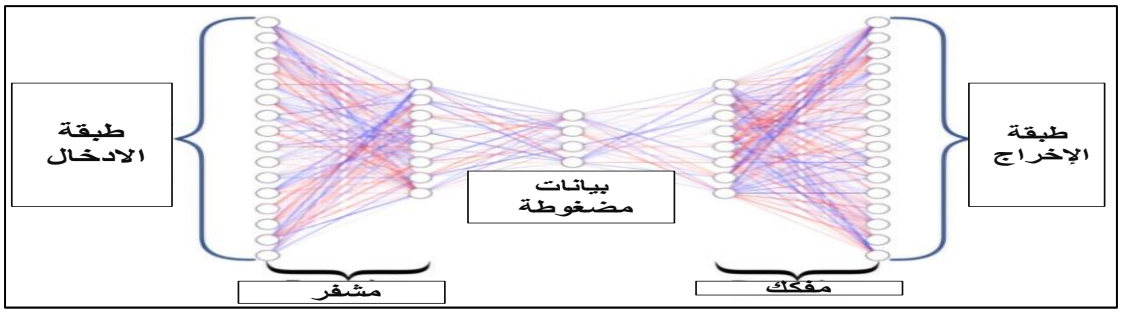


المصدر , بتصرف في الترجمة ,

HONGFANG ZHOUA,ET AL , A DEEP LEARNING HYBRID RNN-LSTM MODEL FOR CREDIT CARD FRAUD DETECTION ,IBID,p7

- **المرمز التلقائي (Autoencoders):** هي خوارزمية تعلم عميق غير خاضعة للإشراف تنتمي الى الشبكات العصبية الاصطناعية، صممت لتعلم تمثيل مضغوط للبيانات، من خلال ضغط المدخلات في طبقة كامنة، واستخراج اهم ميزاتها، تم إعادة بناء البيانات الاصلية انطلاقا من هدا التمثيل، ويهدف هذا النموذج الى تقليل الابعاد واكتشاف الخصائص الجوهرية للبيانات مع الحفاظ على أكبر قدر ممكن من المعلومات، مما يجعله فعالا في تحليل البيانات واستخراج الأنماط الخفية.[122]

الشكل رقم 01 -27: معمارية التشفير التلقائي



المصدر , بتصرف في الترجمة ,

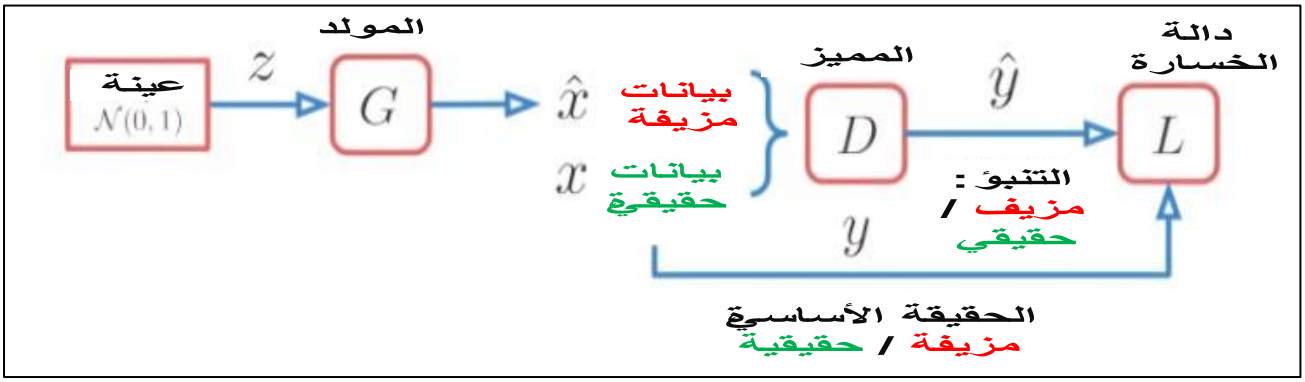
SAHID TUFAIL, HUGO RIGGS, ET Al, AVANCEMENTS AND CHALLENGES IN MACHINE LEARNING : A COMPREHENSIVE REVIEW OF MODELS, LIBRARIES, APPLICATIONS, AND ALGORITHMS, JOURNAL ELECTRONICS, VOL12, N8،4/2023،P20

- **الشبكات التوليدية التنافسية (Generative Adversarial Networks) (GAN):** هي أحد نماذج تعلم الالة المتقدمة، التي تعتمد على مبدا التنافس بين شبكتين عصبيتين، حيث تعمل الشبكة الأولى على توليد بيانات اصطناعية مشابهة للبيانات الحقيقية، بينما تعمل الشبكة الثانية على التمييز بين البيانات الحقيقية والبيانات المولدة، تستخدم في مجال كشف الاحتيال من خلال توليد امثله احتيالية افتراضية تساعد

• [122]CHIE IKEDA, A NEW FEATURE ENGINEERING FRAMEWORK FOR FINANCIAL CYBER FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING, OP CIT, P 51 -52

على تحسين قدرة أنظمة التعلم الالي على التعرف على مختلف أنماط الاحتيال، بما في ذلك الحالات النادرة والمعقدة[123]

الشكل رقم 01- 28: معمارية الشبكات التوليدية التنافسية



المصدر ،بتصرف في الترجمة :

RAMIRO DANIEL CAMINO, MACHINE LEARNING TECHNIQUES FOR SUSPICIOUS TRANSACTION DETECTION AND ANALYSIS, OP.CIT, 8/2020، P71

الفرع الثالث: معايير المقارنة بين خوارزميات تعلم الالة.

لاختيار انسب خوارزمية تعلم الة، يتم الاعتماد على مجموعة من المعايير بدل الاكتفاء بمعيار واحد لان الأداء يرتبط بطبيعة البيانات والمشكلة المطروحة ومن أبرز هده المعايير كما هي موضحة في الشكل التالي:

- **الدقة:** يعتبر أهم معيار من معاير المقارنة تشير الى قدرة النموذج على التنبؤ الصحيح بشأن بيانات جديدة غير مرئية لكنها وحدها لا تكفي لتحديد أفضل خوارزمية في جميع الحالات.
- **قابلية التفسير:** توضح مدى سهولة تفسير وفهم نتائج النموذج والعلاقات بين المتغيرات، اذ تكون بعض من الخوارزميات واضحة متل أشجار القرار بينما تكون الأخرى معقدة متل: الشبكات العصبية.
- **قابلية التوسع:** تعكس قدرة الخوارزمية على التعامل مع كميات كبيرة من البيانات دون انخفاض في الأداء.
- التعقيد: قد تكون بعض الخوارزميات اكتر تكلفة من ناحية القدرة الحسابية وتتطلب ذاكرة أكبر من غيرها مما يجعلها اقل عملية في تطبيقات معينة.
- **زمن التدريب:** تمثل الزمن اللازم لتدريب الخوارزمية خاصة مع البيانات الكبيرة وهو عامل مهم في كشف الاحتيال حيت يكون الوقت مكلف جدا حيت توجد خوارزميات سريعة تدريب متل: خوارزمية أقرب الجيران وتو جد من تتطلب وقتا كبير متل الشبكات العصبية.

[123] MOHAMED KAMEL ALDIN ISMAIL,HARNESSING AI FOR NEXT -GENERATION FINANCIAL FRAUD DETECTION :A DATA-DRIVEN REVOLUTION ,JOURNAL OF ECOHUMANISM,VOL 3,N 7,2024,P 817 - 818

- **المتانة:** تدل على قدرة الخوارزميات في الأداء الجيد في ظل وجود بيانات مبعثرة او غير كاملة، حيت يفضل استخدام الخوارزميات الأكثر متانة للتعامل مع متل هده البيانات.
- **التنظيم:** تدل على مساهمة الخوارزمية في الحد من مشكلة الافراط في التخصيص، مما يساعد على تحسين قدرة النموذج على التعميم مما يجعل لها الأفضلية في تطبيقات معينة.[124]

المطلب الثالث: دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني.

من اجل دراسة دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني قمنا بتقسيم هدا المطلب الى 5 فروع امتدت من ابراز دورها والية عملها في كشف الاحتيال المالي الالكتروني تم اهم التطورات التي شهدتها بالإضافة الى تميزها مقارنة مع الطرق التقليدية وإبراز أهميتها وأخيرا وصولا الى أهم التحديات التي تواجهها.

الفرع الأول: دور خوارزميات تعلم الالة كشف الاحتيال المالي الالكتروني

يعرف الكشف عن الاحتيال المالي الالكتروني بانه عملية تحديد مادا كانت المعاملة الجديدة المصرح بها تصنف ضمن معاملات الاحتيالية او المشروعة. ولا يقتصر دور نظام كشف الاحتيال على تحقيق دقة في التعرف على الحالات الاحتيالية فقط، بل ينبغي أيضا ان يكون اقتصاديا، بحيث لا تتجاوز تكلفة فحص المعاملات حجم الخسائر المحتملة. وقد تمت الإشارة الى ان فحص نسبة صغيرة من المعاملات يمكن ان يساهم في تقليل خسائر الاحتيال، رغم ما قد يصاحبه من ارتفاع في تكاليف الكشف.

في هدا السياق، تلعب خوارزميات تعلم الالة دورا مهما في دعم أنظمة الكشف عن الاحتيال خاصة وان حجم المعاملات المالية الضخم يجعل ن الصعب معالجته يدويا مما يستدعي الاعتماد عليها، حيت تستخدم مع قواعد الخبراء لإجراء مرحلة أولية من التصفية، مما يسمح بالتمييز بين المعاملات العادية والمشبوهة، مع إحالة الحالات ذات الخطورة المرتفعة الى المحققين فقط لمراجعتها.

ففي المرحلة الأولى تخضع المعاملات المالية الالكترونية، لعدد من الفحوصات الأساسية، متل التأكد من معرف صاحب البطاقة، وهل الرصيد كاف، تم يتم تقييمها بواسطة نموذج تنبؤي باستخدام الخبراء و خوارزميات تعلم الالة التي تمكن من اكتشاف الأنماط الاحتيالية والتنبؤ بها بالاعتماد على بيانات سابقة. وغالبا ما يكون هدا النموذج في شكل دالة بارا مترية تسمح بتقدير الاحتيال كون المعاملة احتيالية ام لا حيت يتخذ النظام قرارا اليا رفض او قبول او مراجعة حيت تتعلم الخوارزمية من اخطاءها ومن قرارات الخبراء لتصبح اكتر دقة في الفترات القادمة وهدا ما يسمى بالتغذية الرجعية.

تصنف تقنيات كشف الاحتيال المالي الالكتروني الى فئتين ويظهر بوضوح فيهما دور خوارزميات تعلم الالة:

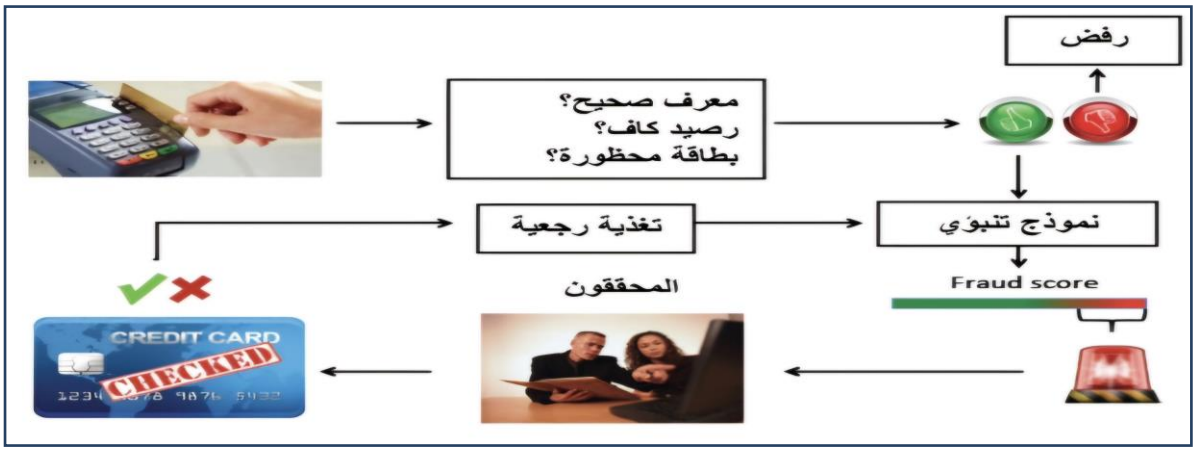
---

[124] علي بن الضب، **دور الذكاء الاصطناعي وتعلم الالة في تعزيز كشف الاحتيال على البطاقات الائتمانية**، صندوق النقد العربي، العدد 23، 2023، ص 34.

- **الفئة الأولى:** تشـمل تحليل الاحتيال حيت تعتمد على النماذج القائمة على البيانات المصـنفة مسـبقا، حيت يتم تدريب النماذج خوارزميات تعلم الالة باسـتخدام بيانات تاريخية مصـنفة الى معاملات احتيالية وأخرى مشـروعة، بهدف بناء نموذج قادر على التنبؤ بحالة المعاملات الجديدة، ومن بين امتله هده الخوارزميات الانحدار اللوجستي، أشـجار القرار، الشـبكات العصـبية، وهي فعالة في التعرف على الأنماط الاحتيال التي لاحظتها من قبل.
- **الفئة الثانية:** تشـمل دراسـة سـلوك المسـتخدم من خلال كشـف الشـدود والأنماط الغير طبيعية حيت تعتمد على النماذج القائمة على البيانات الغير مصنفة مسبقا، اد تعتبر المعاملة احتيالية ادا كانت مختلفة عن السلوك المعتاد لصـاحب الحسـاب، وفي هدا الإطار تسـتخدم خوارزميات تعلم الالة لبناء نموذج يمتل السـلوك الطبيعي لكل مستخدم ومن تم الكشف عن أي انحراف عنه وهو ما يعرف بكشف الشدود.

ورغم الأهمية الكبيرة لخوارزميات تعلم الالة، الا ان استخدامها يواجه بعض التحديات من بينها ضرورة تقليل الأخطاء التي تؤدي الى رفض معاملات مشروعة او حظر بطاقات اصلية، خاصـة وان نسـبة المعاملات الاحتيالية تبقى ضعيفة مقارنة بإجمالي المعاملات ونبرز كل ما قالناه من خلال الشكل الموالي.[125]

الشكل رقم 01 –29: رسم توضيحي لدور خوارزميات تعلم الالة (نموذج تنبؤي) في كشف الاحتيال المالي الالكتروني دراسة حالة بطاقة الائتمان



المصدر , بتصرف في الترجمة :

DAL POZZOLO,ADAPTIVE MACHINE LEARNING FOR CREDIT CARD FRAUD DETECTION ,A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR BHD DEGREE IN COMPUTER SCIENCE ,MACHINE LEARNING GROUP ,UNIVERSITE LIBRE DE BRUXELLES, 12 /2015، P5

الفرع الثاني: التطورات التي شهدتها الخوارزميات في مجال كشف الاحتيال المالي الالكتروني:

عززت التطورات الحديثة في التعلم الالي بشـكل كبير قدرات أنظمة خوارزميات تعلم الالة الكاشـفة للاحتيال وذلك من خلال:

[125] علي لؤي ياسـين، **اسـتخدام طرائق التعلم الالي لاكتشـاف الشـذوذ في مجموعة البيانات**، مذكرة ماجيسـتير في هندسـة البرمجيات ونظم المعلومات، كلية الهندسة المعلوماتية، جامعة البحت، سوريا، ص 6–7.

- **توظيف الشبكات العصبية العميقة:** ساهمت تقنيا التعلم العميق في نقلة نوعية عبر قدرتها العالية على معالجة البيانات الضخمة والغير منظمة. وتكمن قوتها في استنباط ملامح وانماط احتيالية دقيقة ومعقدة يصعب على الأنظمة الكلاسيكية رصدها.
- **تطوير خوارزميات كشف الشدود:** أدت الابتكارات في التعلم الغير خاضع للإشراف الى تطوير خوارزميات متقدمة لكشف الشدود، مما يجعلها مفيدة بشكل خاص في رصد الأساليب الاحتيالية الابتكارية التي لم تظهر من قبل.
- **تحليل المحتوى النصي:** يتم استثمار معالجة اللغات الطبيعية لفحص سياق المراسلات والبيانات النصية، مما يساعد في التنبؤ بمحاولات الخداع او الهندسة الاجتماعية من خلال فهم المعاني والدلالات وراء النصوص المرتبطة بالعمليات المالية.
- **التحليل عبر الرسوم البيانية الترابطية:** تركز هده التقنية في دراسة هيكلية العلاقات بين الحسابات والتعاملات. فهي لا تنظر الى المعاملة بشكل منفرد، بل تحلل شبكة الروابط الخفية، مما يسهل تفكيك مخططات الاحتيال الجماعية والمنظمة.
- **المعالجة في الوقت الفعلي:** اتاحت التطورات الحديثة إمكانية فحص التدفقات البيانية لحظة حدوتها. هده السرعة في المعالجة تمكن الأنظمة من اتخاد قرار استباقي بإيقاف المعاملة المشبوهة فورا. مما يقلل الاضرار المادية بشكل كير ويزيد من ثقة العملاء.[126]

الفرع الثالث: المقارنة بين الطرق التقليدية وتقنيات خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني:

تتجلى الفوارق الجوهرية بين أساليب كشف الاحتيال التقليدية وتقنيات تعلم الالة بوضوح في المنهجية المتبعة وكفاءة اداءها العام حيت يتصادم جمود الأنظمة التقليدية القائمة على القواعد المسبقة مع مرونة تقنيات تعلم الالة وقدراتها التحليلية الفائقة والمرنة وهوما نوضحه في الجدول التالي:

الجدول رقم 01 -15: المقارنة بين الطرق التقليدية خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني

أوجه المقارنة	طرق الكشف التقليدية	طرق الكشف باستخدام خوارزميات تعلم الالة
المنهجية	يعتمد كشف الاحتيال على معايير وانماط مسبقة مستخلصة من البيانات التاريخية والخبرات المتراكمة فمثلا تصنف المعاملات	تتفوق أنظمة تعلم الالة بقدرته الفائقة على تحليل البيانات الضخمة وكشف الأنماط المعقدة التي تعجز عنها الطرق التقليدية فهو لا يكتفي برصد الحالات الشاذة فقط بل يتعلم ويتكيف باستمرار من البيانات

[126] ANTHONY OWEN, SARAH TEMPLER, INTELLIGENT FRAUD DETECTION: DESIGN A MACHINE LEARNING FRAMEWORK FOR REAL-TIME FRAUD PREVENTION IN TRANSACTIONS, RESARCHGATE ,7/2022, p5

	التي تتجاوز سقفا ماليا معينا كنشاط مشبوه يستوجب التحقق.	الجديدة وأساليب الاحتيال المتطورة لضمان حماية استباقية وذكية.
التعامل مع البيانات	تم تصميم الطرق التقليدية للتعامل مع بيانات منظمة وقواعد مسبقة الصنع لكنها تظهر بكفاءة منخفضة بمجرد مواجهة بيانات عشوائية غير مهيكلة وغير قياسية.	يتميز تعلم الالة بقدرة عالية على فحص مختلف انواع البيانات سواء كانت منظمة أو غير منظمة والتي تشمل: النصوص، الصور، التسجيلات الصوتية فهده المرونة تمكنه من كشف الأنماط المخفية ومؤشرات الاحتيال بدقة عبر مصادر بيانات متنوعة.
الكشف في الوقت الفعلي	يعتمد غالبا على المعالجة بالدفعات مما يؤدي الى كشف الأنشطة الاحتيالية بعد وقوعها وبالتالي التأخر في الاستجابة	يتمتع بالقدرة على توفير إمكانية الكشف في الوقت الفعلي او شبه الفعلي مما يسمح بالاستجابة السريعة لمنع او تقليل النشاط الاحتيالي
القدرة على التكيف	يفتقر الى الديناميكية ويحتاج الى تحديثات يدوية ضرورية للأنظمة القائمة على القواعد لاستيعاب خطط الاحتيال الجديدة	يتعلم باستمرار ويعدل سلوكه بناءا على البيانات الجديدة مما يمكنه من التنبؤ مسبقا بتكتيكات الاحتيال المتطورة ومواجهتها مع القدرة على تحديد الأنماط والشدود التي لم تلاحظها من قبل
النتائج الإيجابية الخاطئة	ينتج عددا كبيرا من التنبيهات الخاطئة بسبب القيود الصارمة والغير مرنة للقواعد	يعزز الدقة من خلال دمج نطاق واسع من البيانات وتمييز الأنماط مما يقلل من التنبيهات الخاطئة
قابلية التوسع	يواجه تحديات عند زيادة حجم البيانات وغالبا ما يتطلب تدخلا بشريا وتعديلات يدوية	يمتلك قدرة فائقة ومرنة على التوسع وإدارة كميات هائلة من البيانات والمعاملات بكفاءة عالية
التعلم المستمر	تتطلب مراجعة بشرية وتحديثا يدويا للقواعد لاستيعاب أنماط الاحتيال الناشئة	يتميز بالقدرة على التعلم الذاتي والتحسن التلقائي من خلال التعرض لبيانات جديدة باستمرار

المصدر : من اعداد الطالبة بالاعتماد على مراجعة سابقة [127]

الفرع الرابع: أهمية استخدام خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني:

- **تحسين معدلات الكشف:** أفادت المؤسسات التي اعتمدت نماذج تعلم الالة للكشف عن الاحتيال المالي الالكتروني بقدرتها على اكتشاف الأنماط المعقدة التي قد تغيب عنها الأساليب التقليدية.

[127] C .MALLESHA ,M.HYMAVATHI, A REVIEW ON AI AND FRAUD DETECTION IN ACCOUNTIN :REDUCING RISKS AND ENHANCING FINANCIAL SECURITY , ACADEMY OF ACCOUNTING AND FINANCIAL STUDIES JOURNAL ,VOLUME 28,ISSUE 2, 2024,P 13-14

- **تقليل النتائج الإيجابية الخاطئة:** بفضل خوارزميات تعلم الالة تم خفض العديد من المعاملات المشروعة التي يتم تصنيفها بالخطأ كاحتيال، مما يحسن تجربة العميل ويقلل الضغط.
- **توفير التكاليف:** تعمل على حماية الأرباح عبر الحد من الخسائر المالية الاحتيالية المباشرة، مع خفض التكلفة التشغيلية من خلال اتمتة عمليات المراجعة اليدوية بدقة عالية.
- **قابلية التكيف:** اثبت العديد من اطر خوارزميات تعلم الالة قدرتها على التكيف والتوسع بدرجة عالية مع أنماط الاحتيال المتغيرة، ومع تطور أساليب المحتالين، حيث يمكن إعادة تدريب الإطار ببيانات جديدة. مما يضمن بقاء المؤسسة متقدمة على التهديدات الناشئة.
- **اتخاذ قرارات مبنية على البيانات:** توظيف التحليلات المتقدمة للبيانات من اجل تخصيص الموارد بشكل أفضل وتحسين استراتيجيات كشف الاحتيال.
- **تعزيز ثقة العملاء:** بفضل تحسين قدرات الكشف عن الاحتيال. تمكنت العديد من المؤسسات المالية من تعزيز ثقة عملاءها، من خلال تقليل الاضطرابات والتواصل الفعال بشأن التدابير الأمنية.[128]

الفرع الخامس: تحديات تطبيق نماذج خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني.

تواجه نماذج تعلم الالة العديد من التحديات اثناء تطبيقها ومن أبرز هده التحديات هي:

- **جودة البيانات:** حيث تؤدي البيانات الغير كاملة والمشوشة الى نتائج غير دقيقة وضعف في الأداء.
- **اختيار النموذج المناسب:** يعد اختيار الخوارزمية المناسبة من أبرز التحديات، حيث تختلف النماذج في التعقيد ومتطلبات التدريب والموارد الحسابية.
- الافراط في التعلم ونقص التعلم: الافراط في التعلم يؤدي الى حفظ تفاصيل البيانات بدل تعميمها، بينما نقص التعلم يمنع النموذج من فهم الأنماط الأساسية بشكل صحيح.
- **الخصوصية:** يتطلب استخدام بيانات شخصية او حساسة احترام الخصوصية وضمان عدم كشف هوية الافراد، رغم ان تقنيات كشف الهوية لا تكون دائما كافية.
- **حجم البيانات:** تحتاج النماذج الى كميات كبيرة من البيانات لتتعلم بشكل فعال ونقصها يحد من قدرتها على التعميم.
- **التحيز:** عدم توازن البيانات قد يؤدي الى نتائج منحازة لصالح فئة معينة على حساب الفئات الأخرى، مما يؤثر على عدالة النموذج.
- **كلفة التدريب والموارد:** تتطلب معظم خوارزميات تعلم الالة وقتا طويلا وموارد كبيرة للتدريب، مما يستدعي استخدام معالجات قوية لتسريع العملية.

[128] ANTHONY OWEN, SARAH TEMPLER, INTELLIGENT FRAUD DETECTION: DESIGN A MACHINE LEARNING FRAMEWORK FOR REAL-TIME FRAUD PREVENTION IN TRANSACTIONS, OP CIT, P20 - 21

- **قابلية تفسير النماذج:** النماذج المعقدة، خاصة نماذج التعلم العميق، يصعب تفسير قراراتها، مما يجعل فهم طريقة عملها تحديا مهما.[129]

المبحث الثالث: مراجعة الدراسات السابقة المتعلقة بالدراسة الحالية.

يستعرض هدا المبحث أبرز الادبيات التي لها علاقة بموضوع البحث الحالي والمرتبطة بمتغيراته فبرغم من تنوع المداخل المنهجية لتلك الدراسات واختلاف معالجة مواضيعها ونتائجها تسعى دراستنا لتكون لبنة تكميلية للجهود العلمية السابقة او تسلط الضوء على جوانب بحثية لم تنل حظها الكافي من البحث والتحليل سابقا.

المطلب الأول: الدراسات عربية.

وقد تضمنت الدراسات التالية:

الفرع الأول: دراسة فراحي فضيلة،2025 ،الجزائر

الباحث /السنة	فراحي فضيلة، 2025
عنوان الدراسة	نموذج تعلم الي ذكي لكشف الاحتيال في بطاقة الائتمان – تطبيق عملي على منصة تفاعلية –
نوع ومكان الدراسة	مقالة علمية صادرة بمجلة دفاتر اقتصادية، الجزائر
إشكالية الدراسة	كيف يمكن تطوير نموذج تعلم آلي ذكي باستخدام خوارزمية الغابة العشوائية، يتميز بالدقة والفعالية في كشف الاحتيال في بطاقات الائتمان، مع إمكانية تطبيقه عمليا من خلال منصة تفاعلية تخدم المؤسسات المالية والأمنية؟
هدف الدراسة	تطوير نموذج تعلم الي يعتمد على خوارزمية الغابة العشوائية للكشف عن الاحتيال في بطاقات الائتمان مع تطبيقه على منصة تفاعلية لتسهيل استخدامه في المؤسسات المالية
منهج الدراسة	اعتمدت الدراسة على المنهج الوصفي لوصف الظاهرة المدروسة، وعلى المنهج التجريبي، للتفاعل العملي مع الظاهرة المدروسة.
أداة الدراسة	خوارزمية الغابة العشوائية (Random Forest)، بيانات مالية، برمجية بايثون ومكتبته
العينة	بيانات معاملات بطاقات الائتمان
نتائج الدراسة	تحقيق النموذج دقة عالية تصل الى 90% في تصنيف العوامل المشتبه بها في عمليات الاحتيال المالية مع القدرة على تحديد اهم المتغيرات المؤثرة في كشف الاحتيال ببطاقات الائتمان وتحسين الكشف المبكر للمعاملات الاحتيالية

المصدر: من اعداد الطالبة اعتمادا على معطيات دراسة فراحي فضيلة

الفرع الثاني: دراسة علي بن الضب، 2023، الامارات العربية المتحدة.

[129] MATTHEW N.O.SADIKU,ET AL ,MACHINE LEARNING :AN OVERVIEW ,OP .CIT, P1126 -1127

الباحث /السنة	علي بن الضب،2023
عنوان الدراسة	دور الذكاء الاصطناعي وتعلم الالة في كشف الاحتيال على البطاقات الائتمانية.
نوع ومكان الدراسة	دراسة بحثية صادرة عن صندوق النقد الدولي، ابوظبي، الامارات العربية المتحدة.
إشكالية الدراسة	حاولت هده الدراسة معالجة إشكالية مفادها: هل تقنيات الذكاء الاصطناعي وخوارزميات تعلم الالة تساهم في تعزيز كشف الاحتيال على البطاقات الائتمانية والحد من خسائرها؟
هدف الدراسة	ابرا اهم تطبيقات الذكاء الاصطناعي وتعلم الالة في تعزيز كشف الاحتيال على البطاقات الائتمانية والمقارنة بين نتائج خوارزميات تعلم الالة الخاضع للإشراف.
منهج الدراسة	منهج وصفي، تجريبي.
أداة الدراسة	بيانات اصطناعية (Synthetic Data) واستخدام 4 خوارزميات: الانحدار اللوجيستي، أقرب الجيران، التحليل التمييزي الخطي، شجرة القرار.
العينة	بيانات اصطناعية تم انشاؤها بطريقة عشوائية عن طريق المحاكاة للأرقام العشوائية لعينة تتكون من 200 ألف بطاقة ائتمانية.
نتائج الدراسة	خوارزميات تعلم الالة تساهم في تعزيز كشف الاحتيال على البطاقات الائتمانية بقدرة تنبؤيه فاقت 94% كما ان خوارزمية التحليل التمييزي الخطي كانت أفضل أداء من بقية الخوارزميات المستخدمة مما يدعم التوجه نحو استخدام تقنيات تعلم الالة الحديثة وفرص الاستفادة من العديد من الخوارزميات.

المصدر: من اعداد الطالبة اعتمادا على معطيات دراسة علي بن الضب

الفرع الثالث: دراسة وسن هاشم كساب الكساسبة، 2023، الأردن.

الباحث /السنة	وسن هاشم كساب الكساسبة، 2023
عنوان الدراسة	اتر الذكاء الاصطناعي في الحد من الاحتيال المالي في البنوك التجارية الأردنية
نوع ومكان الدراسة	مقال علمي في مجلة جدارا للدراسات والبحوث، الأردن
إشكالية الدراسة	ما اتر الذكاء الاصطناعي المتمثل (بالجينات الخوارزمية، الوكلاء الاذكياء، الشبكات العصبية، تعلم الالة في الحد من الاحتيال المالي في البنوك التجارية الأردنية المدرجة في بورصة عمان)؟
هدف الدراسة	– التعرف إلى أثر الجينات الخوارزمية في الحد من الاحتيال المالي في البنوك التجارية الأردنية المدرجة في بورصة عمان. – التعرف إلى أثر الوكلاء الأذكياء في الحد من الاحتيال المالي في البنوك التجارية الأردنية المدرجة في بورصة عمان. – التعرف إلى أثر الشبكات العصبية في الحد من الاحتيال المالي في البنوك التجارية والأردنية المدرجة في بورصة عمان.

	– التعـرف إلى أثر تعلم الالة في الحـد من الاحتيال المالي في البنوك التجارية الأردنية المدرجة في بورصة عمان.
منهج الدراسة	منهج وصفي تحليلي
أداة الدراسة	الاستبانة الالكترونية
العينة	العاملين في الدوائر المالية والتدقيق في 12 بنكا تجاريا والبالغ عددهم 227 موظفا
نتائج الدراسة	وجود اتر دال إحصـائيا للذكاء الاصـطناعي والمتمثل في الجينات الخوارزمية، الوكلاء الاذكياء، تعلم الالة في الحد من الاحتيال المالي في البنوك التجارية الأردنية المدرجة في بورصـة عمان كما اوصـت الدراسـة النوك التجارية الأردنية بتبني كافة هده التقنيات لزيادة قدرتها على كشـف الأنشـطة الاحتيالية المشبوهة.

المصدر: من اعداد الطالبة اعتمادا على معطيات دراسة وسن هاشم كساب الكساسبة

المطلب الثاني: الدراسات الأجنبية.

وقد تضمنت الدراسات التالية:

الفرع الأول: دراسةGANESH KHEKARE ,ET AL 2025، الهند

الباحث /السنة	دراسةGANESH KHEKARE ,ET AL 2025
عنوان الدراسة	A COMPREHENSIVE PERFORMANCE COMPARISON OF TRADITIONAL AND ENSEMBLE MACHINE LEARNING MODELS FOR ONLINE FRAUD DETECTION
نوع ومكان الدراسة	دراسة بحتية أجريت في كلية علوم وهندسة الحاسوب، معهد فيلور للتكنولوجيا، فيلور، الهند
إشكالية الدراسة	كيف يمكن التعامل مع التحديات التي تواجه كشف الاحتيال في الوقت الفعلي نتيجة أحجام المعاملات الكبيرة وتعقيد أنماط الاحتيال الحديثة؟
هدف الدراسة	تقديم مقارنة شـاملة للأداء بين نماذج تعلم الآلة التقليدية وطرق التعلم التجميعي لكشـف الاحتيال في بطاقات الائتمان على مجموعة بيانات غير متوازنة للغاية.
منهج الدراسة	منهج تجريبي مقارن يتضـمن المعالجة المسـبقة للبيانات ثم تدريب النماذج وتقييمها باسـتخدام مقاييس الأداء حيث تم المقارنة 6 خوارزميات الغابة العشـــوائية وآلة ناقلات الدعم والانحدار اللوجســـتي و(XGBoost) ومصـــنف التكديس (أسـلوب تجميعي يدمج عدة تنبؤات خوارزميات مختلفة لتحسـين الدقة) ومصنف التصويت (أسلوب تجميعي يعتمد على تصويت الأغلبية لا تخاد القرار النهائي).
أداة الدراسة	تم استخدام لغة البرمجة بايثون (Python) ومكتباتها لبناء واختبار النماذج بالإضـافة إلى البيانات من منصة kaggle والخوارزميات الستة ومؤشرات التقييم للمقارنة

العينة	مجموعة بيانات للاحتيال ببطاقة الائتمان من(Kaggle) تحتوي على 284،807 معاملة إجمالية، منها 492 معاملة احتيالية فقط.
نتائج الدراسة	أظهرت النتائج أن خوارزميات مصنف التصويت (Voting Classifier) و(SVM) والغابة العشوائية حققت أعلى دقة عامة بنسبة 0.94 ومن جهة أخرى، تميزت الأساليب التجميعية مثل مصنف التصويت والتكديس (Stacking) بإحكام (Precision) شبه مثالي وصل إلى 0.99 و0.98 على التوالي، مما يجعلها فعالة للغاية في تقليل الإنذارات الكاذبة بينما تفوقت الطرق التقليدية مثل: (SVM) والغابة العشوائية والانحدار اللوجستي في جانب الاستدعاء (Recall)بنسب تراوحت بين 0.92 و0.93، مما يعني أنها أفضل في رصد أكبر عدد ممكن من حالات الاحتيال الفعلية وبالنظر إلى مقياسF1 الذي يوازن بين الإحكام والاستدعاء، أدى كل من مصنف التصويت والتكديس والغابة العشوائية أداءً قوياً بنسب تفوق 0.93 لتؤكد الدراسة في النهاية أن أساليب التعلم التجميعي هي الأكثر فعالية إجمالاً في كشف المعاملات الاحتيالية

المصدر: من اعداد الطالبة بالاعتماد على: دراسةGANESH KHEKARE ,ET AL

الفرع الثاني: دراسة PASCHAL ALUMONA ,ET AL،سنة 2025، الولايات المتحدة الامريكية

الباحث /السنة	دراسة PASCHAL ALUMONA ,ET AL، سنة 2025
عنوان الدراسة	Fraud Detection in Financial Transactions Using Machine Learning: Insights from the PaySim Mobile Money Dataset
نوع ومكان الدراسة	مقال بحتي منشور في مجلة (World Journal of Advanced Research and Reviews) المكان الولايات المتحدة الامريكية
إشكالية الدراسة	تعجز أنظمة كشف الاحتيال التقليدية القائمة على القواعد عن تغيير معاملاتها بشكل فوري مع أنماط التهديد المتغيرة باستمرار وتدفقات البيانات واسعة النطاق
هدف الدراسة	يهدف البحث الحالي إلى سد الفجوة البحثية من خلال إجراء تحليل (RFM) وتجميع (K-Means) على مجموعة بيانات ضخمة لمعاملات الأموال عبر الهاتف المحمول، يليه تطبيق تعلم الآلة الخاضع للإشراف للكشف عن الاحتيال.
منهج الدراسة	منهج وصفي تجريبي يشمل تصميم إطار عمل تحليلي هجين انطلاقا اعداد البيانات تم مرحلة التوصيف السلوكي انطلاقا من استخدام نموذج (Rfm) لتحليل سلوك المستخدمين تم طبق خوارزمية (K-Means) لتجميع العملاء في فئات تم مرحلة هندسة الميزات بابتكار ميزة جديدة وهي تغيير الرصيد تم قام بتدريب النموذج على أربعة أنواع من خوارزميات تعلم الالة ليرى أيها الأفضل: الانحدار اللوجستي، الجار الأقرب، شجرة القرار، الغابة العشوائية. تم في الأخير مرحلة التقييم والمقارنة بين النماذج.
أداة الدراسة	نموذج (Rfm)، خوارزميات: (K-Means)، الانحدار اللوجستي، الجار الأقرب، شجرة القرار، الغابة العشوائية، مؤشرات تقييم الأداء

العينة	مجموعة البيانات محاكاة لمعاملات الأموال عبر الهاتف المحمول حيث يتم تمثيل بارامترات معينة مثل نوع المعاملة، المبلغ، والأرصدة الأصلية والجديدة
نتائج الدراسة	شجرة القرار (Decision Tree) هي الأفضل عملياً لأنها حققت التوازن بين كشف المحتالين وعدم إزعاج الزبائن العاديين بإنذارات خاطئة.

من اعداد الطالبة بالاعتماد على دراسة PASCHAL ALUMONA ,ET AL

الفرع الثالث: دراسة 2025HONGFANG ZHOU ,ET AL، الصين

الباحث /السنة	**دراسة 2025HONGFANG ZHOU ,ET AL**
عنوان الدراسة	A Deep Learning Hybrid RNN-LSTM Model for Credit Card Fraud Detection
نوع ومكان الدراسة	مقالة بحتية اكاديمية، الصين
إشكالية الدراسة	لمعالجة القصور الذي تعاني منه نماذج التصنيف التقليدية عندما تواجه بيانات شديدة الاختلال في التوازن في كشف احتيال بطاقات الائتمان
هدف الدراسة	إجراء تحليل منهجي لخصائص توزيع الفئات لمجموعات بيانات المعاملات الحقيقية والدمج مع معالجة التوازن بالعينات العلوية أو السفلية، بهدف إنشاء شبكة عصبية عميقة قادرة على تعلم الاعتماديات الزمنية. تطرح هذه الورقة نموذجًا مدمجًا يدمج بنية الشبكة العصبية المتكررة والذاكرة طويلة المدى (RNN-LSTM) مع استراتيجية أخذ عينات هجينة
منهج الدراسة	منهج تجريبي.
أداة الدراسة	تمثلت أداة الدراسة في اربع خوارزميات هي: الأولى هي نموذجًا هجين يدمج بنية الشبكة العصبية المتكررة والذاكرة طويلة المدى (RNN-LSTM) قاما بتصميمه بالإضافة الى مقارنتها مع خوارزمية (kNN)، (LTSM)،(AdaBoost) مع استراتيجية أخذ عينات هجينة مزيج من (SMOTE)، (Random Oversampling)، (ADASYN)، (NearMiss)، وغيرها.
العينة	مجموعة البيانات الأوروبية لبطاقات الائتمان (European Credit Card Dataset) المتاحة على منصة (Kaggle). تحتوي على إجمالي 284،807 معاملة، من بينها 492 معاملة احتيالية، وهو ما يمثل حوالي 0.172% من جميع المعاملات
نتائج الدراسة	اظهرت النتائج التجريبية أن نموذج RNN-LSTM المحسّن يحقق أداءً ثوريًا، حيث يحسن درجة F1 بنسبة 5.31% (لتصل إلى 0.8544)، ويحافظ على دقة إجمالية قدرها 99.96%، ويحقق نسبة استدعاء للاحتيال قدرها 80.56%، ويتفوق على النماذج المرجعية في الدقة الإيجابية (84.12%) وقيمة.(0.932) AUC

من اعداد الطالبة بالاعتماد على دراسة، Hongfang Zhou ; et al

الفرع الرابع: دراسة M. HYMAVATHI ,C. MALLESHA، 2024، الهند

الباحث /السنة	**دراسة M .HYMAVATHI ,C.MALLESHA** سنة 2024
عنوان الدراسة	A review on ai and fraud detection in accounting: reducing risks and enhancing financial security

نوع ومكان الدراسة	مقالة علمية، منشورة في مجلة (Academy of Accounting and Financial Studies Journal)، المكان جامعة انوراغ الهند
إشكالية الدراسة	الأساليب التقليدية لكشف الاحتيال، التي تعتمد بشكل كبير على الفحص اليدوي والخوارزميات القائمة على القواعد، أثبتت عدم كفايتها في ظل استراتيجيات الاحتيال المتطورة بسرعة مما يستدعي البحث عن تقنيات أفضل.
هدف الدراسة	تحليل مجموعة من تقنيات الذكاء الاصطناعي وتعلم الالة في قدرتها على كشف الشدود وتحديد الأنماط الاحتيالية المشبوهة وتقييم دقة وفعالية هده أنظمة مقارنة بالأساليب اليدوية التقليدية.
منهج الدراسة	وصفي تحليلي حيت ان أن الباحثين قاموا بجمع الأبحاث السابقة والتقنيات الموجودة وقاموا بتحليل نتائجها ومقارنتها ببعضها
أداة الدراسة	المسح المكتبي للبيانات المنشورة مسبقاً. استخدموا الوثائق والتقارير العلمية وقاموا بتحليلها ومقارنتها كأداة لاستخراج المعلومات.
العينة	بيانات مستخلصة من ابحاث ومقالات علمية متخصصة في كشف الاحتيال
نتائج الدراسة	تفوقت أساليب كشف الاحتيال القائمة على الذكاء الاصطناعي وتعلم الالة على الأساليب التقليدية من حيث القدرة على التكيف، الدقة، الكشف في الوقت الفعلي، والقدرة على التعامل مع أنواع البيانات المتنوعة مع ضرورة التحديث المستمر للأنظمة كشف الاحتيال.

من اعداد الطالبة بالاعتماد على دراسة (M .Hymavath،C. Mallesha)

الفرع الخامس: دراسة،(SAGAR BHARAT SHAH،2024)، الولايات المتحدة الامريكية

الباحث /السنة	سنة SAGAR BHARAT SHAH 2024
عنوان الدراسة	Improving Financial Fraud Detection System with Advanced Machine Learning for Predictive Analysis and Prevention
نوع ومكان الدراسة	مقال علمي نشر في مجلة (IJSRCSEIT) المكان الويات المتحدة الامريكية
إشكالية الدراسة	يمثل الاحتيال في بطاقات الائتمان مشكلة كبرى للمؤسسات المالية. يكلف الاحتيال في بطاقات الائتمان أكثر من مليون شخص كل عام عبر عدة دول مختلفة. كما أن الدراسات البحثية التي تتضمن بيانات حقيقية لبطاقات الائتمان قليلة ومتباعدة بسبب قضايا الخصوصية.
هدف الدراسة	تهدف هذه الورقة إلى تحليل نظام كشف الاحتيال المالي الذي يستخدم خوارزميات تعلم الآلة مع التركيز بشكل خاص على بيانات بطاقات الائتمان.(CCFD)
منهج الدراسة	تبعت الدراسة منهجًا تجريبيا مقارن لتصميم أنموذج يبدأ بجمع البيانات، ثم المعالجة المسبقة للبيانات (إزالة التكرارات ومعالجة القيم المفقودة)، ثم موازنة البيانات باستخدام تقنيةBorderline-SMOTE ، ثم تقسيم البيانات إلى 70% للتدريب و30% للاختبار، ثم تصنيف المعاملات باستخدام خوارزميات تعلم الآلة، وأخيرًا تقييم الأداء باستخدام مؤشرات التقييم

أداة الدراسة	استخدم الباحث خوارزميات: الغابة العشوائية، شجرة القرار، الة المتجهات الداعمة، الشبكات دات الذاكرة طويلة – قصيرة المدى بالإضافة لتقنية (Smote)
العينة	بيانات حقيقية لحاملي بطاقات ائتمان أوروبيين مخفاة الهوية تتكون من 284،807 معاملة تحتوي على 30 ميزة (خاصية)، وتهدف إلى اكتشاف الأنشطة الاحتيالية. البيانات غير متوازنة بشكل كبير، حيث تحتوي على 492 حالة احتيال فقط مقابل 284،315 معاملة غير احتيالية.
نتائج الدراسة	بعد المقارنة بين النماذج، أثبتت النتائج أن خوارزمية الشبكات ذات الذاكرة قصيرة وطويلة المدى هو الأفضل والأكثر دقة في كشف الاحتيال المالي، متفوقًا على خوارزميات: شجرة القرار، الغابة العشوائية، والة المتجهات الداعمة.

المصدر: من اعداد الطالبة بالاعتماد على دراسة سنة 2024 SAGAR BHARAT SHAH

الفرع السادس: دراسة، TOTOK DEWAYANTO ,NADIA HUSNANINGTYAS، 2023، إندونيسيا

الباحث /السنة	دراسة، TOTOK DEWAYANTO ,NADIA HUSNANINGTYAS، 2023
عنوان الدراسة	Financial fraud detection and machine learning algorithm (unsupervised learning): systematic literature review
نوع ومكان الدراسة	مقالة بحتية نشرت في مجلة (Akuntansi dan Bisnis Airlangga) صادرة عن جامعة ايرلانجا في مدينة سورابايا اندونيسيا
إشكالية الدراسة	تتطلب تعقيدات وتطور الأنشطة الاحتيالية مناهج مبتكرة للكشف عنها، بينما لا يزال التعلم غير الخاضع للإشراف (وخاصة تقنيات التجميع) ممثلا بشكل ناقص في الأدبيات الحديثة
هدف الدراسة	يهدف هذا البحث إلى تقييم استخدام التعلم غير الخاضع للإشراف في كشف الاحتيال المالي عبر مختلف القطاعات المالية من خلال تحديد البنى المعرفية، والفوائد، والتحسين الاقتصادي، والتحديات.
منهج الدراسة	تتبع الدراسة منهجية المراجعة الأدبية وفقا لبروتوكول (PRIMS) لاختيار المقالات حيت ان الباحثون قاموا بدور المحلل للأبحاث السابقة بدلا من تصميم نموذج واحد قاموا بفحص مئات الأبحاث التي فيها تصميم لنماذج ليعرفوا ماهي أفضل خوارزمية والنتائج التي وصل اليها العلم الى حد الان
أداة الدراسة	الأدوات المستخدمة هي قاعدة بيانات SCOPUSللبحت عن المصادر وإطار عمل PICO(السكان التدخل المقارنة النتائج) لتصميم أسئلة البحت
العينة	في هده الدراسة البيانات هي المقالات العلمية المنشورة في منصة SCOPUSمن فترة 2010 الى فترة 2023 ووجدوا 3283 مقال تم قاموا بتصنيفها بناءا على معايير صارمة متل لغة المقال وتخصصه في التعلم الغير خاضع للإشراف حتى وصلوا الى عينة 27 مقالا هي الأكثر أهمية وجودة في هدا التخصص وهي التي خضعت للتحليل الدقيق

نتائج الدراسة	كشفت النتائج أن التعلم غير الخاضع للإشراف قد تم تطبيقه في قطاعات مالية متنوعة، وأبرزها الخدمات المصرفية لكشف الشذوذ في معاملات البطاقات الائتمانية. وتعد خوارزمية (K-Means) هي الطريقة الأكثر شعبية، مع استمرار تحديات مثل عدم توازن الفئات وتعقد الأنشطة الاحتيالية

من اعداد الطالبة بالاعتماد على دراسة TOTOK DEWAYANTO ,NADIA HUSNANINGTYAS

الفرع السابع: دراسة ANTIGONI KRUTI ,SONJOY RANJON DAS ,ET AL، 2023 ،إنجلترا

الباحث /السنة	ANTIGONI KRUTI ,SONJOY RANJON DAS ,ET AL، سنة 2023
عنوان الدراسة	Evaluation of Machine Learning Models for Credit Card Fraud Detection : A Comparative Analysis of Algorithmic Performance and their efficacy
نوع ومكان الدراسة	مقال بحثي أكاديمي جامعة نورثمبريا (Northumbria University) في المملكة المتحدة (إنجلترا)، بالتعاون مع جامعة تريبوفان في نيبال منشور في مجلة. FMDB
إشكالية الدراسة	كيف يمكن تقييم ومقارنة أداء خوارزميات تعلم الآلة المختلفة لتصميم حلول قوية قادرة على اكتشاف والتنبؤ بالمعاملات الاحتيالية في بطاقات الائتمان، ومعالجة تحديات البيانات المعقدة لضمان أمن المعاملات؟
هدف الدراسة	هدف البحث إلى تطوير آلية تعتمد على مصنفات ذكية) مثل(ann) و(svm) و(naive bayes) لاكتشاف الأنشطة المالية المشبوهة، وتوفير حل قوي لسيناريوهات الاحتيال الحقيقية مع مراعاة معدلات الدقة العالية
منهج الدراسة	منهج تجريبي مقارن الذي يعتمد على معالجة البيانات، هندسة الميزات، تقليل الأبعاد الهجين، وتقسيم البيانات لتدريب واختبار النماذج
أداة الدراسة	خوارزميات تعلم الآلة (ANN)، Logistic Regression، Random Forest، Naive Bayes ، SVM، (XGBoost واستخدام تقنيات المعالجة مثل Quantile Transformer و PCA وAutoencoder
العينة	مجموعة بيانات معاملات بطاقات الائتمان لحاملي بطاقات أوروبيين في سبتمبر 2013، وتتضمن 284،807 معاملة (منها 492 معاملة احتيالية بنسبة 0.172%)
نتائج الدراسة	اظهرت النتائج أن نموذج الشبكة العصبية الاصطناعية (ANN) حقق أعلى درجة استدعاء (Recall)بنسبة 0.81، يليه الانحدار اللوجستي و SVCبنسبة 0.76

من اعداد الطالبة بالاعتماد على دراسة Antigoni Kruti .et al،Sonjoy Ranjon Das ،

الفرع الثامن: دراسة ANMOL VARSHNEY ,PALAK GUPTA ,ET AL، 2023 ،الهند

الباحث /السنة	دراسة ANMOL VARSHNEY ,PALAK GUPTA ,ET AL، 2023

عنوان الدراسة	Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques
نوع ومكان الدراسة	مقال علمي نشـر في مجلة (Procedia Computer Science) تابعة لدار النشـر الشـهيرة (Elsevier) الهند مدينة ديرادون
إشكالية الدراسة	تكمن إشكالية الدراسة في تزايد الاحتيال المالي وفشل النماذج التقليدية في كشفها بدقة بسبب عدم توازن البيانات حيت ان معاملات الاحتيال قليلة جدا مقارنة بالسـليمة مما يؤدي الى نتائج منحازة وغير دقيقة
هدف الدراسة	تحليل أداء خوارزميات التصـنيف المختلفة تحت ظروف البيانات غير متوازنة والمتوازنة واقتراح افضل تقنية موازنة لتحسين دقة الاحتيال
منهج الدراسة	منهج تجريبي
أداة الدراسة	اتباع اطار عمل تجريبي يتكون من معالجة البيانات مسـبقا، اختيار السـمات، موازنة البيانات، تم تدريب اربع خوارزميات تصـنيف: الانحدار اللوجسـتي، شـجرة القرار، الشـبكات العصـبية، (XGBOOST) تم أخيرا تقييم الأداء بواسطة مؤشرات تقييم الأداء
العينة	داتا سـات تم الحصـول عليها من منصـة (kaggle) خاصـة بالاحتيال ببطاقة الائتمان تتكون من 284،807 عملية مالية بالبطاقات الائتمانية، منها 284،315 عملية سليمة و492 عملية احتيالية فقط
نتائج الدراسة	أظهرت الدراسة أن خوارزمية (XGBoost) هي الأفضل أداء بشكل عام، وأن تقنية زيادة العينات (Random Oversampling) ضل تقنية موازنة، حيث حققت دقة كشف غير منحازة تصل إلى 99.8%

المصدر: من اعداد الطالبة بالاعتماد على دراسة ANMOL VARSHNEY ,PALAK GUPTA ,ET AL

الفرع التاسع: دراسة M. A. THINESH S. S. MUKHIL VARMANN ,ET AL2023، الهند

الباحث /السنة	دراسة M. A. THINESH S. S. MUKHIL VARMANN ,ET AL سنة 2023
عنوان الدراسة	Detection of Credit Card Fraud Using Random Forest Classification Model
نوع ومكان الدراسة	مقال علمي Model منشورة في مجلة FMDB Transactions on Sustainable Technoprise Letters، الهند
إشكالية الدراسة	كيف يمكن تطوير نماذج تعلم آلة مدربة بشكل أفضل وذات تقييمات عالية قادرة على كشف الاحتيال في بطاقات الائتمان، خاصـة في ظل التغيرات المسـتمرة في أسـاليب الاحتيال، وقلة البيانات المتاحة، وضعف النماذج الحالية في التعامل مع بيانات الاحتيال بشكل جيد؟
هدف الدراسة	اسـتخدام مصـنف غابة القرار العشـوائي بهدف تحديد المعاملات الاحتيالية بدقة وتقليل النتائج الإيجابية الكاذبة، وذلك للوصـول إلى مسـتوى عالٍ من الدقة في كشـف الاحتيال، مع ضـمان عدم وضـع علامة "احتيال" على المعاملات الشرعية بالخطأ.

منهج الدراسة	منهج تجريبي
أداة الدراسة	لغة البرمجة Python بالإضافة الى مكتبات البرمجية pandas:،numpy،matplotlib،seaborn ، sklearn وتحديداًRandomForestClassifier
العينة	مصدر البياناتKaggle وحجم العينة (مجموعة البيانات): 7231 معاملة عدد الخصائص (الأعمدة) 30 عموداً (28 عموداً لبيانات شخصية مشفرة، وعمود المبلغ، وعمود التصنيف احتيال/غير احتيال)
نتائج الدراسة	حقق مصنف غابة القرار العشوائي المقترح نتائج جيدة حيث بلغت الدقة = 99.59%، متوسط الدقة الإيجابية = 100%، متوسط الاستدعاء = 88%، متوسط درجة F1= 93%، النوعية = 100% ومعدل الخطأ = 0.41 %من منحنىROC، نجد أن درجة AUC للنموذج المقترح هي 0.94، وهي عالية جداً حيث أن نطاق درجةAUC هو من 0 إلى 1، و0.94 قريب جداً من 1، مما يظهر الأداء الفعال للنموذج في التمييز بين الأمثلة الإيجابية والسلبية

من اعداد الطالبة بالاعتماد على M. A. THINESH S. S. MUKHIL VARMANN ,ET AL

الفرع العاشر دراسة (ET AL، SHAHNAWAZ KHAN ,ABDULLAH ALOURANI 2022)المملكة العربية السعودية

الباحث /السنة	دراسة ET AL، SHAHNAWAZ KHAN ,ABDULLAH ALOURANI سنة 2022
عنوان الدراسة	Developing a Credit Card Fraud Detection Model using Machine Learning Approaches
نوع ومكان الدراسة	دراسة بحثية نشرت في مجلة (IJACSA)، المملكة العربية السعودية
إشكالية الدراسة	هل يمكن تطوير نظام آلي فعال يمكنه تصنيف المعاملات المالية كاحتيالية أو حقيقية بدقة، مع التغلب على مشكلة عدم توازن البيانات الضخمة؟
هدف الدراسة	تهدف هذه الدراسة البحثية إلى تطوير نموذج لكشف الاحتيال في بطاقات الائتمان يمكنه تصنيف المعاملات عبر الإنترنت بفعالية إلى احتيالية أو حقيقية
منهج الدراسة	منهج تجريبي مقارن القائم على تعلم الآلة الخاضع للإشراف حيث تم المقارنة بين 3 خوارزميات: الانحدار اللوجستي(LR)، الشبكات العصبية الاصطناعية(ANN)، وآلات المتجهات الداعمةSVM) من خلال مؤشرات تقييم الأداء
أداة الدراسة	استخدمت الدراسة ثلاث تقنيات أساسية لتعلم الآلة: الانحدار اللوجستي(LR)، الشبكات العصبية الاصطناعية(ANN)، وآلات المتجهات الداعمة.(SVM) مع استخدام تقنيات "إعادة أخذ العينات (RESAMPLING) المعالجة للبيانات غير المتوازنة قبل التدريب .
العينة	مجموعة بيانات تحتوي على معاملات أجراها حاموا بطاقات أوروبيون في سبتمبر 2013، وتضم 284،807 معاملة تمت خلال يومين، منها 492 معاملة احتيالية فقط.

نتائج الدراسة	أظهر التحليل أن المصنف القائم على "آلة المتجهات الداعمة (SVM) "يتفوق على المصنفات الأخرى (الانحدار اللوجستي والشبكات العصبية) في كافة مقاييس الأداء.

المصدر: من اعداد الطالبة بالاعتماد على دراسة ABDULLAH ALOURANI ,SHAHNAWAZ KHAN ،ET AL

الفرع الحادي عشر: دراسة PAUL SANT ,ET AL، 2022، بريطانيا

الباحث /السنة	دراسة PAUL SANT ,ET AL، سنة 2022
عنوان الدراسة	Review of Machine Learning Approach on Credit Card Fraud Detection
نوع ومكان الدراسة	مقالة بحثية نشرت بمجلة Human-Centric Intelligent Systems بجامعة بدفوردشاير بالمملكة المتحدة بريطانيا
إشكالية الدراسة	تمحورت إشكالية الدراسة في العديد من الأسئلة أهمها: • ما مدى تأثير مشكلة عدم التوازن للبيانات على كفاءة تصنيف الخوارزميات وكيف نعالجها؟ • كيف يمكن تصميم نظام قادر على كشف المعاملات الاحتيالية المتنوعة بغض النظر عن الموقع الجغرافي والعملة المستخدمة؟ • لمادا تعجز الخوارزميات التقليدية عن تقديم أداء متالي وفي الوقت الفعلي عند التعامل مع مجموعة بيانات ضخمة؟
هدف الدراسة	تسعى هده الورقة البحثية الى مراجعة وتقييم جوانب مختلفة من كشف الاحتيال في بطاقة الائتمان والخصم وتدرس تقنيات مختلفة لكشف معاملات بطاقة الائتمان الاحتيالية وتسعى لاقتراح أنموذج هجين لكشف الاحتيال ببطاقة الائتمان
منهج الدراسة	منهجي تحليلي تجريبي حيت أجرى الباحثون تحليلا مقارنا لمراجعة الادبيات مع مراعاة تقنيات التعلم الالي لكشف الاحتيال ببطاقة الائتمان وسرية البيانات بالإضافة الى تصميم أنموذج هجين مقترح.
أداة الدراسة	تتمثل أداة الدراسة في النموذج الهجين المقترح الدي صممه الباحثون ويتكون من تقنيتين Annو اطار التعلم الاتحادي كأداة تنظيمية تسمح بتدريب الخوارزميات على أجهزة البنوك نحليا دون الحادة الى نقل البيانات فعليا لضمان الخصوصية كما استخدمت تقنية smotلمعالجة البيانات عدم توازن البيانات عبر زيادة عينات الاحتيال اصطناعيا
العينة	عينة بيانات ضخمة بين معاملات مالية حقيقية وبيانات تجريبية مخبرية شملت الدراسة مجموعات بيانات من بنوك أوروبية وبنوك أسترالية، والمانية، وصينية من حاملي بطاقة الائتمان تحتوي على 284،807 معاملة مشروعة مقابل 492 مقابل 492 معاملة احتيالية فقط
نتائج الدراسة	اشارت المراجعة إلى أن استخدام الشبكات العصبية (ANN) مع خوارزميات التدريب المناسبة حقق دقة وصلت إلى 99.96 % في بعض الحالات التطبيقية

	فعالية النموذج الهجين: أثبت الجانب التطبيقي أن دمج ANN مع التعلم الاتحادي هو حل فعال لتحقيق دقة عالية مع الامتثال لقوانين حماية البيانات تحسين الكشف: النموذج المقترح الهجين يساهم في تقليل الإنذارات الكاذبة (False-alarms) وتحسين سرعة الكشف في الوقت الفعلي مقارنة بالخوارزميات التقليدية مثل SVM التي تتباطأ مع البيانات الضخمة

من اعداد الطالبة بالاعتماد على دراسة Paul Sant،ET AL

الفرع الثاني عشر: دراسة PRATYUSH SHARMA ,ET AL 2021،الهند

الباحث /السنة	دراسة PRATYUSH SHARMA ,ET AL 2021
عنوان الدراسة	Machine Learning Model for Credit Card Fraud Detection- A Comparative Analysis
نوع ومكان الدراسة	مقالة بحتية من كلية علوم الحاسوب نشر في مجلة (IAJIT)، الهند
إشكالية الدراسة	الأنشطة الاحتيالية في ازدياد؛ لذا فإن تنفيذ نظام منهجي لكشف الاحتيال أمر لا غنى عنه والأساليب التقليدية تستهلك الكثير من الوقت وغالباً ما تكون غير فعالة
هدف الدراسة	استخدام خوارزميات تعلم آلة مختلفة لتدريب نموذج تعلم آلة بناءً على مجموعة بيانات معطاة وإنشاء دراسة مقارنة حول الدقة والمقاييس المختلفة.
منهج الدراسة	منهج وصفي تجريبي حيت تم جمع البيانات متبوعاً بالمعالجة المسبقة تم إيجاد الارتباط بين مجموعة البيانات واستخدام خوارزميات تعلم آلة مختلفة. باستخدام التحليل المقارن بناءً على مقياس الأداء المختلفة
أداة الدراسة	استخدم الباحثون 4 خوارزميات تعلم الة: الانحدار اللوجستي، الة المتجهات الداعمة، الغابة العشوائية، الشبكة العصبية الاصطناعية للمقارنة فيما بينها في كشف الاحتيال ببطاقة الائتمان باستخدام مؤشرات الأداء بالإضافة الى مكتبات (sklearn) و(imblearn)، ووظائف (StandardScaler) و (Grid Search CV) لضبط المعلمات.
العينة	تم جلب مجموعة البيانات خاصة بالاحتيال ببطاقة الائتمان من موقع (Kaggle) بإجمالي 284،807 معاملة
نتائج الدراسة	خلصت دراستنا إلى أن الشبكة العصبية الاصطناعية (ANN) حققت أفضل أداء مقارنة بالخوارزميات الأخرى وهي الأنسب في كشف الاحتيال المالي والأكثر دقة

من اعداد الطالبة بالاعتماد على دراسة,PRATYUSH SHARMA ,ET AL

الفرع الثالث عشر :دراسة (VIKAS THMMANNA GOWDA)، 2021، الولايات المتحدة الامريكية

الباحث /السنة	دراسة VIKAS THMMANNA GOWDAسنة 2021
عنوان الدراسة	Credit Card Fraud Detection using Supervised and Unsupervised Machine Learning

نوع ومكان الدراسة	ورقة بحثية منشورة في مؤتمر CSIT2021، الولايات المتحدة الأمريكية
إشكالية الدراسة	ما هو أفضل خوارزمية تعلم آلي (خاضع للإشراف أو غير خاضع للإشراف) لكشف احتيال بطاقات الائتمان عند تطبيقه على مجموعة بيانات غير متوازنة، وذلك بناءً على مقاييس الأداء؟
هدف الدراسة	تقييم مجموعة بيانات غير متوازنة باستخدام عدة خوارزميات تعلم آلي (ثلاث خاضعة للإشراف وثلاث غير خاضعة للإشراف) وتحديد أفضل خوارزمية لكشف احتيال بطاقات الائتمان.
منهج الدراسة	منهج تجريبي مقارن مقارنة بين 6 خوارزميات تعلم الة
أداة الدراسة	• خوارزميات تعلم الالة الستة: منها 3 خوارزميات تعلم خاضعة للإشراف: الانحدار اللوجستي، الة المتجهات الداعمة، الغابة العشوائية، و3 خوارزميات غير خاضعة للإشراف متمثلة في: غابة العزل، عامل الشدود المحلي، متوسط K. • المقاييس: الدقة (Accuracy)، الاستدعاء(Recall)، الدقة الإيجابية (Precision)، درجةF1 • البيانات: مجموعة بيانات (Kaggle) لمعاملات بطاقات ائتمان عام 2013.
العينة	مجموعة بيانات Kaggle لمعاملات بطاقات ائتمان عام 2013، إجمالي المعاملات: 284،807 معاملة. – المعاملات الاحتيالية: 492 معاملة (نسبة 0.173%). – المعاملات الشرعية: الباقي. – الخصائص: 30 عموداً
نتائج الدراسة	خوارزمية (SVM) هي الأفضل بين جميع الخوارزميات المستخدمة لكشف الاحتيال، بدقة 98.49% وقيم عالية لكل من Precision وRecall أما بين خوارزميات التعلم غير الخاضع للإشراف، فخوارزمية K-Means هي الأفضل.

من اعداد الطالبة بالاعتماد على دراسة VIKAS THMMANNA GOWDA

الفرع الرابع عشر: دراسة AHMAD ALALI ,MATAR AL MARRI، 2020، دبي– الامارات العربية المتحدة

الباحث /السنة	دراسة AHMAD ALALI ,MATAR AL MARRI سنة 2020
عنوان الدراسة	Financial Fraud Detection using Machine Learning Techniques
نوع ومكان الدراسة	مذكرة ماجيستير في العلوم: تحليل البيانات. قسم برامج الدراسات العليا والبحث، معهد روتشستر للتكنولوجيا، دبي دولة الإمارات العربية المتحدة،
إشكالية الدراسة	الزيادة السريعة في الاحتيال المالي الذي يحدث في أنظمة الدفع تتطلب ضرورة استكشاف نهج لحل مشكلة اكتشاف المدخلات/المعاملات الاحتيالية في كميات كبيرة من البيانات من أجل الاستعداد بشكل أفضل لحل قضايا الجرائم السيبرانية
هدف الدراسة	– دراسة الأدبيات المتعلقة بكشف الاحتيال المالي وفهم الجوانب المختلفة للمشكلة – حل مشكلة كشف الاحتيال المالي على مجموعة بيانات عينة متاحة للجمهور باستخدام تقنيات تعلم الآلة الخاضعة للإشراف

	– مقارنة تقنيات التصنيف المختلفة لفهم أيهما الأنسب لهذا التطبيق
منهج الدراسة	منهج تجريبي حيث تم اتباع نهج تعلم الآلة النموذجي انطلاقا من تحليل مجموعة البيانات بالتفصيل وتحديد المتنبئات المحتملة للاحتيال تم تجريب تقنيتين من تقنيات تعلم الآلة الخاضعة للإشراف – الانحدار اللوجستي والغابة العشوائية حيث تم تطوير النماذج مع التحقق المتقاطع (cross-validation) لتجنب الإفراط في التخصيص. تم استخدام خوارزميتين والمقارنة بينهم انطلاقا من مؤشرات تقييم نماذج تعلم الالة
أداة الدراسة	الانحدار اللوجستي والغابة العشوائية
العينة	مجموعة بيانات اصطناعية تخص الاحتيال في المعاملات (Transaction Fraud) وتحديدا كل ما ينطبق على مدفوعات الهاتف المحمول متاحة للجمهور على (Kaggle) تحتوي مجموعة البيانات على 11 عموداً من المعلومات لحوالي 6 ملايين صف من البيانات
نتائج الدراسة	نلاحظ أن الغابة العشوائية (Random Forest) تؤدي بشكل أفضل في هذا التطبيق مع درجات دقة واستدعاء تصل إلى 100% تقريباً. بينما نموذج الانحدار اللوجستي الافتراضي قادر على التقاط نصف حالات الاحتيال الفعلية فقط. يمكننا استنتاج أن كشف الاحتيال في المعاملات المالية ناجح في مجموعة البيانات هذه، وأفضل خوارزمية لهذا الغرض هي الغابة العشوائية

من اعداد الطالبة بالاعتماد على دراسةAHMAD ALALI ,MATAR AL MARRI

الفرع الخامس عشر: دراسة FAKHRA AKHTAR ,ET AL 2020، باكستان

الباحث /السنة	دراسة FAKHRA AKHTAR ,ET ALسنة 2020
عنوان الدراسة	Credit card fraud detection through model Testing using Orange Tool
نوع ومكان الدراسة	مقالة، منشورة في مجلة International Journal of Latest Engineering and Management Research (IJLEMR)، باكستان
إشكالية الدراسة	تتمثل إشكالية الدراسة في تصاعد عمليات الاحتيال عبر بطاقات الائتمان رغم توفر اليات متعددة لمكافحتها.
هدف الدراسة	الهدف من هده الدراسة تطوير نظام لكشف الاحتيال عبر مقارنة خوارزميات تعلم الة مختلفة
منهج الدراسة	منهج وصفي تجريبي
أداة الدراسة	تم استخدام برنامج Orangeو3 خوارزميات للمقارنة بين اداءها: وهي خوارزمية الغابة العشوائية، الانحدار الخطي والَ AdaBoost
العينة	تم استخدام مجموعة بيانات متاحة للعموم من مستودع UCI لتعلم الالة تتعلق بالاحتيال في بطاقات الاءتمان ، تحتوي على 31 سمة .
نتائج الدراسة	اظهرت نتائج التقييم أن نموذج AdaBoost حقق أعلى قيمة لمعامل التحديد R حيث بلغت 0.984 يليه نموذج Forest Random بقيمة 0.975 في حين جاء نموذج Regression Linear في المرتبة الأدنى بقيمة 0.396 أما فيما يخص قيم التنبؤ مقابل المتغير المستهدف v1، فقد تفوق نموذجLinear Regression بنسبة 88%، يليه Random Forest بنسبة83%

بينما كان أدنى قيمة لنموذج AdaBoost بنسبة52% وخلص الباحثون إلى أن نموذجي Regression Linearو Random Forest هما الأفضل للتنبؤ بالاحتيال على بطاقات الائتمان	

من اعداد الطالبة بالاعتماد على دراسة FAKHRA AKHTAR ,ET AL

المطلب الثالث: المقارنة بين الدراسة الحالية والدراسات السابقة

يركز هدا المطلب على مقارنة دراستنا الحالية بالدراسات السابقة المذكورة سابقا من خلال ذكر اهم أوجه الاختلاف والتشابه بينهم.

الفرع الأول: المقارنة بين الدراسة الحالية مع الدراسات العربية.

تتلخص اهم الفروقات بين دراستنا والدراسات العربية من خلال الجدول التالي:

المقارنة	أوجه التشابه	أوجه الاختلاف
المقارنة مع دراسة فراحي فضيلة	كلاهما يستخدمان خوارزمية الغابة العشوائية وتحللان أهمية المتغيرات، ويستهدفان كشف نوع من أنواع الاحتيال المالي الالكتروني حيت دراستنا تكشف الاحتيال في المعاملات المالية بينما الأخرى تكشف الاحتيال ببطاقة الائتمان	تبرز دارستنا في تقييم شامل لمختلف مقاييس الأداء ومنحنيات التقييم بينما الدراسة الأخرى ركزت على مقاييس قليلة بالإضافة الى استخدامنا طريقة التحقق المتقاطع دي الخمس طيات بدل من التقسيم البسيط. إضافة الى تحقيق نتائج اعلى في مختلف المقاييس على سبيل المتال دراستنا حققت دقة كلية بلغت 95،8% بينما الأخرى حققت دقة 90% إضافة الى ان دراستنا استخدمت برمجية(Orange) بينما الأخرى اعتمدت بايثون ومكتباته.
المقارنة مع دراسة علي بن الضب	كلاهما تستخدم بيانات اصطناعية محاكاة، وتهدفان الى اكتشاف الاحتيال على المعاملات المالية	ركزت دراستنا التطبيقية على تصميم انموذج بخوارزمية واحدة وهي الغابة العشوائية ودراستها بتعمق انطلاقا من تحليل شامل لمختلف المقاييس وأظهرت تفوقها العالي بينما الأخرى قارنت 4 خوارزميات تعلم الة دون تعمق في أي منها، كدلك قامت دراستنا بتحليل أهمية المتغيرات بينما الأخرى لم تتطرق لهدا التحليل، استخدمت دراستنا تقسيم بواسطة التحقق المتقاطع دي ال 5 طيات بينما الأخرى اعتمدت تقسيم بسيط. كما ان دراستنا استخدمت برمجية (Orange) بينما الأخرى اعتمدت بايثون ومكتباته.
المقارنة مع دراسة وسن هاشم كساب الكساسبة	كلاهما يؤكدان دور خوارزميات تعلم الالة في كشف الاحتيال المالي	اعتمدت دراستنا على بيانات اصطناعية وتصميم أنموذج عملي ينتج نتائج رقمية قابلة للقياس، بينما الأخرى اعتمدت على استبانة وهدا فرق جوهري بين الدراسة العملية والدراسة النظرية حيت دراستنا لم تعتمد على عينة بشرية ولا تعاني من التحيز وتعتمد على نتائج كمية وموضوعية قابلة لتحقق والقياس بالإضافة الى استخدام برنامج برمجي (Orange)

مقارنة الدراسة الحالية مع الدراسات العربية، من اعداد الطالبة بالاعتماد على الدراسات السابقة

الفرع الثاني: المقارنة بين الدراسة الحالية والدراسات الأجنبية.

تتلخص اهم الفروقات بين دراستنا والدراسات الأجنبية من خلال الجدول التالي:

المقارنة	أوجه التشابه	أوجه الاختلاف
دراسة Ganesh Khekare، et al ،2025 الهند	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية يستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات وبيانات من منصة (kaggle)	دراستنا تركز على خوارزمية واحدة بعمق بدلا من المقارنة بين 6 خوارزميات بالإضافة الى انها تعطي تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس MCC ومنحنيات الأداء ومخطط المعايرة و محنى ROC، كما اننا اعتمدنا على برنامج (Orange) بينما الأخرى اعتمت على python، دراستنا حققت تفوق عالي في جميع المؤشرات التقييم مقارنة بنتائج الدراسة الأخرى، وحللت أهمية المتغيرات، واستخدمت تقسيم التحقق المتقاطع بدلا من التقسيم البسيط.
دراسة Paschal Alumona et al ، 2025، الولايات المتحدة الامريكية	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية يستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات وبيانات اصطناعية محاكاة من منصة (kaggle)	دراستنا حققت نتائج ممتازة بمنهجية مباشرة الاعتماد خوارزمية الغابة العشوائية والتحقق المتقاطع بينما الأخرى استخدمت اطارا هجينا معقدا (k-means+RFM+هندسة الميزات + 4 خوارزميات) ومع ذلك حققت شجرة القرار أفضل أداء وليس خوارزمية الغابة العشوائية، بالإضافة الى دراستنا تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس MCC ومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت (python)
دراسة، Hongfang Zhoua، et al 2025، الصين	كلاهما يهدفان الى كشف الاحتيال المالي ويستخدمان بيانات اصطناعية محاكاة من منصة (kaggle)	دراستنا استخدمت خوارزمية واحدة وحققت نتائج ممتازة بينما الأخرى استخدمت نموذجا عميقا معقدا (RNN−LTSM الهجين) مع استراتيجية أخذ عينات متعددة (Smot،Adasyn، NearMiss) الا ان دراستنا حققت نتائج مرتفعة مقارنة بنتائجها، بالإضافة الى انها تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس (MCC) ومنحنيات الأداء ومخطط المعايرة ومحنى (ROC) وكدلك تحديد أهمية المتغيرات، كما اننا اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت (python).
دراسة C. Mallesha ،M . Hymavathi ،2024، الهند	كلاهما تؤكد دور خوارزميات وتقنيات تعلم الالة والذكاء الاصطناعي في كشف الاحتيال المالي على الأساليب التقليدية.	دراستنا تطبيقية عملية ام الأخرى فهي دراسة مرجعية، حيت تقدم دراستنا تصميم انموذج عملي وتقييمه بمقاييس تقييم شاملة ومنحنيات بينما الاخرى مجرد مراجعة شاملة لنتائج الأبحاث السابقة التي تثبت دور تقنيات تعلم الالة في كشف الاحتيال المالي دون أي تطبيق عملي او نتائج جديدة وهي عبارة عن تجميع لما هو موجود.
دراسة Sagar Bharat Shah ،2024،	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية	دراستنا تستخدم بيانات اصطناعية محاكاة بينما الأخرى تستخدم بيانات حقيقية لحاملي بطاقات ائتمان أوروبيين، دراستنا استخدمت 4 خوارزمية واحدة و حققت نتائج ممتازة بينما الأخرى استخدمت

الولايات المتحدة الامريكية	يستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات	خوارزميات تعلم الة و تقنية موازنة البيانات (Smot) بالإضافة الى اعتمادها تقسيم بسيط 70−30 بينما دراستنا استخدمت التقسيم المتقاطع دي الخمس طيات ، كما ان دراستنا حققت نتائج مرتفعة مقارنة بنتائجها، بالإضافة الى انها تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس (MCC) ومنحنيات الأداء ومخطط المعايرة ومحنى (ROC) وكدلك تحديد أهمية المتغيرات، كما اننا اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت (python).
دراسة Nadia Husnaningtyas، Totok Dewayanto 2023، أندونيسيا،	كلاهما تهدف الى اتبات دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني.	دراستنا تطبيقية عملية ام الأخرى فهي دراسة مرجعية، حيت تقدم دراستنا تصميم انموذج عملي وتقييمه بمقاييس تقييم شاملة ومنحنيات بينما دراستهم مجرد مراجعة شاملة لنتائج الأبحاث السابقة التي تثبت دور تقنيات تعلم الالة في كشف الاحتيال المالي دون أي تطبيق عملي او نتائج جديدة وهي عبارة عن تجميع لما هو موجود. وتحليل لا بحات سابقة. تتناول خوارزميات التعلم الغير خاضع للاشراف بينما دراستنا ركزت على خوارزمية الغابة العشوائية تطبيقيا.
دراسة Sonjoy Ranjon Das، Antigoni Kruti .et al 2023،، إنجلترا،	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات وبيانات اصطناعية محاكاة من منصة (kaggle) كشف الاحتيال	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 6 خوارزميات دون تعمق، كما ان نتائج دراستنا مرتفعة بكتير مقارنة مع نتائج الأخرى، بالإضافة الى دراستنا تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس MCCومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج Orangeبينما الأخرى على اعتمدت python
دراسة Palak Gupta ،Anmol varshney ،et al 2023، الهند،	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان بيانات اصطناعية محاكاة من منصة (kaggle)	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 4 خوارزميات دون تعمق، بالإضافة الى انها استخدمت تقنية موازنة البيانات بينما دراستنا لم تعتمدها وتناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس (MCC) ومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات واستخدمت الية التحقق دي 5 طيات بدلا من التقسيم البسيط، اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت python
دراسة M. A. Thinesh، S. S. Mukhil	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان خوارزمية الغابة العشوائية ضمن	حجم بيانات دراستنا المستخدمة في تصميم أنموذج دراستنا بلغت 50000 معاملة بينما هم استخدموا بيانات ذات 7231 معاملة فقط كما ان نتائج دراستنا مرتفعة بكثير مقارنة مع نتائج الأخرى، بالإضافة الى دراستنا تناولت تحليل شامل لمختلف المقاييس بينما

Varmann .et al ، ، 2023 ،الهند	الخوارزميات وبيانات اصـــطناعية محاكاة من منصة (kaggle)	الأخرى تجاهلت العديد منها متل مقياس MCCومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج Orangeبينما الأخرى على اعتمدت pythonواعتمدت الأخرى على التقسيم البسيط بينما دراستنا على التقسيم دي ال 5 طيات.
دراسة Shahnawaz Khan، Abdullah Alourani،et al ،2022،المملكة العربية السعودية	كلاهما يهدفان الى كشـــف الاحتيال في المعاملات المالية ويســـتخدمان بيانات اصـــطناعية محاكاة من منصةkaggle	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 3 خوارزميات دون تعمق، كما ان نتائج دراستنا مرتفعة بكثير مقارنة مع نتائج الأخرى، بالإضافة الى دراستنا تناولت تحليل شـــامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس MCCومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج Orangeبينما الأخرى على اعتمدت pythonواعتمدت الأخرى على التقسيم البسيط بينما دراستنا على التقسيم دي ال 5 طيات. بالإضـــافة الى ان الأخرى اســـتخدمت تقنية موازنة البيانات بينما دراستنا لم تعتمدها.
دراسة Rejwan Bin Sulaiman، Vitaly Schetinin، Paul Sant ، 2022 ، بريطانيا	كلاهما تهدف الى كشـــف الاحتيال المالي الالكتروني بواسطة خوارزميات تعلم الالة.	اعتمدت دراســـتنا على بيانات اصـــطناعية محاكاة لمعاملات مالية بينما الأخرى اعتمد على بيانات حقيقية تخص بطاقات الائتمان من بنوك اوروبية واســـترالية والمانية وصـــينية، كما انها اجرت تحليلا لدراسـات السـابقة حول كشـف الاحتيال ببطاقات الائتمان واعتمدت على نموذج هجين يجمع بين خوارزمية الشـــبكة العصـــبية و اطار التعلم الاتحادي و تقنية معالجة توازن البيانات ، بينما دراستنا ركزت بعمق على خوارزمية واحدة ، بينما اظهر نموذج الدراســـة الأخرى دقة كلية بلغت 99،96% بينما نموذجنا حقق دقة بلغت 95،8% الا ان دراسـتنا تناولت تحليل شـامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس MCCومنحنيات الأداء ومخطط المعايرة ومحنى ROC وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنـامج Orangeبينمـا الأخرى على اعتمـدت pythonواعتمـدت الأخرى على التقسـيم البسـيط بينما دراسـتنا على التقسـيم دي ال 5 طيات.
دراسة Pratyush Sharma، Souradeep Banerjee،et al ،2021،الهند	كلاهما يهدفان الى كشـــف الاحتيال في المعاملات المالية ويســـتخدمان خوارزمية الغابة العشـــوائية ضـــمن الخوارزميات وبيانات اصـــطناعية محاكاة من منصة (kaggle)	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 4 خوارزميات دون تعمق، كمان نتائج دراســـتنا مرتفعة بكثير مقارنة مع نتائج الأخرى، بالإضافة الى دراستنا تناولت تحليل شـــامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس (MCC) ومنحنيات الأداء ومخطط المعايرة ومحنى (ROC) وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج

		(Orange) بينما الأخرى على اعتمدت (python) واعتمدت الأخرى على التقسيم البسيط بينما دراستنا على التقسيم دي ال 5 طيات. بالإضافة الى ان الأخرى استخدمت تقنية موازنة البيانات بينما دراستنا لم تعتمدها
دراسة Vikas Thammanna Gowda ، 2021، الولايات المتحدة الامريكية	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات وبيانات اصطناعية محاكاة من منصة (kaggle)	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 6 خوارزميات دون تعمق، اظهر نموذج الدراسة الأخرى دقة كلية بلغت، 98 ،49% لخوارزمية SVMبينما نموذجنا حقق دقة بلغت 95،8% . دراستنا تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد منها متل مقياس (MCC) ومنحنيات الأداء ومخطط المعايرة ومحنى (ROC) وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت (python) واعتمدت الأخرى على التقسيم البسيط بينما دراستنا على التقسيم دي ال 5 طيات.
دراسة Matar Al Marri، Ahmad AlAli– دبي، 2020، الامارات العربية المتحدة	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات وبيانات اصطناعية محاكاة من منصة (kaggle) وكلاهما يستخدمان الية التحقق المتقاطع كلاهما اتبت ان انموذج خوارزمية الغابة العشوائية فعال في	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين خوارزميتين الغابة العشوائية والانحدار اللوجستي دون تعمق، دراستنا تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد وكدلك تحديد أهمية المتغيرات، اعتمادنا على برنامج (Orange) بينما الأخرى على اعتمدت (python)
، دراسة Fakhra Akhtar ، et al، 2020،باكستان	كلاهما يهدفان الى كشف الاحتيال في المعاملات المالية ويستخدمان خوارزمية الغابة العشوائية ضمن الخوارزميات ويستخدمان بيئة orange كلاهما اتبت ان انموذج خوارزمية الغابة العشوائية فعال في كشف الاحتيال	دراستنا ركزت بعمق على خوارزمية واحدة واظهرت اداءا مميزا بينما الأخرى قارنت بين 3خوارزميات دون تعمق، بيانات دراستنا من منصة (Kaggle) بينما الأخرى من مستودع (UCI) لتعلم الالة، دراستنا تناولت تحليل شامل لمختلف المقاييس بينما الأخرى تجاهلت العديد وكدلك تحديد أهمية المتغيرات. واعتمدت الأخرى على التقسيم البسيط بينما دراستنا على التقسيم دي ال 5 طيات.

المصدر: من اعدادا الطالبة بالاعتماد على الدراسات السابقة

خلاصة الفصل الاول:

يلخص الفصـــل الأول الإطار النظري لموضـــوع دور خوارزميات تعلم الالة في كشـــف الاحتيال المالي الالكتروني، وذلك من خلال التطرق الى ثلاثة مباحث، حيت تم في المبحث الأول عرض الإطار المفاهيمي للاحتيال المالي الالكتروني، وذلك من خلال التطرق الى ماهيته وخصـــائصـــه واركانه واهم اســـاليبه واتاره، إضـــافة الى ابراز قصـور الطرق التقليدية في الكشـف عنه امام التطورات الحديثة التكنولوجية. أما البحت الثاني فقد تخصـيصـه للإطار المفاهيمي لخوارزميات تعلم الالة ودورها في كشـــف الاحتيال المالي الالكتروني حيت تم اســـتعراض ماهية الذكاء الاصـــطناعي وتعلم الالـة واهم خوارزميـاتهمـا والية عملهـا وانواعهـا المختلفـة مع التركيز على الـدور الـدي تؤديـه خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني وتحسين أنظمة الحماية والإنذار المبكر داخل المؤسسات المالية. بينما في المبحث الثالث تم التطرق الى الدراسات السابقة العربية والأجنبية المتعلقة بموضوع الدراسة الحالية، ومن خلال عرض وتحليل أهم الدراســات التي تناولت تطبيق خوارزميات تعلم الالة في مجال كشـف الاحتيال المالي الالكتروني، ومع ابراز أوجه التشــابه والاختلاف بينها وبين الدراســة الحالية، مع ابراز أوجه التشــابه والاختلاف بينها وبين الدراسة الحالية. وبعد الالمام بمختلف بالجوانب النظرية الأساسية للموضوع والاطلاع على اهم الدراسات السابقة التي عالجت متغيرات الدراســات، تم التوصــل الى أهمية خوارزميات تعلم الالة باعتبارها من أحد التقنيات التي اثبت كفاءة ودقة عالية في كشـف المعاملات الاحتيالية والتنبؤ بها، الامر الذي سـاعد على تحديد منهجية الدراسـة وضـبط متغيراتها تمهيدا للانتقال الى الجانب التطبيقي الذي سيتم التطرق إليه في الفصل الثاني.

الفصل الثاني:

تصميم أنموذج خوارزمية تعلم الالة لكشف الاحتيال المالي الالكتروني

تمهيد

يهدف هذا الفصـــل الى الانتقال من الجانب النظري الى الجانب التطبيقي للدراســـة، وذلك من خلال تصـــميم انموذج عملي يعتمد على خوارزمية الغابة العشـــوائية للكشـــف عن عمليات الاحتيال المالي الالكتروني، باســـتخدام مجموعة بيانات جاهزة (Dataset) من منصة Kaggleبعنوان (Fraud detection Transactions Dataset) وهي مجموعة بيانات عالية الجودة تم توليدها بشكل اصطناعي (Synthetic) , بالاستعانة ببرنامج (Orange).

يتضـمن هدا الفصـل عرضـا شـاملا لمختلف المراحل التطبيقية، التي تم اتباعها في الدراسـة، بداءات من جمع البيانات والتحليل الاســتكشــافي من غير معالجة عدم توازن البيانات للتمثيل الواقعي لســيناريو الاحتيال المرتفع في المعاملات المالية الالكترونية تم اختيار خوارزمية الغابة العشـوائية وضـبط معلماتها وتدريبه وصـولا الى تقييم الأداء وتفسير النتائج النهائية.

وقد تم تقسـيم هذا الفصـل الى مبحثين رئيسـين: المبحث الأول يخصـص للإطار المنهجي للدراسـة التطبيقية، بينما يتناول المبحث الثاني الجانب التطبيقي لبناء النموذج وتقييمه.

المبحث الأول: منهجية الدراسة التطبيقية ومراحل بناء انموذج خوارزمية التعلم الالي

يتناول هذا المبحث الجانب المنهجي الدي تقوم عليه الدراسة التطبيقية، حيث سيتم عرض مجتمع وعينة الدراسة ومصدر البيانات، وأسباب اختيارها، إضافة الى عرض متغيرات الدراسة، والتعرف على بيئة العمل البرمجية (Orange data mining)، تم تقديم المراحل النظرية العامة لبناء أنموذج خوارزمية تعلم الالة التي تشكل الأساس العلمي للدراسة.

المطلب الأول: مجتمع وعينة الدراسة.

يتناول هدا المطلب تحديد مجتمع الدراسة، وعينة الدراسة المختارة بطريقة قصدية ومصدرها، مع ايراد الأسباب التي دعت الباحثة الى اختيار هده البيانات تحديدا.

- **أولا: مجتمع الدراسة:** يتكون مجتمع الدراسة من جميع المعاملات المالية الالكترونية (بطاقات اءتمان، محافظ الكترونية، تحويلات بنكية) التي قد تكون عرضة لعمليات الاحتيال.
- **ثانيا: عينة الدراسة:** تم اختيار عينة الدراسة بطريقة قصدية (purposive Sampling) حيت تم تحميل مجموعة البيانات المحددة من منصة (Kaggle) بعنوان (Fraud detection Transactions Dataset) وهي بيانات اصطناعية (Synthetic)عالية الجودة صممت لمحاكاة أنماط المعاملات المالية المعاصرة وتعكس مختلف خصائصها تخص معاملات سنة 2023 تتكون العينة من 50000معاملة مصرفية
- **ثالثا: اسباب اختيار عينة الدراسة (بيانات اصطناعية محاكاة عالية المخاطر):**

  - **عدم إمكانية الحصول على بيانات حقيقية:** لكشف الاحتيال المالي وبناء نماذج بالاعتماد عليها بسبب السرية المصرفية.
  - **بيانات اصطناعية مصممة خصيصا لكشف الاحتيال المالي الالكتروني:** صممت هده البيانات بشكل اصطناعي لتكون مثالية لمشكلات التصنيف الثنائي في مجال كشف الاحتيال.
  - **توفر العينة على جميع المتغيرات المطلوبة لتحقيق اهداف الدراسة:** حيت تضم 20 ميزة تغطي جوانب متعددة (مالية، جغرافية، سلوكية) مما يحقق الاهداف ويزيد من قدرة النموذج على التعلم.
  - **حجم العينة المناسب:** الدي يكفي لتدريب واختبار النموذج بموثوقية.
  - **تتمتع بدرجة عالية من التنظيم والجودة:** أظهرت عملية الفحص الاولي لمجموعة البيانات انها تتمتع بدرجة عالية من التنظيم، كونها بيانات اصطناعية مهيأة مسبقا لأغراض بناء نماذج كشف الاحتيال المالي الالكتروني. ولم تسجل مشكلات جوهرية او أخطاء هيكلية، لذلك اقتصرت عملية المعالجة المسبقة على فحص سلامة البيانات وتحديد المتغيرات والتحليل الوصفي لها.

- **حداثة البيانات:** معاملات مالية تخص سنة 2023، مما جعلها قريبة جدا من أنماط الاحتيال المعاصرة.
- **بيئة احتيال واضحة:** ان البيانات المختارة لتصميم أنموذج الدراسة تعكس بيئة احتيال مرتفعة بالمقارنة مع الكثير من البيانات المتاحة في منصة (Kaggle) التي قد تبلغ فيها نسبة 1%حيت بلغت نسبة الاحتيال في البيانات المختارة للدراسة نسبة 32،13% وذلك بهدف اختبار قدرة انموذج الدراسة في ظروف احتيال واضحة.

المطلب الثاني: متغيرات الدراسة والفحص الاولي للبيانات

يتناول هدا المطلب تحديد المتغير التابع والمتغيرات المستقلة لبيانات الدراسة التطبيقية واجراء الفحص الاولي لها حيت تتكون عينة البيانات المسماة ب (Fraud detection Transactions Dataset) المحملة من منصة (Kaggle) من 50000 معاملة مصرفية موصوفة ب 21 سمة (عمودا) منها خاصية تابعة واحدة و 18 خاصية مستقلة.

وتشمل متغيرات الدراسة:

- **المتغير التابع:** عمود (Fraud Label) متغير تنائي الفئات:
- 0: معاملة سليمة (Non-Fraud)
- 1: معاملة احتيالية (Fraud)
- **المتغيرات المستقلة:** وتشمل 18 خاصية سنبرزها في التالي.

يوضح الجدول الموجود في الأسفل ادناه وصفا لمجموعة بيانات المعاملات الاحتيالية، والتي تتضمن بيانات شاملة عن المعاملات المصرفية لحسابات العملاء للكشف عن الأنشطة الاحتيالية. حيت تتكون مجموعة البيانات التي تم جمعها من الميزات الثمانية التالية بكل ميزة مجموعة من الخصائص كما هو موضح فيما يلي:

1. المعرفات (Identifiers)

- Transaction_ID
- User_ID

2. معلومات المعاملة Transaction Info

- Transaction – Amount
- Transaction – Type
- Timestamp
- Merchant – Category
- Is – Weekend

3. معلومات الحساب والبطاقة Account & Card Info

- Account – Balance
- Card – Type
- Card – Age

4. معلومات الجهاز والوصول Device & Access Info

- Device – Type –
- IP – Address – Flag –
- Authentication – Method –

5. معلومات الموقع الجغرافي Location Info

- Location –
- Transaction — Distance –

6. الميزات السلوكية والإحصائية Behavioral & Statistical Features

- Daily – Transaction – Count –
- Avg – Transaction – Amount -7 d –
- Failed – Transaction – Count -7 d –
- Previous – Fraudulent – Activity –

7. متغير المخاطرRisk Variable

- Risk – Score –

8. المتغير الهدف Target

- Fraud –Label –

الجدول رقم 02-16: وصف خصائص بيانات الدراسة التطبيقية

الخاصية	الوصف
Transaction_ID	معرف فريد لكل معاملة
User_ID	معرف فريد للمستخدم
Transaction – Amount	مبلغ المعاملة
Transaction – Type	نوع المعاملة (اونلاين، المتجر، ATM.....)
Timestamp	تاريخ ووقت المعاملة
Merchant – Category	نوع التاجر (تجزئة، طعام، سفر .....)
Is – Weekend	هل المعاملة في عطلة نهاية الأسبوع؟
Account – Balance	رصيد الحساب قبل المعاملة
Card – Type	نوع البطاقة (ائتمانية، خصم، مدفوعة مسبقا ....)
Card – Age	عمر البطاقة بالأشهر
Device – Type	نوع الجهاز المستخدم (موبايل، حاسوب، ....)
IP – Address – Flag	هل عنوان IPمشبوه؟ تاخد القيم 0 او 1
Authentication – Method	طريقة المصادقة (PIN، بيو مترية، .....)
Location	الموقع الجغرافي للمعاملة
Transaction — Distance	المسافة بين الموقع المعتاد وموقع المعاملة

Daily – Transaction – Count	عدد المعاملات في اليوم
Avg – Transaction – Amount -7d	متوسط مبلغ المعاملات خلال 7 أيام
Failed – Transaction – Count -7 d	عدد المعاملات الفاشلة خلال 7 أيام
Previous – Fraudulent – Activity	عدد حالات الاحتيال السابقة للمستخدم
Risk – Score	درجة خطر الاحتيال المحسوبة للمعاملة
Fraud -Label	المتغير الهدف 0 احتيال 1 عدم احتيال

المصدر :من اعداد الطالبة بالاعتماد على منصة (kaggle) https://www.kaggle.com/datasets/samayashar/fraud-detection-transactions-dataset تاريخ الاطلاع 2026/4/3

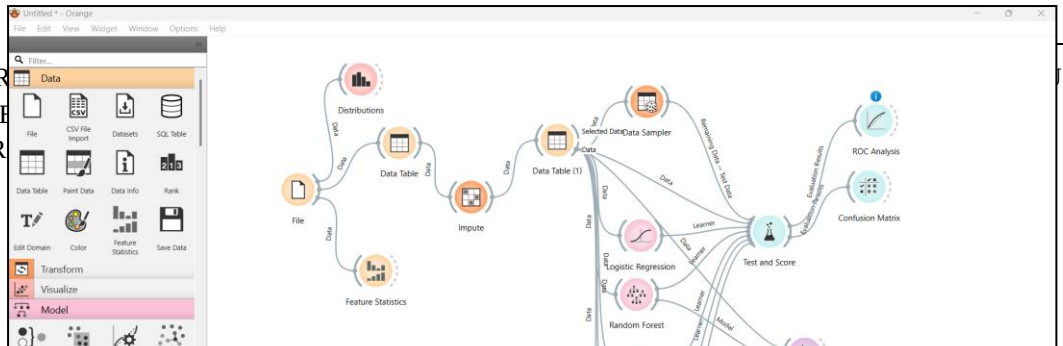
المطلب الثالث: تعريف بيئة العمل البرمجية (Orange Data Mining) وأسباب اختيارها

يتم في هدا المطلب عرض البيئة العملية التي اعتمدت عليها الدراســـة في الجانب التطبيقي، والمتمثلة في برنامج (Orange)، من خلال تعريفه، وذكر أسباب اختياره.

الفرع الأول: تعريف البيئة البرمجية (Orange data mining)

لقد قمنا في هده الدراســة التطبيقية باســتخدام برنامج (Orange data mining) بإصــدار (orange3.38) وهو برنامج لتعلم الالة مفتوح المصدر، مخصصة لتحليل البيانات وتصورها، وتدعم عمليات التنقيب عن البيانات من خلال البرمجة المرئية، مع إمكانية استخدام البرمجة النصية عبر لغة Python. يضم البرنامج مجموعة واسعة من خوارزميات تعلم الالة، الى جانب إضافات متخصصة في المعلوماتية الحيوية واستخراج النصوص وتحليل البيانات، توفر هده المنصة بيئة متكاملة تساعد الباحثين على تنفيذ مراحل المعالجة المسبقة للبيانات وتمثيلها بصريا باستخدام الرسوم البيانية ، وتطبيق نماذج تعلم الالة المختلفة، إضافة الى اختبار أداء الخوارزميات وقياس دقتها على مجموعة بيانات متعددة، وتســـتعمل في علم البيانات لتجريب خوارزميات جديدة وتطوير تقنيات حديثة في التحليل الذكي للبيانات، بالإضافة الى استخدامه في النمذجة التنبؤية وأنظمة التوصية وتصميم التجارب.[130]

الشكل رقم 02 -30: واجهة المستخدم البرمجية المرئية لبرنامج (Orange)



[130] FAKHR... USING ORANGE... RESEAR...

المصدر : برنامج (Orange)

الفرع الثاني: أسباب اختيار (Orange) كبيئة عمل برمجية للدراسة التطبيقية

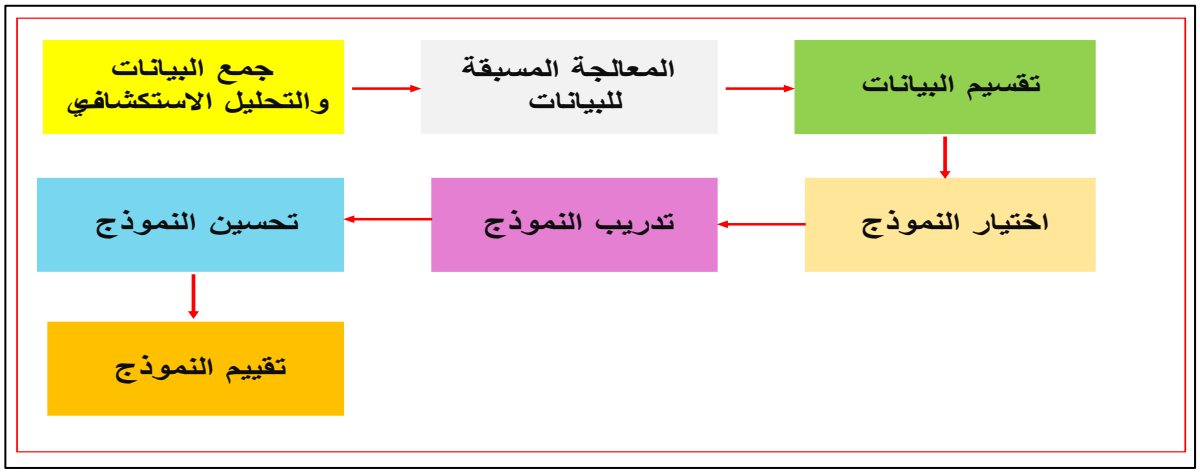
- **توفير واجهة مستخدم رسومية فعالة:** يتمتع البرنامج بمستوى عالي من التفاعل مع المستخدم وتحليل النتائج حيت تمكن المستخدم من اختيار الخوارزميات المختلفة، تقييم اداءها، عرض النتائج بصريا من خلال الرسوم البيانية، مما يدعم دقة التحليل واتخاد القرار.
- **مفتوح المصدر وقابل للتطوير:** يتيح البرنامج للمستخدمين الوصول المجاني الى مختلف وظائفها، مع إمكانية تطويرها والاستفادة من الإضافات والتحديثات المتاحة.
- **اعتماده على الوحدات الوظيفية (widgets)** : يعتمد البرنامج على مجموعة من المكونات الوظيفية التي يتم ربطها فيما بينها لإنشاء سير عمل متكامل (workflow) لتحليل البيانات وتطبيق خوارزميات تعلم الالة بطريقة فعالة و منظمة .[131]
- **دعم البرمجة المرئية و البرمجة بلغة بايثون:** يتيح البرنامج تحليل البيانات اما عبر برمجة نصية او من خلال واجهة المرئية الرسومية .
- **دعم خاصية السحب والافلات:** تسمح هده الخاصية للمستخدم ببناء نماذج العمل وربط الوحدات الوظيفية المختلفة من خلال السحب والافلات[132].

[131] AHMAD ABUASHOUR, ET AL, COMPARATIVE STUDY OF CLASSIFICATION MECHANISMS OF MACHINE LEARNING ON MULTIPLE DATA MINING TOOL KITS, AMERICAN JOURNAL OF BIOMEDICAL SCIENCE & RESEARCH, VOL 22, N 1,ISSN :2642 -1747,4 /2024, P34 -35

[132]MOHAMMED MAABDEH, RUBA OBIEDAT, DEVELOPING A MODEL TO PREDICT DEFAULTING CREDIT CARD CLIENTS USING BUSINESS INTELLIGENCE TECHNIQUES, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON ADVANCED RESEARCH IN MANAGEMENT BUSINESS AND FINANCE, Vol. 1, ISSUE. 1, 2024 P34

المطلب الرابع : المراحل النظرية لتصميم أنموذج خوارزمية تعلم الالة

الشكل رقم 02 -31 : مراحل بناء انموذج خوارزميات تعلم الالة لكشف الاحتيال المالي الالكتروني



المصدر :من اعداد الطالبة بالاعتماد على:

GANESH KHEKARE, ET AL,A COMPREHENSIVE PERFORMANCE COMPARISON OF TRADITIONAL AND ENSEMBLE MACHINE LEARNING MODELS FOR ONLINE FRAUD DETECTION ,ARXIV PREPRINT ARXIV : , A COMPREHENSIVE PERFORMANCE :2509.17176 ,2025,P 3

الفرع الأول: جمع البيانات ((Data Collection والتحليل الاستكشافي ((Exploratory Data Analysis:

- **جمع البيانات** :ان البيانات تعد عنصرا أساسيا في أي مجال بحتي وفي مجال تعلم الالة على وجه الخصوص، حيث ان الحصول على بيانات خاصة تتعلق بالاحتيال المالي يعد امرا صعبا جدا، بسبب التردد في الكشف عن هدا النوع من البيانات في المؤسسات المالية، لما ينطوي عليه من مخاطر تتعلق بفقدان السمعة او انتهاك الخصوصية، لدلك يتم الاعتماد على بيانات ثانوية متاحة للعموم، حيث تكون بيانات المعاملات الاحتيالية نادرة مقارنة بالبيانات المشروعة فيتم استخدام بيانات مولدة تتكون من بيانات واقعية تحاكي المعاملات الحقيقية ومصنفة الى بيانات احتيالية وأخرى مشروعة لتحسين قابلية التفسير وتجنب التحيز في النتائج وهي مزيج من المعرفة التقنية ومعرفة المجال التي تشمل اليات المعاملات المالية، وسلوكيات الانفاق، فتستخدم هده البيانات لإنشاء نموذج لكل عميل على حدة متل: الدخل، التوزيع الجغرافي ....الخ.[133]
- **التحليل الاستكشافي للبيانات**: تهدف الى فهم خصائص البيانات وطبيعتها عبر عرضها برسوم ومخططات بيانية بشكل اولي في واجهة Orange، نبدأ أولا باستيراد ملف متل EXEL،CSV عبر أداة Widget Fille، تم نستكشف متغيرات الدراسة وانواعها عبر أداة Data Table ونحصل على إحصائيات وصفية من حيث عدد القيم،

[133] MOHAMMED NAJIM UDDIN,FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS , OP CIT, P43

المتوسط، الانحراف المعياري، القيم الدنيا والعليا، إضافة الى التأكد من عدم وجود قيم مفقودة باستخدام، Info كما نرسم توزيعات المتغيرات عبر أداة Distributions ونحلل العلاقات فيما بينها .[134]

الفرع الثاني: المعالجة المسبقة للبيانات (Data pre-processing):

تنقسم المعالجة المسبقة للبيانات الى مرحلتين أساسيتين:

- **تنظيف البيانات ومعالجتها (Date Cleaining and Processing):** تهدف للتخلص من البيانات المكررة، تصحيح الأخطاء الإملائية ،إزالة الضجيج كذلك تشمل عملية معالجة القيم المفقودة وعملية تطبيع الميزات لتغيير مقياس البيانات الرقمية لتصبح جميعها في نطاق محدد لضمان عدم سيطرة ميزة ذات ارقام كبيرة على بقية الميزات بالإضافة الى تحويل البيانات النصية الى ارقام للتعامل معها الخوارزميات[135] حيت ان البيانات المتوفرة في المصادر الثانوية تكون غير متوازنة، لذلك يتم تحقيق التوازن قبل استخدامها، اما عن طريق زيادة عينات الفئة الأقل (oversampling) أو تقليل العينات الأكبر (Undersampling).
- **استخراج وهندسة الخصائص:** يعتبر استخراج الخصائص (Feature extraction) عنصرا مهما في تصنيف البيانات حيت في نماذج تعلم الالة التقليدية، يقوم خبراء المجال بإنشاء الخصائص يدويا، وتسمى هده العملية هندسة الخصائص (Feature engineering). اما في نماذج تعلم الالة الحديثة، فيتم استخراج الخصائص تلقائيا عبر مستويات مختلفة من التمثيل، مما يسمح بالتقاط خصائص غير خطية معقدة دون الحاجة لتدخل يدوي. كما يتم في بعض الاحيان استخدام طريقة توليد الخصائص العميقة (Deep Feature Synthesis) لاستخراج الخصائص من بيانات المعاملات الاحتيالية، وهي طريقة تلقائية لهندسة الخصائص تنتج خصائص قابلة للتفسير من طرف الانسان، على عكس نماذج تعلم الالة التي قد تنتج خصائص اقل قابلية للتفسير. وقد أظهرت هده الطريقة قدرتها على تقليل معدلات الإيجابيات الكاذبة (False positive rates)[136]

الفرع الثالث: تقسيم البيانات واختيار النموذج

أولا: تقسيم البيانات: تعد مرحة تقسيم البيانات خطوة أساسية في بناء نموذج تعلم الالة، حيت يتم عادة تقسيم البيانات بالطريقة التقليدية الى تلات مجموعات رئيسية: بيانات التدريب، بيانات الاختبار، وأحيانا بيانات تحقق او باستخدام أسلوب التحقق المتقاطع الدي يساعد على استغلال البيانات بشكل أفضل.[137]

---

[134] علي بن الضب، **دور الذكاء الاصطناعي وتعلم الالة في تعزيز كشف الاحتيال على البطاقات الاءتمانية**، مرجع سبق دكره، ص 28

[135] ANAVENA RAJKUMAR, MACHINE LEARNING TECHNIQUES FOR REAL-TIME FRAUD DETECTION IN FINANCIAL, LLOYD BUSINESS REVIEW, VOL 4, N1, P98

[136] MOHAMMED NAJIM UDDIN, FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS, OP CIT, p44

[137] ARIMONDO SCRIVANO, FRAUD DETECTION PIPELINE USING MACHINE LEARNING: METHODS, APPLICATIONS AND FUTURE DIRECTIONS, RESACHGATE, 7/2025, P 4 –5

ثانيا : اختيار النموذج: تتمثل مرحلة اختيار النموذج في العميلة التي يتم من خلالها اختيار خوارزمية من عدة خورزميات تعلم الة بهدف تحديد النموذج الأكثر ملاءمة لمشكلة كشف الاحتيال. ودلك بالاعتماد على اداءه وقدرته على التنبؤ، مع الاستفادة من مزايا وعيوب كل نموذج لاختيار الحل الأنسب.[138]

الفرع الرابع: تدريب النموذج وتحسينه

- **تدريب النموذج:** هي المرحلة التي يتم فيها تدريب النموذج التنبؤي لخوارزمية تعلم الالة على مجموعة بيانات سابقة تحتوي على معاملات طبيعية وأخرى غير طبيعية. بهدف تمكين النموذج من التعلم وتحسين قدرته على التمييز بين السلوكيات الاحتيالية والعادية.[139]
- **تحسين النموذج:** المرحلة التي يتم من خلالها ضبط المعلمات الفائقة وتجريب اعدادات مختلفة للنموذج بهدف اختيار أفضل تكوين يحقق اعلى أداء ممكن مع الحفاظ على قدرة النموذج عند تعميمه على بيانات مختلفة.
- **تقييم النموذج:** تتمثل مرحلة تقييم النموذج العملية التي يتم فيها اختبار النموذج أو النماذج المدربة باستخدام بيانات اختبار منفصلة لم تستخدم خلال مرحلة التدريب، وذلك بهدف قياس اداءها الحقيقي وقدرتها على التمييز بين المعاملات الاحتيالية والمعاملات الغير احتيالية ويتم هدا التقييم بالاعتماد على مجموعة من المقاييس الإحصائية المشتقة من مصفوفة الارتباك [140]ونذكرها فيما يلي:

1. مصفوفة الارتباك:

تعد مصفوفة الارتباك حجر الزاوية في هذه العملية التقييمية، من أجل قياس أداء النموذج بشكل دقيق من خلال المقارنة بين التوقعات التي يعطيها النموذج بالقيم الحقيقية مما يسمح بتحديد أنواع الأخطاء وقياس كفاءة النموذج بشكل دقيق ومفصل حيث يصنف بشكل منهجي الى 4 مكونات أساسية:

الشكل رقم 02 –32: مصفوفة الارتباك

		p	n
Hypothesized Class	Y	True Positives (TP)	False Positives (FP)
	N	False Negatives (FN)	True Negatives (TN)
	Column Totals:	P	N

[138] GANESH KHEKARE, ET AL, A COMPREHENSIVE PERFORMANCE COMPARISON OF TRADITIONAL AND ENSEMBLE MACHINE LEARNING MODELS FOR ONLINE FRAUD DETECTION, OP CIT, P 3

[139] VAISHNAVI NATH DORNADULA, GEETHA SA, CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS, PROCEDIA COMPUTER SCIENCE, Vol 165,2019, P636

[140]MOHAMMED NAJIM UDDIN, FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS, OP CIT, p49 -50

المصدر: دعاء المحيتاوي، وآخرون، نموذج محسن في مسالة كشف الاحتيال لبطاقات الائتمان باستخدام خورزميات تعلم الالة، منشورات المعهد العالي للعلوم التطبيقية والتكنولوجيا، دمشق، 2019/7، ص 3

- **True positive = (TP)** تعبر عن القيم الإيجابية المتوقعة بشكل صحيح
- **False Negative=(TN)** تعبر عن القيم السلبية المتوقعة بشكل صحيح
- **False positive=(FP)** تعبر عن القيم الإيجابية المتوقعة بشكل خاطئ
- **False Negative= (FN)** تعبر عن القيم الإيجابية المتوقعة بشكل خاطئ [141]

2.تستخدم هده الفئات في حساب مؤشرات الأداء الأساسية التالية:

جدول رقم 02 –17: مؤشرات قياس الأداء الأساسية لنماذج تعلم الالة

المؤشر	تعريفه	معادلته
الدقة الكلية (Classification Accuracy)	هي مقياس يعبر عن نسبة العينات التي تم تصنيفها بشكل صحيح سواء إيجابية او سلبية من اجمالي عدد العينات.	**Classification Accuracy**=(TP +TN)/(TP+TN+FP+FN)
الدقة الإيجابية (Precision)	هي مقياس يحدد مدى صحة التوقعات الإيجابية للنموذج، أي نسبة الحالات التي تم تصنيفها كإيجابية وكانت صحيحة فعلا.	**Precision** =(TP/TP+FP)
معدل الاستذكار (Recall)	هو مقياس يوضح قدرة النموذج على اكتشاف جميع الحالات الإيجابية الحقيقية الموجودة في البيانات.	**Recall**= (TP/TP+FN)
معامل F1–Score	هي مقياس يجمع بين الدقة الإيجابية والاستذكار في قيمة واحدة، وذلك من خلال استخدام المتوسط التوافقي بينهما لتحقيق توازن في التحقيق.	**F1–Score** =2. (Precision. Recall) /(Precision + Recall)
النوعية (Specificity)	هي مقياس يعبر عن قدرة النموذج على التعرف بشكل صحيح على الحالات السلبية الحقيقية.	**Specificity**=TN/(TP+TN)
معامل ارتباط ما تيوس: Matthews Corrélation Coefficient	هو مقياس احصاءي يستخدم لتقييم نمادج التصنيف التناءي، يتميز بانه يوفر تقييما متوازنا حتى في حالات اختلال توازن الفئات وتتراوح قيمه بين –1 تنبؤ معاكس تماما و+1 تطابق تام بينما تشير القيمة 0 الى تنبؤ عشواءي	**MCC**=(TP×TN−FP×FN) / [(TP+FP)(TP+FN)(TN+FP)(TN+FN)]

من اعداد الطالبة بالاعتماد على [142] [143]

[141] ARIMONDO SCRIVANO, FRAUD DETECTION PIPELINE USING MACHINE LEARNING: METHODS, APPLICATIONS AND FUTURE DIRECTIONS, RESACHGATE, OP CIT, P6

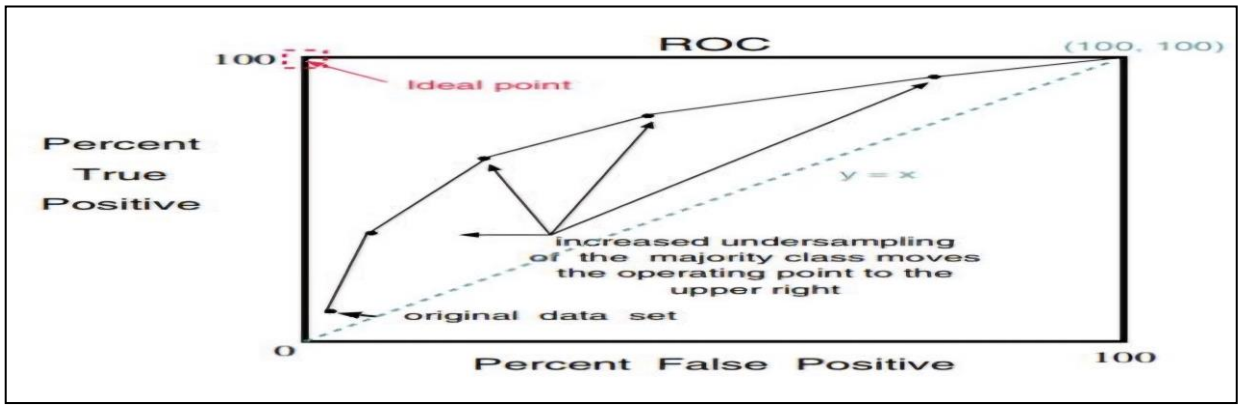
[142] علي لؤي ياسين، **استخدام طرائق التعلم الالي لاكتشاف الشذوذ في مجموعة البيانات**، مذكرة ماجيستير في هندسة البرمجيات ونظم المعلومات، مرجع سابق، ص 64 – 66

[143] JUN TAMURA, ET AL, STATISTICAL INFERENCE OF THE MATTHEWS CORRELATION COEFFICIENT FOR MULTICLASS CLASSIFICATION, ARXIV:2503.06450v1 [stat.ME] , 3/2025, P 2

3.الى جانب هده المقاييس الأساسية يتم استخدام المنحنيات التالية على نطاق واسع لتحليل شامل للأداء من بينها ما يلي:

(ROC Curve) منحنى خصائص تشغيل المستقبل هو منحنى بياني يستخدم لتقييم أداء النموذج من خلال تمثيل العلاقة بين معدل الإيجابية الصـــحيحة ومعدل الإيجابية الخاطئة عبر عتبات قرار مختلفة مما يســـمح بتحليل أداء النموذج في ظروف مختلفة.[144]

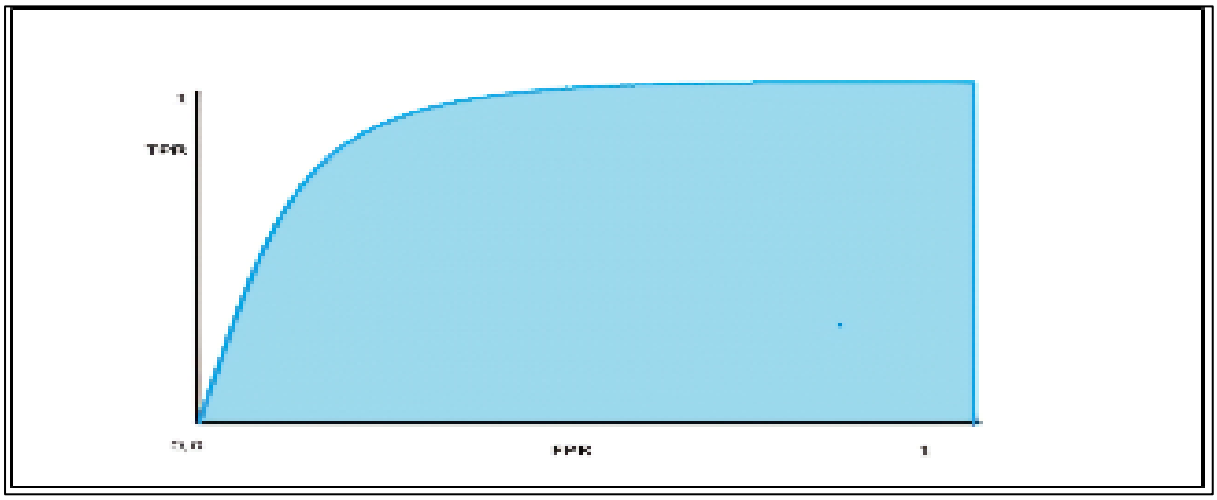
الشكل رقم 02- 33: منحنى ROC



المصدر: دعاء المحيتاوي، واخرون، نموذج محسن في مسالة كشف الاحتيال لبطاقات الائتمان باستخدام خورزميات تعلم الالة، مرجع سبق دكره، ص 4

2. (AUC–ROC): المساحة تحت منحنى خصائص تشغيل المستقبل: يمتل مقياسا عدديا يعبر عن الأداء العام للنموذج عبر جميع عتبات القرار، من خلال حساب المساحة تحت منحنى ROC [145]

الشكل رقم 02 -34: المساحة تحت منحنى خصائص تشغيل المستقبل



[144]ARIMONDO SCRIVANO, FRAUD DETECTION PIPELINE USING MACHINE LEARNING: METHODS, APPLICATIONS AND FUTURE DIRECTIONS, RESACHGATE, OP CIT, P6

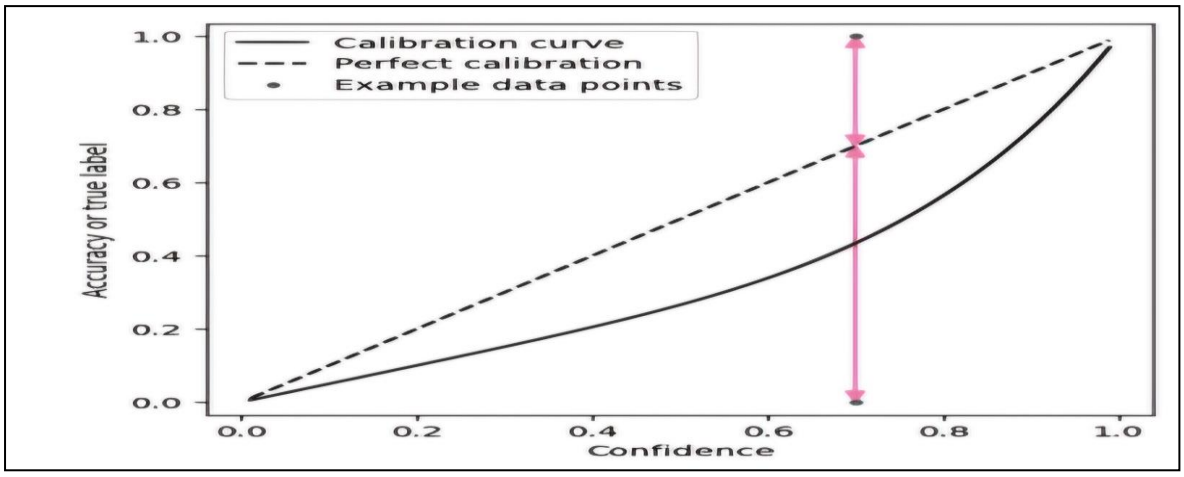
[145] ARIMONDO SCRIVANO, FRAUD DETECTION PIPELINE USING MACHINE LEARNING: METHODS, APPLICATIONS AND FUTURE DIRECTIONS, RESACHGATE, IBID, P6

المصدر:

MOHAMMED NAJIM UDDIN, FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS, OP CIT, p51

3. مخطط المعايرة (Calibration Plot):هو تمتيل بياني يوضـــح العلاقة بين الاحتمالات او درجات الثقه التي يتنبأ بها النموذج (على المحور الافقي) والنســـبة الفعلية للنتائج الإيجابية او التكرار الحقيقي لها (على المحور الراسي) مع مقارنته مع خط المعايرة المتالي الذي يمتل التوافق التام بين القيم المتوقعة والفعلية.[146]

الشكل رقم 02 –35: تمتيل نظري لمخطط المعايرة يوضح العلاقة بين الثقة المتوقعة والدقة الفعلية

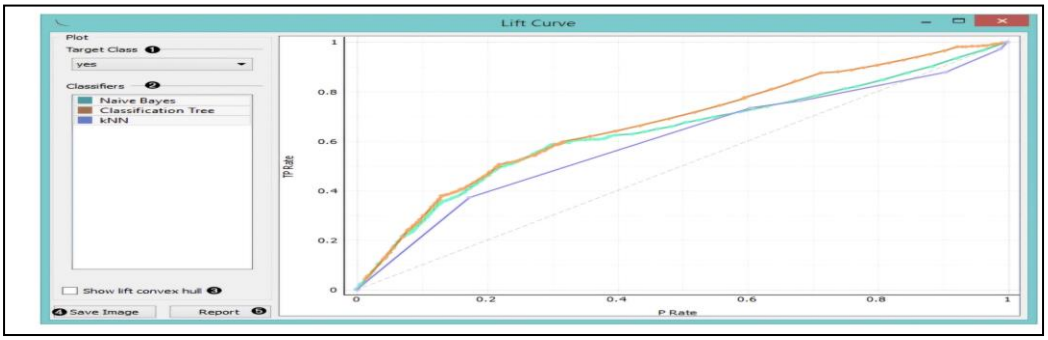


المصدر:

RICHARD OLIVER LANE, A COMPREHENSIVE REVIEW OF CLASSIFIER PROBABILITY CALIBRATION METRICS ,IBID ,P 4

4. منحنى الرفع (Lift curve) التابع لمنحنيات الأداء (Performance Curves): يعد منحنى الرفع أداة أساسية لتقييم الأداء، حيث يقيس المصـنف المختار مقابل المصـنف العشـوائي، يوضـح المنحنى العلاقة بين المعاملات المتوقعة الاحتيالية والمعاملات الاحتيالية الحقيقية المكتشفة، مما يساعد على مقارنة النموذج بمصـنف عشواءي وتحديد العتبة المثلى لزيادة اكتشاف الاحتيال وتقليل الإنذارات الخاطئة.[147]

الشكل رقم 02 -36: منحنى الرفع (Lift curve)



[146]RICHARD OLIVER LANE, A COMPREHENSIVE REVIEW OF CLASSIFIER PROBABILITY CALIBRATION METRICS ,ARIVEX:2504 .18278, 4/2025,P 4 -5

[147] الموقع الالكتروني , على الانترنت: ORANGE DATA MINING, WIDGET CATALOG متاح على الرابط https://orangedatamining.com/widget-catalog تاريخ الاطلاع 10 /3/ 2026

المصدر:

ORANGE DATA MINING, WIDGET CATALOG متاح على الرابط https://orangedatamining.com/widget-catalog / تاريخ الاطلاع 10 /4/ 2026

المبحث الثاني: التصميم الفعلي لأنموذج خوارزمية تعلم الالة (الغابة العشوائية) وتقييم اداءه.

يتناول هدا المبحث الجانب التطبيقي للدراسة من خلال التطبيق الفعلي لمراحل تصميم أنموذج الدراسة، على البيانات المختارة (Fraud detection Transactions Dataset) باستخدام برنامج (Orange) وادواته الوظيفية، وعرض خطوات سير العمل ومخرجاته، وذلك بهدف كشف الاحتيال وتحليل أداء أنموذج الدراسة عبر مؤشرات تقييم الأداء إضافة الى تحديد متغيرات بيانات الدراسة الأكثر تأثيرا في كشف الاحتيال .حيت تم الاعتماد في هذا المبحث على الأدوات الوظيفية لبرنامج (Orange Data Mining) الموضحة في الجدول ادناه والتي ساهمت في تنفيذ مختلف المراحل بشكل متسلسل ابتداء من جمع البيانات وصولا الى تقييم أداء النموذج.

الجدول رقم 02-18: الأدوات الوظيفية لبرنامج (Orange) المستخدمة في دراستنا التطبيقية

الأداة الوظيفية (widgets) المستخدمة في برنامج أورانج	وظيفتها في دراستنا التطبيقية
FILE	يقوم تحميل مجموعة البيانات Synthetic -Fraud Dataset .CSV من ملف CSVوقراءة بياناتها وقيمها وارسال مجموعة البيانات الى قناة الإخراج الخاصة بها بالإضافة الى الاحتفاظ بسجل لاحدث الملفات التي تم فتحها. وتحديد المتغير التابع Fraud –Label كفئة (Category)
Distribution	يعرض توزيعات القيم لسمة واحدة حيت يرسم توزيع المتغير التابع (معاملات سليمة 0/ معاملات احتيالية 1) للكشف عن عدم توازن البيانات.
Feature statistics	عرض الإحصائيات الوصفية للمتغيرات المستقلة (المتوسط، الانحراف المعياري، الحد الأدنى، الحد الأعلى، الوسيط ..... الخ)
Data table	يعرض بيانات السمة والقيمة في جدول بيانات للاطلاع على القيم الفعلية للمعاملات والمتغيرات كما تدعم هده الأداة التحديد اليدوي للبيانات.
Correlation	لعرض جميع الارتباطات بين متغيرات الدراسة.
Test & score	يختبر خوارزميات تعلم الالة على بيانات الدراسة وتقييم أداء النموذج حسب مقاييس الأداء كما تدعم الأداة طرق اخد العينات المختلفة حيت في دراستنا استخدامنا تقسيم عملية التحقق المتقاطع ب 5 طيات
Random Forest	بناء وتدريب نموذج الغابة العشوائية (Random Forest) وتحديد معلماته: عدد الأشجار، معيار التقسيم العمق...الخ
Confusion matrix	استخراج مصفوفة الارتباك لتحليل التنبؤات الخاطئة التنبؤات الصحيحة.
Roc analysis	رسم منحنى (Roc analysis) وحساب قيمة المساحة تحت المنحنى (AUC)

Performance curve	رسم منحنى الأداء (Precision –Recall Curve)
Calibration plot	رسم مخطط المعايرة لمقارنة الاحتمالات المتوقعة للنموذج مع التكرارات الفعلية للفئة الموجبة احتيال
Feature importance	تحديد اهم المتغيرات المستقلة المؤثرة في التنبؤ بالاحتيال وترتيبها تنازليا حسب مساهمتها.

المصدر :من اعداد الطالبة بالاعتماد علىOrange data mining، Widget Catalog متاح على الرابط https://orangedatamining.com

تاريخ الاطلاع 12 /4/ 2026

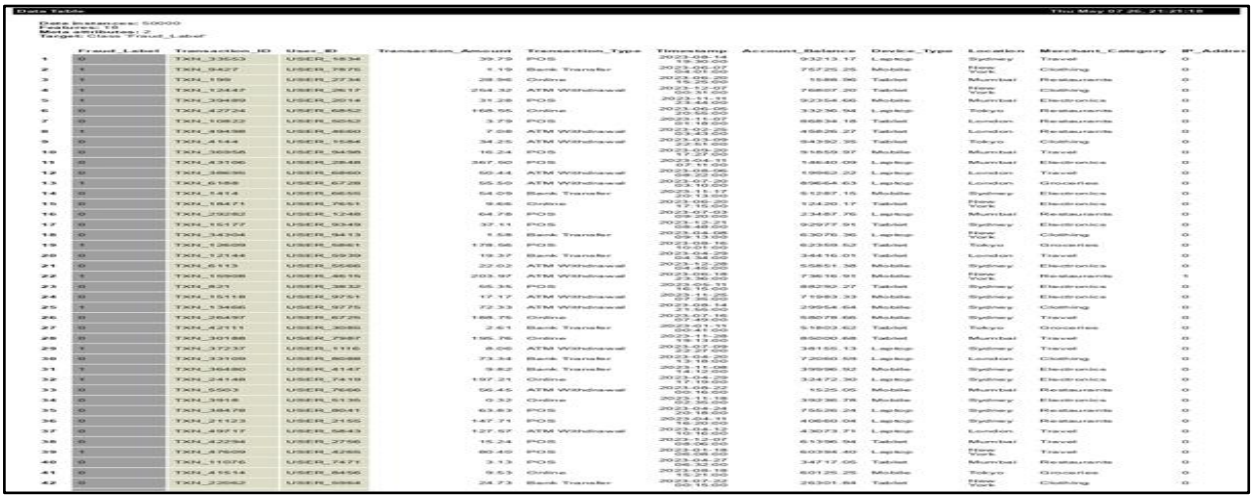
المطلب الأول: جمع البيانات والتحليل الاستكشافي لها.

يتضمن هدا المطلب المرحلة الأولى من عملية تصميم أنموذج خوارزمية الغابة العشوائية، حيت تعد من اهم مراحل الدراسة، يتم فيها جمع البيانات من مصدرها الأصلي تم تحليليها استكشافيا ووصفيا بهدف فهم خصائصها واكتشاف بنيتها الداخلية والتأكد من صلاحيتها قبل بناء أنموذج الدراسة.

الفرع الأول: العرض الاولي لمجموعة البيانات المستخدمة في الدراسة.

بعد عملية جمع بيانات الدراسة من منصة (Kaggle) قمنا بتحميلها في برنامج (orange data mining) عبر أداة (File) تم قمنا بعدها باستعراض البيانات الأولية عبر أداة (Data Table) والتعرف على خصائصها الأساسية قبل الشروع في بناء النموذج العملي، حيت تضم البيانات 50000 معاملة مالية بها 21 ميزة، و18 متغير مستقل بالإضافة الى المتغير الهدف (Fraud-Label) الدي يحدد ما اذا كانت المعاملة احتيالية ام لا .اظهر استعراض البيانات مجموعة من المتغيرات المهمة التي يمكن ان تؤثر في اكتشاف عمليات الاحتيال المالي الالكتروني، من بينها معرف المستخدم، قيمة المعاملة، نوع المعاملة، وقت تنفيذها، رصيد الحساب، نوع الجهاز المستخدم، الموقع الجغرافي بالإضافة الى مؤشرات أخرى مرتبطة بسلوك المعاملات المالية، حيت تم في هده المرحلة استعراض البيانات الأولية والتعرف على عدد السجلات والمتغيرات ونوع البيانات المستخدمة. بالإضافة الى ان بيانات الدراسة منظمة ولا تحتوي على قيم مفقودة او مشاكل هيكلية، كما يبينه الشكل الموالي:

الشكل رقم 02 –37: عرض اولي لمجموعة البيانات المستخدمة في الدراسة



المصدر : مخرجات برنامج (Orange)

الفرع الثاني: الإحصاءات الوصفية لمتغيرات بيانات الدراسة.

يوضح الشكل ادناه مجموعة من المؤشرات الإحصائية الوصفية، متل المتوسط الحسابي والانحراف المعياري والقيم الدنيا والعليا، مما يساعد على فهم خصائص المتغيرات الرقمية.

الشكل رقم: 02 -38 الإحصاءات الوصفية لمتغيرات الدراسة الخاصة بالبيانات المستخدمة

Feature Statistics — Thu May 07 26, 21:21:00

	Name	Distribution	Mean	Mode	Median	Dispersion	Min.	Max.	Missing
N	Transaction_Amount		99.4110	7.65	69.66	0.9927	0.00	1174.14	0 (0 %)
N	Account_Balance		50294.0660	639.34	50384.43	0.5718	500.48	99998.31	0 (0 %)
N	Daily_Transaction_Count		7.49	3	7	0.54	1	14	0 (0 %)
N	Avg_Transaction_Amount_7d		255.2719	82.26	256.0850	0.5538	10.00	500.00	0 (0 %)
N	Failed_Transaction_Count_7d		2.00	3	2	0.71	0	4	0 (0 %)
N	Card_Age		120.00	80	120	0.57	1	239	0 (0 %)
N	Transaction_Distance		2499.1642	951.92	2490.7850	0.5770	0.25	4999.93	0 (0 %)
N	Risk_Score		0.501556	0.6917	0.502250	0.573758	0.0001	1.0000	0 (0 %)
T	Timestamp		2023-07-02 12:47:11.064000	2023-06-04 06:35:00	2023-07-02 14:00:00	~11 months	2023-01-01 00:01:00	2023-12-31 23:50:00	0 (0 %)
C	Transaction_Type			POS		1.39			0 (0 %)
C	Device_Type			Tablet		1.1			0 (0 %)
C	Location			Tokyo		1.61			0 (0 %)
C	Merchant_Category			Clothing		1.61			0 (0 %)
C	IP_Address_Flag			0		0.199			0 (0 %)
C	Previous_Fraudulent_Activity			0		0.322			0 (0 %)
C	Card_Type			Mastercard		1.39			0 (0 %)
C	Authentication_Method			Biometric		1.39			0 (0 %)
C	Is_Weekend			0		0.611			0 (0 %)
C	Fraud_Label			0		0.628			0 (0 %)

المصدر: مخرجات برنامج Orange

– نقوم بتحليل وصفي شامل متغيرات الدراسة بالاعتماد على الشكل الموضح أعلاه في الجداول التالية:

أولا: التحليل الوصفي المتغيرات العددية:

الجدول رقم 02 –19: التحليل الوصفي للمتغيرات العددية

المتغير	التحليل والتفسير الوصفي للمتغيرات
مبلغ المعاملة	يتراوح المبلغ المنفق بين 0 و1174،14 وحدة نقدية ، بمتوسط حسابي بلغ 99،41 اعلى من الوسيط 69،66 مما يشير الى توزيع منحرف نحو اليمين أي وجود عدد محدود من المعاملات الكبيرة التي ترفع المتوسط، حيت بلغ معامل التشتت 0،9927 قريب من ال1 وهو دليل على تباين كبير جدا في قيم المعاملات وهده سمة شائعة في بيانات الاحتيال حيت تميل المعاملات الاحتيالية الى قيم غير اعتيادية مرتفعة او منخفضة جدا، بلغ المنوال 7،65 وهوما يعكس ان المعاملات الصغيرة هي الأكثر تكرارا، مما يفرض على خوارزميات تعلم الالة حساسية الكشف اتجاه القيم المتطرفة.
رصيد الحساب قبل المعاملة	بلغ المتوسط قيمة 50294 وهو قريب جدا من الوسيط 50384 مما يشير الى توزيع طبيعي في حين ان المنوال اقل بكثير حيت بلغ 639،34 مما يعني ان معظم الحسابات صغيرة الرصيد رغم وجود ارصدة ضخمة حتى 99998 في حين بلغ التشتت 0،75 مما يدل على ان الاحتيال قد يستهدف الحسابات الغنية او يحدث في حسابات صغيرة فجأة.
عدد المعاملات في اليوم	بلغ المتوسط قيمة 7،49، ووسيط 7، ومنوال بلغ 3، تشتت 0،54 الأغلبية أيام قليلة المعاملات، لكن وجود 14 معاملة يوميا يشير الى نشاط غير طبيعي (استنزاف سريع للحساب)
متوسط مبلغ المعاملات خلال 7 أيام	بلغ المتوسط 255،27، ووسيط بلغ 256،09 وهو ما يشير الى توزيع متماثل تقريبا في حين كان المنوال اقل 82،26 أي انحراف حاد عن متوسط العميل الأسبوعي يعتبر مؤشر احتيال.
عدد المعاملات في اليوم	بلغ المتوسط 2 والوسيط 2 والمنوال 3 مما يشير الى ان معظم الحالات لديها 3 معاملات فاشلة أسبوعيا في حين بلغ التشتت 0،71 وهو مرتفع نسبيا والمدى يمتد من 0 الى 4 حيت تشير قيمة 4 الى علامة خطر قوية.
عمر البطاقة بالأشهر	بلغ المتوسط 120 يوم، ووسيط 120 ومنوال 80، ومدى يمتد من 1 الى 239 يوم والتوزيع متماثل. وهوما يوضح ان البطاقات الجديد ذات عمر ال 1 يوم اكتر عرضة للاحتيال وذات 239 يوم مستقرة
المسافة بين الموقع المعتاد وموقع المعاملة	بلغ المتوسط 2499 كلم، ووسيط بلغ 2940، ومنوال بلغ 952 ومدى يمتد من 0،25 –5000 وتشتت بلغ 0،577 وهوما يدل على مسافات قصيرة جدا محلية وأخرى عابرة للانتقال، حيت ان الانتقال المفاجئ بين المسافات المتباعدة في زمن قصير يشير الى احتيال جغرافي.

درجة خطر الاحتيال المحسوبة للمعاملة	بلغ المتوسط 0،5016، ووسيط 0،5023 ومنوال بلغ 0،6917 وهو ما يشير الى توزيع شبه منتظم مناسب للتصنيف الثنائي. والمنوال اعلى من المتوسط مما يعني: ان معظم العينات تميل الى خطورة متوسطة –عالية.

المصدر :من اعداد الطالبة، بالاعتماد على الإحصاءات الوصفية للمتغيرات المستخرجة من برنامج Orange

- **متغير(Timestamp)**: هو متغير زمني يحدد فترة الدراسة الممتدة من 1 جانفي الى 31 ديسمبر 2023 ، بدقة زمنية تصل الى الثانية، ويستخدم في سياق البيانات من أجل استخراج متغيرات مساعدة متل الفارق الزمني بين المعاملات والساعة والشهر، وي متغيرات بالغة الأهمية في كشف الاحتيال الجغرافي والزمني.

ثانيا: التحليل الوصفي للمتغيرات الفئوية:

الجدول رقم 02 –20: التحليل الوصفي للمتغيرات الفئوية، من اعداد الطالبة، بالاعتماد على الإحصاءات الوصفية للمتغيرات المستخرجة من برنامج Orange

المتغير	القيمة	التحليل التفسير
نوع المعاملة	المتغيرات الفئوية: POS/Bank Transfer/Online/ATM Withdrawal القيمة الرقمية التشتت:1،39	القيمة تمثل متوسطا او نسبة بعد الترميز (مثلا :1 يعني نعم ،0 يعني لا) حيت تشير القيمة 1 الى ان استخدام POS المادي هو الغالب في العينة. دلالته في الاحتيال: ان المعاملات التي تمت عبر POS المادي اقل خطورة من المعاملات عبر الانترنت، لكنها ليست خالية من الاحتيال.
نوع الجهاز المستخدم	المتغيرات الفئوية: Laptop/Mobile /Tablet القيمة الرقمية التشتت:1،1	الجهاز اللوحي كوسيلة لإجراء المعاملة، القيمة قريبة من ال 1 تعني ان معظم المعاملات تمت عبر أجهزة لوحية، دلالته في الاحتيال: الأجهزة اللوحية قد تكون اقل امانا من الهواتف الذكية الحديثة مما يزيد خطر الاحتيال قليلا.
الموقع الجغرافي للمعاملة	المتغيرات الفئوية: Sydney /New York/Mumbai/London/ Tokyo/ القيمة الرقمية التشتت: 1،61	المتغير الجغرافي: هل المعاملة تمت في طوكيو؟ القيمة 1،61 قد تعني ان نسبة مرتفعة من المعاملات حدثت في طوكيو، دلالته في الاحتيال: ان المدن الكبرى تشهد معاملات اكتر وبالتالي احتيالا اكتر، لكن وجود معاملة من طوكيو تم من مدينة أخرى بفارق زمني قصير يعتبر علامة خطر.
نوع التاجر	المتغيرات الفئوية: Clothing/Restaurents/ Electronics /Gro cerise/Tavel القيمة الرقمية التشتت :1،61	فئة المنتج: ملابس، القيمة 1،61 مشابهة لطوكيو، وقد تعني الى ان الملابس هي الفئة الأكثر شيوعا. دلالته في الاحتيال: بعض فئات المنتجات متل: الالكترونيات وبطاقات الهدايا

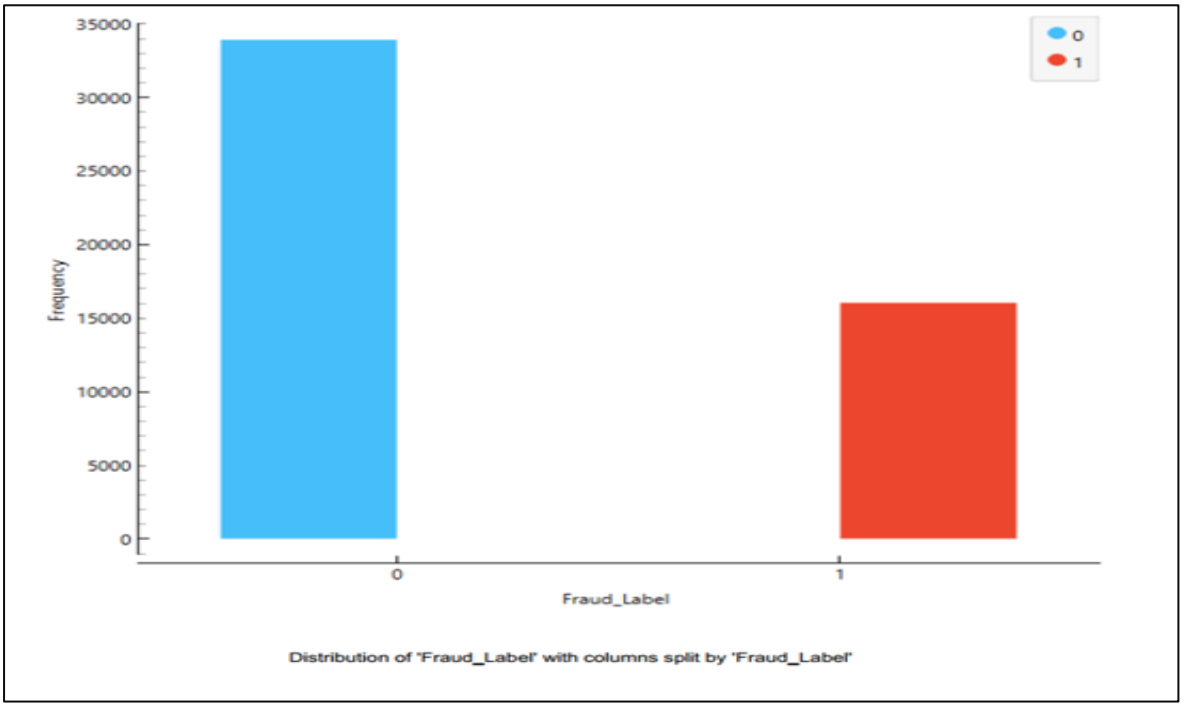
		تجدب المحتالين اكتر من الملابس لكن ارتفاع القيمة هنا قد يكون بسبب كترة المعاملات
هل عنوان IP مشبوه؟	المتغيرات الفئوية: القيمة 0 والقيمة 1 القيمة الرقمية التشتت: 0،199	القيمة 0 تعني غياب عناوين IP المشـــبوهة في هده العينة، دلالته في الاحتيال وجود علامة ال 1 يعتبر من اقوى مؤشرات الاحتيال، لكن غيابها لا يعني امانا مطلقا.
عدد حالات الاحتيال السابقة للمستخدم	المتغيرات الفئوية: 1,0 القيمة الرقمية التشتت: 0،322	القيمة 0،322 تعني وجود سـجل احتيالي سـابق للحسـاب او البطاقة في هده العينة بهذا التشـــتت، دلالته في الاحتيال: السـجل الاحتيالي السـابق يزيد احتمالية الاحتيال المسـتقبلي بشـــكل كبير (تكرار المحتالين)، لكن غيابه لا ينفي حدوت احتيال اولي.
نوع البطاقة	المتغيرات الفئوية: Visa،Mastercard /American Express القيمة الرقمية التشتت: 1،39	القيمة 1،39 يشـــير الى ان غالبية البطاقات من نوع بطاقة ماســـتر كارد، دلالته في الاحتيال: بطاقات الائتمان غالبا ما تكون اكتر استهدافا من بطاقات الخصم بسبب حدود الائتمان العالي وحماية المستهلك.
طريقة المصادقة	المتغيرات الفئوية: PIN / Biometric القيمة الرقمية تشتت :1،39	القيمة 39. 1 تمثل الطريقة الأكثر شـــيوعا ;وأنها الطريقة الغالبة متل (Pinاو التوقيع)، دلالته في الاحتيال: المصـــادقة البيو مترية: متل البصـــمة، الوجه، تقلل الاحتيال بشـكل كبير والقيمـة 1،39 هنـا قد تعني وجود البيو مترية مما يقلل من خطر الاحتيال.
هل المعاملة في عطلة نهاية الأسبوع؟	المتغيرات الفئوية: القيمة0 والقيمة 1 القيمة الرقمية التشتت: 0 .611	القيمة 0 تعني ان معظم المعاملات حدثت في أيام الأســبوع، دلالته في الاحتيال: بعض الدراســـات تشـــير الى ان زيادة الاحتيال في عطل نهاية الأسـبوع بسـبب ضـعف رقابة البنوك في هده العطلة، لكن العينة تظهر تركيزا على أيام الأسـبوع ولا معاملات في العطلة.

المصدر :من اعداد الطالبة، بالاعتماد على الإحصاءات الوصفية للمتغيرات المستخرجة من برنامج Orange

الفرع الثالث: توزيع المتغير المستهدف

يبين الشـــكل ادناه توزيع فئتي البيانات وفق متغير الهدف (Fraud-Label) حيت يوضـــح عدد العمليات الاحتيالية مقارنة بالعمليات السـليمة، مما يسـاعد في معرفة ما إذا كانت البيانات متوازنة او غير متوازنة قبل تدريب النموذج.

الشكل رقم 02 –39: توزيع المعاملات الاحتيالية والغير احتيالية لمجموعة البيانات المستخدمة

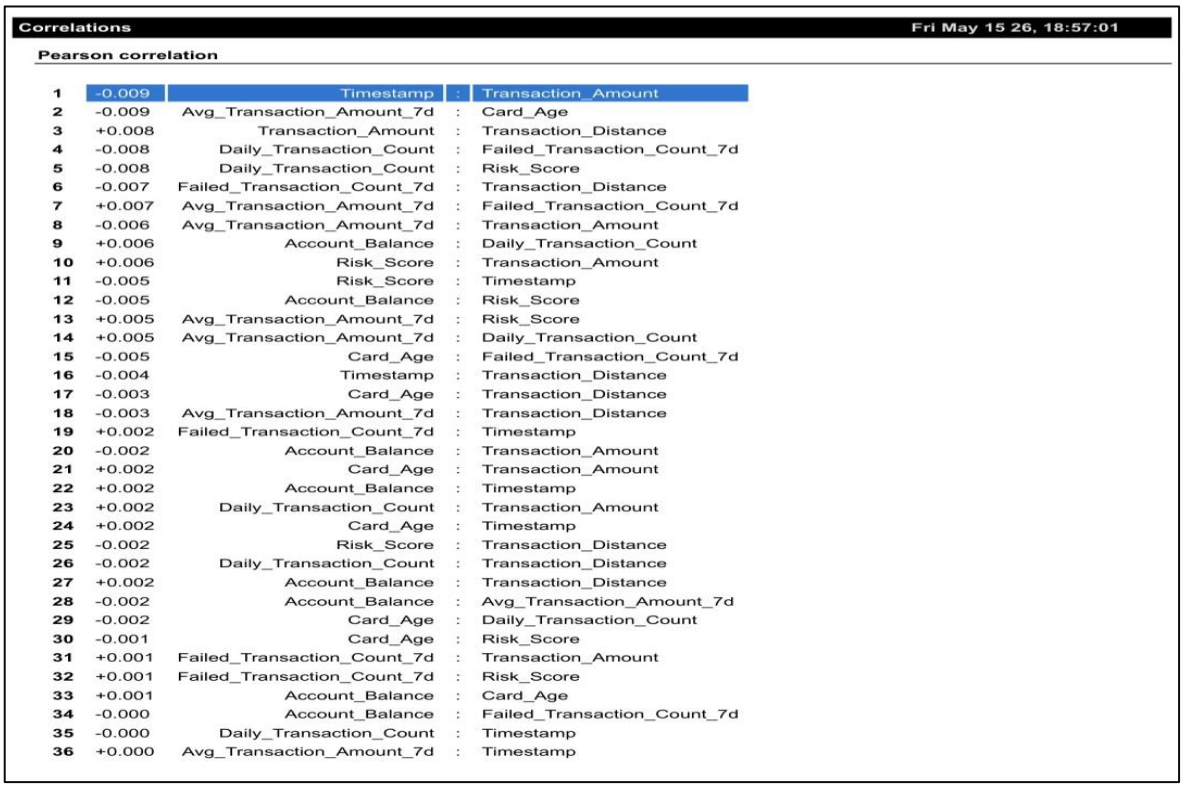


المصدر : مخرجات برنامج Orange

- نلاحظ من الشكل ان الخاصية (Label_Fraud) هي سمة تنائيه حيت يشير الرقم 0 الى معاملة غير احتيالية، بينما يشير الرقم 1 الى معاملة احتيالية، حيت يظهر توزيع المتغير المستهدف انه يوجد 33933 معاملة غير احتيالية بنسبة 67،87% و16067 معاملة احتيالية بنسبة 32،13%، حيت تمتل المعاملات الغير احتيالية النسبة الاكبر، ونظرا لان هذا التفاوت لم يكن حادا مقارنة ببيانات الاحتيال التي غالبا ما تكون اكتر عدما للتوازن، لم يتم تطبيق تقنيات معالجة التوازن، وتم الاعتماد على البيانات بصيغتها الاصلية في بناء أنموذج الدراسة، وهي معدة مسبقا في منصة (Kaggle) بصورة مناسبة لأغراض الدراسة.

الفرع الرابع: دراسة الارتباط بين متغيرات بيانات الدراسة

الشكل رقم 02–40: الارتباط بين متغيرات بيانات الدراسة، المصدر مخرجات برنامج (Orange)



Correlations — Fri May 15 26, 18:57:01

Pearson correlation

1	-0.009	Timestamp	:	Transaction_Amount
2	-0.009	Avg_Transaction_Amount_7d	:	Card_Age
3	+0.008	Transaction_Amount	:	Transaction_Distance
4	-0.008	Daily_Transaction_Count	:	Failed_Transaction_Count_7d
5	-0.008	Daily_Transaction_Count	:	Risk_Score
6	-0.007	Failed_Transaction_Count_7d	:	Transaction_Distance
7	+0.007	Avg_Transaction_Amount_7d	:	Failed_Transaction_Count_7d
8	-0.006	Avg_Transaction_Amount_7d	:	Transaction_Amount
9	+0.006	Account_Balance	:	Daily_Transaction_Count
10	+0.006	Risk_Score	:	Transaction_Amount
11	-0.005	Risk_Score	:	Timestamp
12	-0.005	Account_Balance	:	Risk_Score
13	+0.005	Avg_Transaction_Amount_7d	:	Risk_Score
14	+0.005	Avg_Transaction_Amount_7d	:	Daily_Transaction_Count
15	-0.005	Card_Age	:	Failed_Transaction_Count_7d
16	-0.004	Timestamp	:	Transaction_Distance
17	-0.003	Card_Age	:	Transaction_Distance
18	-0.003	Avg_Transaction_Amount_7d	:	Transaction_Distance
19	+0.002	Failed_Transaction_Count_7d	:	Timestamp
20	-0.002	Account_Balance	:	Transaction_Amount
21	+0.002	Card_Age	:	Transaction_Amount
22	+0.002	Account_Balance	:	Timestamp
23	+0.002	Daily_Transaction_Count	:	Transaction_Amount
24	+0.002	Card_Age	:	Timestamp
25	-0.002	Risk_Score	:	Transaction_Distance
26	-0.002	Daily_Transaction_Count	:	Transaction_Distance
27	+0.002	Account_Balance	:	Transaction_Distance
28	-0.002	Account_Balance	:	Avg_Transaction_Amount_7d
29	-0.002	Card_Age	:	Daily_Transaction_Count
30	-0.001	Card_Age	:	Risk_Score
31	+0.001	Failed_Transaction_Count_7d	:	Transaction_Amount
32	+0.001	Failed_Transaction_Count_7d	:	Risk_Score
33	+0.001	Account_Balance	:	Card_Age
34	-0.000	Account_Balance	:	Failed_Transaction_Count_7d
35	-0.000	Daily_Transaction_Count	:	Timestamp
36	+0.000	Avg_Transaction_Amount_7d	:	Timestamp

المصدر مخرجات برنامج (Orange)

تظهر نتائج تحليل الارتباط بين متغيرات الدراسة قيما منخفضة جدا لمعاملات ارتباط بيرسون، حيت تتراوح جميعها بين الـــ −0،000 و +0،008 أي انها تقترب بشدة من الصفر، وهذا يشير الى غياب أي علاقة طية ذات ذلالة إحصائية بين المتغيرات المذكورة أعلاه، ومن هنا نستنتج مجموعة من التفسيرات:

- **استقلالية المتغيرات:** بما ان معاملات الارتباط شبه معدومة، فهدا يعني ان المتغيرات لا تؤثر خطيا على بعضها البعض.
- **ميزة للنماذج المعتمدة على تعلم الالة:** انخفاض الارتباطات يعني غياب الخطية المتعددة بين المتغيرات، وهدا امر إيجابي جدا عند استخدام خوارزميات متل خوارزمية الغابة العشوائية، لاتها تفترض استقلالية نسبية بين المتنبئات فكل متغير يحمل معلومات فريدة لا تتكرر في متغير اخر.
- **العلاقات الغير خطية محتملة:** عدم وجود ارتباط خطي لا ينفي وجود علاقات غير خطية متل أنماط الاحتيال المعقدة او التفاعلات بين المتغيرات. ففي الاحتيال المالي غالبا ما تكون العلاقات غير خطية مثلا زيادة حادة في قيمة المعاملة بعد عدة محاولات فاشلة، وهذه لا تظهر في معامل بيرسون، لذلك يوصى باستخدام خوارزميات قادرة على التقاط التعقيدات متل خوارزمية الغابة العشوائية.
- **تفسيرات الطابع الزمني (Timestamp):** نلاحظ ان ارتباطه شبه معدوم مع باقي المتغيرات حيت بلغت أكبر قيمة 0،008 + يعني ان الزمن لا يرتبط بحجم المعاملات والمخاطر، مما يشير الى ان النمط الزمني للاحتيال غير منتظم أو موسمي.

المطلب الثاني: التطبيق العملي لمراحل تصميم أنموذج خوارزمية الغابة العشوائية

في هدا المطلب يتم تنفيذ مختلف خطوات تصـــميم أنموذج الدراســـة بعد عملية جمع البيانات والتحليل الاستكشافي السابق، وذلك بشكل عملي داخل البيئة البرمجية (orange) حيت ساهمت في تنفيذ مختلف المراحل التطبيقية وبناء أنموذج وتقييمه بشكل مرئي ومنظم. ودلك حسب بيانات الدراسة المختارة وجاهزيتها.

الفرع الأول: المعالجة المسبقة لبيانات الدراسة.

ان البيانات المختارة للدراسة لم تتعرض لمرحلة المعالجة المسبقة وذلك لأنها منظمة وموثوقة مما اسهم رفع جاهزيتها للتحليل المباشر، كما ان التحليل الاستكشافي للبيانات اظهر خلوها التام من القيم المفقودة وهو ما يعفى من الحاجة الى اية معالجة استيفاءيه قد تدخل تحيزا في البيانات الاصلية بالإضافة الى ان تحليل الارتباط بين المتغيرات عن علاقات ضعيفة جدا سواءا اكانت سلبية ام إيجابية، مما يعني غياب مشكلة الترابط الخطي المرتفع بين المتغيرات المستقلة، وبالتالي فان جميع المتغيرات تسهم بمعلومة مستقلة نسبيا تتري النموذج دون تكرار، بالإضافة الى هدا حاولنا تطبيق المنهجية من غير معالجة التوازن للتمثيل الواقعي للســـيناريو الاحتيال المرتفع في المعاملات المالية الالكترونية, وبناءا على هدا انتقلنا مباشرة الى مرحلة تقسيم النموذج باستخدام التحقق المتقاطع ب 5 طيات بوصفها الأسلوب الأمثل لضمان موثوقية النتائج وتعميمها.

الفرع الثاني: تقسيم البيانات.

قسم انموذج خوارزمية الغابة العشوائية باستخدام التحقق المتقاطع ذي الخمس طيات (folds K5 Validation Cross)، حيث قُسّـــمت بيانات التدريب إلى خمس مجموعات فرعية متســـاوية. في كل تكرار، اســـتُخدمت أربع مجموعات بيانات للتدريب، بينما استُخدمت المجموعة المتبقية للتحقق، وتكررت هذه العملية خمس مرات. تم الإبلاغ عن الأداء النهائي كمتوســـط لجميع مجموعات البيانات الخمس، مما يضـــمن تقييمًا أكثر دقة وموثوقية، ويقلل من مخاطر التخصيص الزائد لأي تقسيم بيانات محدد. ومن مبرراتنا لاستخدام هدا التقسيم:

- اختبار كل البيانات وتقليل التباين (Variance) للنتائج.
- النموذج يختبر على 5 تقسيمات مختلفة والنتيجة هي المتوسط.
- لا وجود للصدفة نتيجة لإخضاع كل البيانات للاختبار لان التقسيم منظم وليس عشوائيا.
- لتجنب التحيز وزيادة الموثوقية (مستقلة عن التقسيم).
- الطريقة المفضلة في أبحاث التعلم الآلي.
- إعطاء تقدير أكثر استقرارا للوضع الحقيقي.

- **خطوات عملية التقسيم:** التحقق المتقاطع أسلوب إحصائي يقيّم أداء النموذج بصورة موثوقة ويقلل من الإفراط في التخصيص. في هذه الدراسة استُخدمK=5طيات. ونبرز الية عمليه في دراستنا التطبيقية من خلال الجدول التالي:

الجدول رقم 02 –21: الية عمل التحقق المتقاطع دي ال 5 طيات

الخطوة	الوصف
1	يُقسَّم مجموع البيانات (50.000 مشاهدة) إلى 5طيات متساوية، كل طية = 10.000 مشاهدة
2	في كل تكرار تُستخدم 4 طيات للتدريب (40.000 وطية واحدة للاختبار 10.000)
3	تتكرر العملية 5 مرات بحيث تكون كل طية مرة واحدة كبيانات اختبار
4	تُحسب مقاييس الأداء لكل (fold) ثم تُحسب القيمة النهائية كمتوسط النتائج الخمس

المصدر : من اعداد الطالبة بالاعتماد على بيانات الدراسة وبرنامج (Orange)

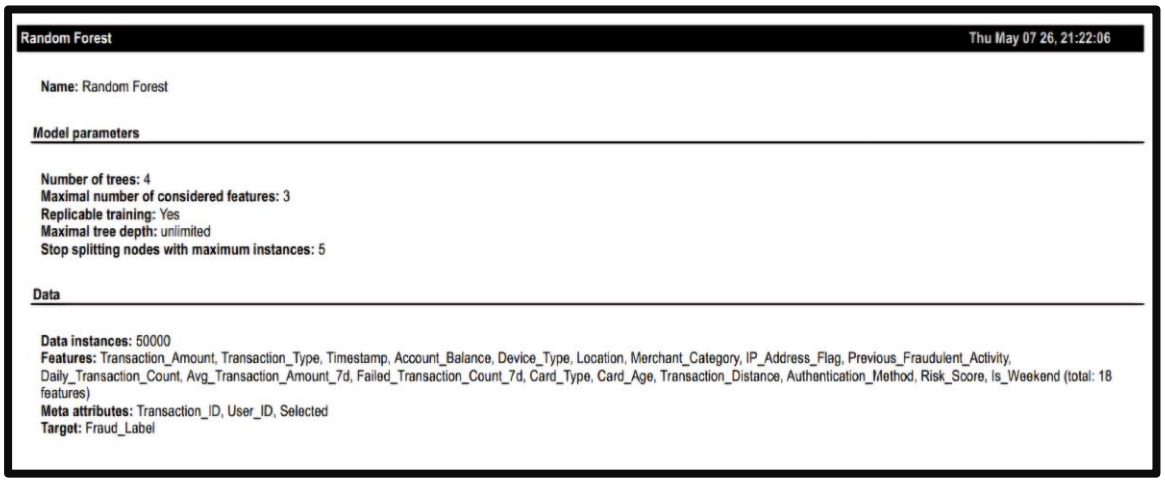
الفرع الثالث: اختيار النموذج

لتصـميم أنموذج الدراسـة قمنا باختيار خوارزمية الغابة العشـوائية نظرا لقدرتها على التعامل مع البيانات الغير خطية (تفاعل عدة عوامل أي علاقة معقدة) بالإضـــافة الى مقاومتها لمشـــكلة الإفراط في التعلم وفعاليتها المثبتة في كشف الاحتيال المالي الإلكتروني انطلاقا من الدراسات البحثية السابقة ،كما انها تعد أكثر استقرارا مع البيانات المالية وأقل حساسية للمعلمات بالإضافة الى انها لا تحتاج ضبطا معقدا ومناسبة لحجم بيانات الدراسة بالإضافة الى انه في الأبحاث الأكاديمية في مجال المحاســبة والتدقيق والتكنولوجيا المالية ليس الهدف تحقيق أعلى دقة فقط بل اســتخراج أهمية المتغيرات وتفســير النتائج فنموذج (RF) يتوفر على تفســير أهمية المتغيرات + اســتقرار في النتائج وســهولة تفسيرها .

الفرع الرابع: تدريب وتحسين النموذج

تم ضبط إعدادات (المعلمات) خوارزمية الغابة العشوائية بدقة وعناية فائقة للحصول على نتائج موثوقة ببرنامج أورانج، ففي انموذج خوارزمية الغابة العشوائية تم إستخدام عدد كبير من الأشجار –200 300 100– لكنه لم يسجل تحسنا ملحوظا ما أدى ذلك الى ضبط الإعدادات بالشكل الموضح ادناه من اجل زيادة الدقة للتوصل إلى نتائج جيدة جدا وتجنب المثالية (أي عدم المبالغة) مما سجل قيم مقاييس أداء متقاربة تدل على أن النموذج يعمم جيدا.

شكل رقم 02 –41: تحسين وتدريب خوارزمية الغابة العشوائية، المصدر مخرجات برنامج (Orange)



المصدر مخرجات برنامج (Orange)

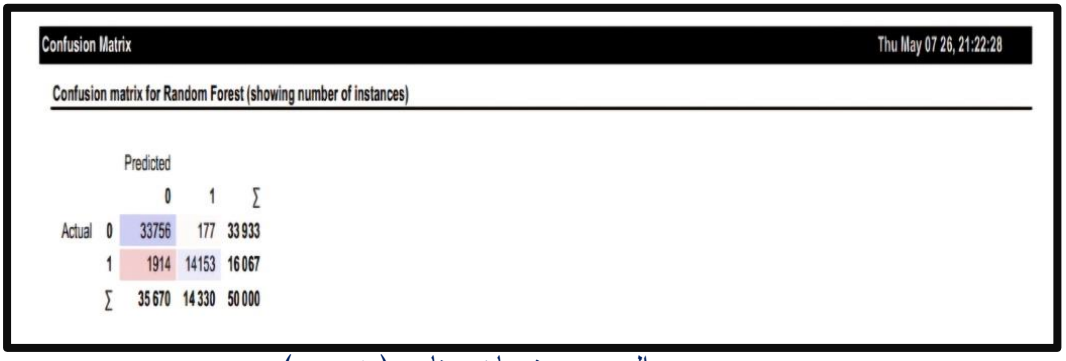
- **شرح ضبط المعلمات:** بناءً على معلمات النموذج المُعرَّفة في برنامج:Orange قبل الوصول إلى النتائج النهائية مرّ النموذج بمرحلة ضـبط تدريجي للمعلمات، إذ جرى رفع قيم بعضـها وخفض قيم أخرى حتى تم التوصـل إلى التوليفة المثلى التالية:
  - **عدد الأشجار:** (تم استخدام عدد صغير نسبيًا من الأشجار)
  - **الحد الأقصى لعدد الميزات المُعتبرة:** 3 (يمكن للنموذج اعتبار الميزات المتاحة لاتخاذ قرارات التقسيم).
  - **إمكانية تكرار التدريب:** نعم (يمكن إعادة إنتاج النتائج بدقة عبر عمليات التشغيل).
  - **الحد الأقصى لعمق الشجرة:** غير محدود (يمكن للأشجار أن تنمو دون قيود على العمق).
  - **إيقاف تقسـيم العقد ذات الحد الأقصـى من الحالات:** الى 5 (حيث لن يتم تقسـيم العقد إذا كانت تحتوي على 5 حالات أو أقل).
- يمثل هذا التكوين تطبيقًا أساسـيًا للغابة العشـوائية مع قيود قليلة على نمو الشـجرة حيت تم اختبار اعداد أكبر من الاشجار متل: 50و 100 و200 شجرة، الا ان النتائج لم تظهر أي تحسن، بل سجل انخفاض طفيف في بعض مقاييس التقييم. وهدا يتوافق مع ما اوضـحه Breimanمن ان خطا التعميم في الغابة العشـوائية يتقارب تدريجيا نحو قيمة مسـتقرة مع زيادة عدد الاشـجار. اما في هده الدراسـة فيفسـر الانخفاض الطفيف بطبيعة البيانات الاصـطناعية المصـممة لمحاكاة بيئة احتيال عالية المخاطر، حيت تكون الانماط الاحتيالية والاشـارات التميزية اكتر وضوحا مقارنة بالبيانات الواقعية عالية الضجيج. ونتيجة لدلك بلغ النموذج مرحلة التشبع التصنيفي عند عدد منخفض نسبيا من الاشجار، بينما اصبحت الاشجار الاضافية محدودة الفائدة من ناحية التعميم و هو ما يعرف بمرحلة العائد المتناقص.[148]
- وقد أثبتت هذه التوليفة المضبوطة فاعليتها من خلال النتائج اللاحقة التي سيتم عرضها.

[148] LEO BRIMANE, RANDOM FORESTS, MACHINE LEARNING, VOL 45, N 1, ,2001, P 7

المطلب الثالث: تقييم أداء أنموذج خوارزمية الغابة العشوائية.

الفرع الأول: مصفوفة ارتباك أنموذج خوارزمية الغابة العشوائية.

الشكل رقم: 02-42: مصفوفة الارتباك لأنموذج خوارزمية الغابة العشوائية



المصدر مخرجات برنامج (orange)

ادن نفسر شكل مصفوفة الارتباك لأنموذج خوارزمية الغابة العشوائية المصمم من خلال الجدول الموضح اسفله حيت ان مصفوفة الارتباك التالية هي المجموع التراكمي لنتائج الطيات الخمس جميعها، أي ان كل مشاهدة من ال 50000 قد مرت مرة واحدة كبيانات اختبار:

الجدول رقم 02-22: تفسير قيم مصفوفة الارتباك.

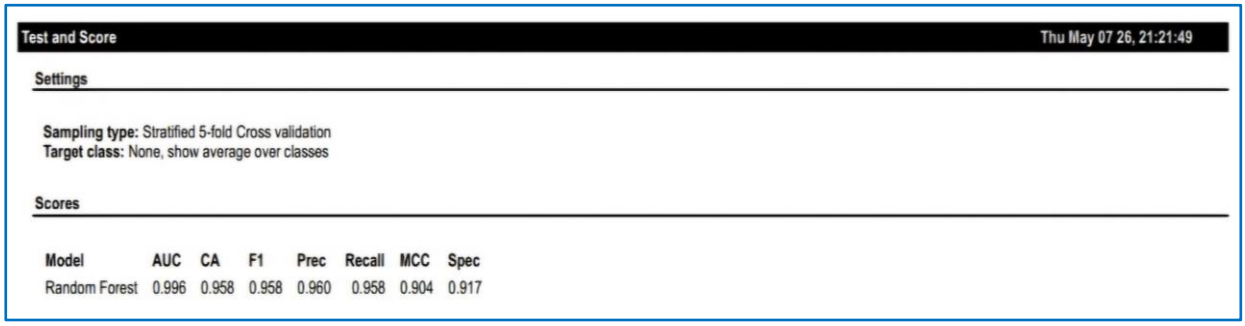
الرمز	الاسم	القيمة	التفسير
TP	True Positive	14153	تم التنبؤ ب 14153 قيمة بشكل صحيح بواسطة النموذج، حيت توقع النموذج وجود احتيال في 14153حالة والتي احتوت بالفعل على احتيال.
TN	True Negative	33756	توقع النموذج بشكل صحيح ان 33756 حالة خالية من الاحتيال، مقارنة ب 33933
FP	False Positive	177	بلغ عدد الحالات المصنفة خطا على انها احتيال 177 حالة، حيت توقع النموذج وجود احتيال رغم ان هذه الحالات كانت سليمة، فعليا وهو ما يمتل إنذارات خاطئة فعلا.
FN	False Negative	1914	بلغ عدد الحالات التي فشل النموذج في اكتشافها 1914 حالة، حيت صنفها النموذج على انها

غير احتيالية بالرغم انها تحتوي على احتيال، مما يعكس محدودية النموذج في كشف جميع حالات الاحتيال.	

المصدر :من اعداد الطالبة بالاعتماد على مصفوفة ارتباك أنموذج خوارزمية تعلم الالة.

الفرع الثاني: مقاييس تقييم أنموذج خوارزمية الغابة العشوائية

الشكل رقم 02 –43: مقاييس أداء انموذج خوارزمية الغابة العشواءية



المصدر : مخرجات برنامج (Orange)

- اظهر انموذج خوارزمية الغابة العشـوائية أداءً تنبؤيًا قويًا في جميع مقاييس التقييم. حيث حقق النموذج دقة عالية، حيث صـنف غالبية المعاملات بشـكل صـحيح. من حيث الاسـتدعاء، أثبت النموذج فعاليته في تحديد حالات الاحتيال، مما قلل من عدد حالات الاحتيال التي لم يتم اكتشافها – وهو أمر بالغ الأهمية نظرًا لعدم توازن الفئات في مجموعة البيانات. عكست درجة(F1) توازنًا جيدًا بين الدقة والاستدعاء، مما يشير إلى أن النموذج حافظ على أداء موثوق دون التضـحية بأحد المقياسين على حساب الآخر. أخيرًا، أكدت درجة (AUC–ROC) قدرة النموذج القوية على التمييز بين المعاملات الاحتيالية وغير الاحتيالية عبر عتبات تصـــنيف مختلفة. تشـــير هذه النتائج مجتمعة إلى أن نموذج الغابة العشـــوائية مرشـــح قوي لمهام كشـــف الاحتيال المالي الالكتروني. وهوما ســـنبرزها بالتفصيل من خلال اثبات هده المقاييس بالاعتماد على قوانينها النظرية ومعطيات مصفوفة الارتباك.

1. اثبات الدقة الكلية ((Classification Accuracy)CA) :

تقيس نسبة التصنيفات الصحيحة إجمالاً من مجموع المشاهدات.

$$CA = (TP + TN) / (TP + TN + FP + FN)$$
$$CA = (14153 + 33756) / (14153 + 33756 + 177 + 1914)$$
$$CA = 47909 / 50000$$
$$CA = 0.9582 \approx 0.958$$

- **التفسـير الاقتصـادي لنتيجة الدقة الكلية:** حقق أنموذج خوارزمية الغابة العشـوائية دقة كلية بلغت 95،8 %مما يعني ان النموذج تمكن من تصنيف معظم المعاملات بشكل صحيح، سواء اكانت المعاملات سليمة او احتيالية. وهو ما يدل على موثوقية النموذج في بيئة المعاملات الالكترونية ذات الحجم الكبير.

2. اثبات الدقة الإيجابية (Precision (Weighted Average

يقيس نسبة التنبؤات الصحيحة من إجمالي ما صنّفه النموذج بالفئة نفسها. يستخدم Orange المتوسط الموزون.

أ) دقة الفئة 0 (طبيعي):

Prec_0 = TN / (TN + FN) = 33756 / (33756 + 1914) = 33756 / 35670 = 0.9463

ب) دقة الفئة 1 (احتيال):

Prec_1 = TP / (TP + FP) = 14153 / (14153 + 177) = 14153/14 330=0.9876

ج) المتوسط الموزون النهائي:

Prec_w = (Prec_0 × n_0 + Prec_1 × n_1) / N
Prec_w = (0.9463 × 33933 + 0.9876 × 16067) / 50000
Prec_w = (32113 + 15873) / 50000 = 47986 / 50000
Precision = 0.9597 ≈ 0.960

- **التفسير الاقتصادي لنتيجة الدقة الايجابية:** تشير قيمة الدقة الإيجابية الى ان 96 %من المعاملات التي صنفها النموذج على انها احتيالية كانت فعلا معاملات احتيالية حقيقية، في حين ان نسبة قليلة فقط كانت إنذارات خاطئة، وتكتسب هذه النتيجة أهمية كبيرة في القطاع المالي لأنها تقلل من تعطيل المعاملات السليمة للعملاء وتخفض التكاليف الناتجة عن التحقيق في العمليات الغير احتيالية.

3. الحساسية :(Recall (Weighted Average)

يقيس قدرة النموذج على اكتشاف الحالات الفعلية لكل فئة. يستخدم Orange المتوسط الموزون

ا) الحساسية الفئة 0 (طبيعي):

Recall_0 = TN / (TN + FP) = 33756 / (33756 + 177) = 33756 /33933 = 0.9948

ب) الحساسية الفئة 1 (احتيال) — منفردة:

Recall_1 = TP / (TP + FN) = 14153 / (14153 + 1914) = 14153/ 16067 = 0.8808

ج) المتوسط الموزون النهائي:

Recall_w = (Recall_0 × n_0 + Recall_1 × n_1) / N
Recall_w = (0.9948 × 33933 + 0.8808 × 16067) / 50000
Recall_w = (33756 + 14153) / 50000 = 47909 / 50000
Recall (Weighted) = 0.9582 ≈ 0.958

- **التفسير الاقتصادي لنتيجة الحساسية:** بلغت قيمة الحساسية نسبة 95.8% وهوما يدل على قدرة النموذج على اكتشاف اغلب العمليات الاحتيالية وعدم ترك عدد كبير منها يمر دون اكتشاف، وهو عنصر بالغ الأهمية لان فشل النظام في اكتشاف العمليات الاحتيالية قد يؤدي الى خسائر مالية مباشرة للمؤسسة والعملاء.

4. مقياس F1 Score (Weighted Average)

يجمع بين الدقة الإيجابية والحساسية في مقياس متوازن واحد، ومفيد بشكل خاص في البيانات غير المتوازنة.

أ) F1 الفئة 0 الطبيعية:

$F1_0 = 2 \times (Prec_0 \times Recall_0) / (Prec_0 + Recall_0)$
$F1_0 = 2 \times (0.9463 \times 0.9948) / (0.9463 + 0.9948) = 1.8826/1.9411 = 0.9699$

ب) F1 الفئة 1 الاحتيالية:

$F1_1 = 2 \times (Prec_1 \times Recall_1) / (Prec_1 + Recall_1)$
$F1_1 = 2 \times (0.9876 \times 0.8808) / (0.9876 + 0.8808) = 1.7404/1.8684 = 0.9314$

ج) المتوسط الموزون النهائي:

$F1_w = (F1_0 \times n_0 + F1_1 \times n_1) / N$
$F1_w = (0.9699 \times 33933 + 0.9314 \times 16067) / 50000$
$F1_w = (32913 + 14965) / 50000 = 47878 / 50000$
$F1\ Score\ (Weighted) = 0.9576 \approx 0.958$

- **التفسير الاقتصادي للنتيجة:** بلغت قيمة مؤشر F1 Score نسبة 95.8% مما يعكس وجود توازن جيد بين القدرة على اكتشاف الاحتيال وتقليل الإنذارات الخاطئة.

5. النوعية (Specificity (Weighted Average

تقيس قدرة النموذج على تصنيف الحالات الطبيعية بشكل صحيح. يستخدم Orange المتوسط الموزون.

أ) النوعية الفئة 0 الطبيعية:

$Spec_0 = TP / (TP + FN) = 14153 / 16067 = 0.8808$

ب) النوعية الفئة 1 الاحتيالية:

$Spec_1 = TN / (TN + FP) = 33756 / 33933 = 0.9948$

ج) المتوسط الموزون النهائي

$Spec_w = (Spec_1 \times n_0 + Spec_0 \times n_1) / N$
$Spec_w = (0.9948 \times 33933 + 0.8808 \times 16067) / 50000$
$Spec_w = (33756 + 14153) / 50000 = 47909 / 50000$
$Specificity\ (Weighted) \approx 0.917$

- **التفسير الاقتصادي للنتيجة:** تفسر النتيجة على أن النموذج تمكن من تصنيف حوالي 91،7 من المعاملات السليمة بشكل صحيح على انها غير احتيالية، مما يعكس قدرته على تقليل الإنذارات الكاذبة وعدم تعطيل العمليات المالية الشرعية للعملاء وهو ما يساهم في تحسين كفاءة أنظمة الدفع الالكتروني وتقليل التكاليف التشغيلية المرتبطة بالتحقق اليدوي من المعاملات.

6. معامل ارتباط ماثيوس MCC

يُعدّ MCC الأدق للبيانات غير المتوازنة لأنه يأخذ بالاعتبار جميع قيم مصفوفة الارتباك الأربع.

$MCC = [(TP \times TN) - (FP \times FN)] / sqrt[(TP+FP)\ (TP+FN)\ (TN+FP)\ (TN+FN)]$

أ. حساب البسط:

$TP \times TN = 14153 \times 33756 = 477738468$

FP × FN = 177 × 1914 = 338778
477738468-338778=477399690

ب. حساب المقام:

(TP+FP) = 14330 | (TP+FN) = 16067 | (TN+FP) = 33933 | (TN+FN) = 35670
Sqrt (14330 × 16067 × 33933 × 35670) = sqrt (2.787 ×10^17) = 527،919،486

ج. النتيجة:

MCC = 477،399،690 / 527،919،486
MCC = 0.9043 ≈ 0.904

- **التفسـير الاقتصـادي للنتيجة:** فتوكد هده النتيجة المرتفعة جودة النموذج حتى مع عدم وجود بيانات متوازنة بين المعاملات الاحتيالية والغير احتيالية وهو مؤشـر اكتر موثوقية في دراسـات الاحتيال المالي لان هدا النوع من البيانات غالبا ما يكون غير متوازن.

7. مساحة تحت منحنى (AUC-ROC)

القيمة الأساسية من نقطة قطع 0.5

AUC_basic = (Recall_0 + Recall_1) / 2 = (0.9948 + 0.8808) / 2= 0.9378
AUC = 0.996 (من منحنى ROC الكامل في Orange)

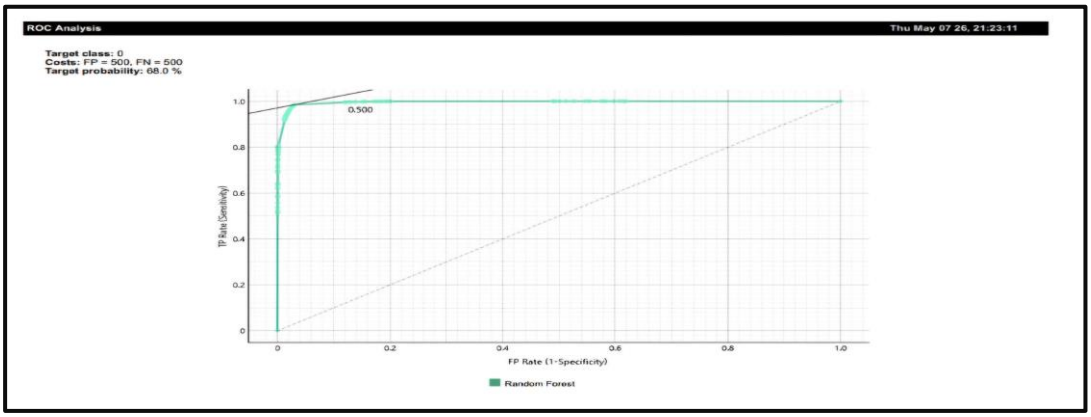
التفسير الاقتصادي للنتيجة: بلغت قيمة AUCنسبة 99،6% وهي نسبة مرتفعة جدا، وتشير الى قدرة النموذج على التمييز بدقة كبيرة بين المعاملات الاحتيالية والمعاملات السـليمة، أي ان النظام يسـتطيع ترتيب العمليات حسـب درجة خطورتها بكفاءة عالية، وهو امر بالغ الأهمية في المؤسـسـات المالية التي تحتاج الى اكتشـاف العمليات المشبوهة قبل اتمامها.

الفرع الثالث: منحنيات تقييم أداء خوارزميات تعلم الالة

1. منحنيات خصائص التشغيل المستقبل: (ROC Curve)

أولا: منحنى خصائص التشغيل عند فئة المعاملات الطبيعية:

الشكل رقم 02-44: منحنى (ROC) عند الفئة 0 المعاملات الطبيعية،

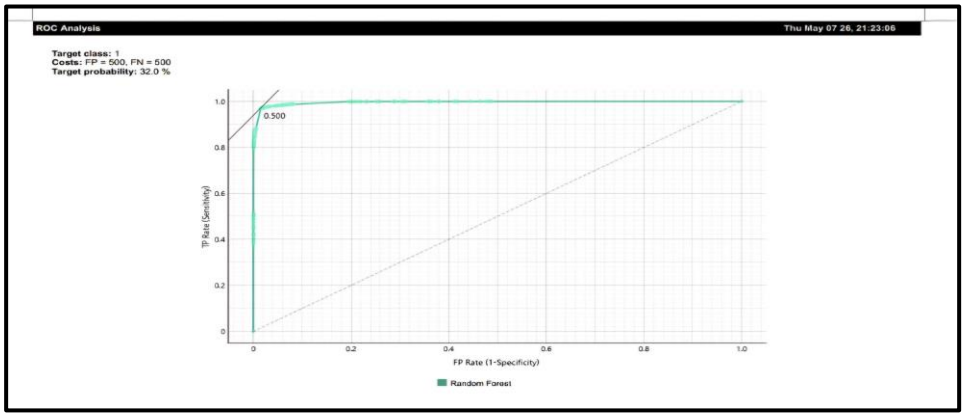


المصدر: مخرجات برنامج (Orange)

الاحظ من الشكل الموضح أعلاه: ان منحنى (ROC) للفئة 0 يكشف عن أداء استثنائي للنموذج، فالمنحنى يقفز بشكل شبه عمودي نحو الزاوية العلوية اليسرى منذ البداية قبل أن يستقر أفقياً عند مستوى الحساسية 1.0 تقريباً. وما يلفت الانتباه هنا هو أن نقطة العتبة المثلى 0.500 تقع في الجزء العلوي الأيسر من المنحنى، وهو الموقع المثالي الذي يعكس قدرة النموذج على التمييز بين المعاملات الطبيعية والاحتيالية بأقل قدر ممكن من الإنذارات الكاذبة. والجدير بالذكر أن احتمال الخطأ في تصنيف المعاملات الطبيعية بلغ 0.068 فقط، وهو رقم يعكس دقة النموذج في حماية المعاملات السليمة من التصنيف الخاطئ، وهذا يتوافق تماماً مع قيمة النوعية المحققة 0.917.

ثانيا: منحنى خصائص التشغيل عند فئة المعاملات الإحتيالية:

الشكل رقم 02-45: منحنى (ROC) عند الفئة 1 المعاملات الاحتيالية



المصدر: مخرجات برنامج (Orange)

ألا حظ من الشكل ان: منحنى (ROC) للفئة 1 فيُظهر صورة مشابهة لكنها أكثر إثارة للاهتمام من الناحية التطبيقية. المنحنى يرتفع بسرعة لافتة نحو الزاوية العلوية اليسرى ويحافظ على مستوى حساسية مرتفع جداً عبر مختلف عتبات التصنيف. ونقطة العتبة 0.500 تقع هي الأخرى في الموضع الأمثل من المنحنى. ومما يثير الاهتمام أن احتمال الخطأ في تصنيف حالات الاحتيال بلغ 0.324، وهو أعلى نسبياً مقارنة بالفئة 0، وهذا أمر متوقع نظراً لتنوع أنماط الاحتيال في بيانات المحاكاة وتعقيدها مقارنة بالمعاملات الطبيعية المتسقة. غير أن هذه النسبة تبقى مقبولة جداً في ضوء القيمة الكلية لمساحة تحت المنحنى.

- بالنظر الى منحنيي (ROC) الخاصين بالفئتين 0 و1 نلاحظ ان كلا المنحنيين يقعان بالقرب من الزاوية العلوية اليسرى، مما يدل على ارتفاع معدل الإيجابيات الحقيقية وانخفاض معدل الإيجابيات الكاذبة، حيت بلغ معدل الإيجابيات الحقيقية معدل 91,7% مقابل معدل منخفض للإيجابيات الكاذبة يقدر بحوالي 6,8%، وهو ما يعكس قدرة عالية للنموذج على التمييز بين المعاملات الطبيعية والمعاملات الاحتيالية، كما تشير قيم المساحة تحت المنحنى الى جودة الأداء التمييزي للنموذج، إذ يمكن تفسير أن قيم المساحة تحت منحنى ROC(AUC-ROC) يمكن تفسيرها على النحو التالي:

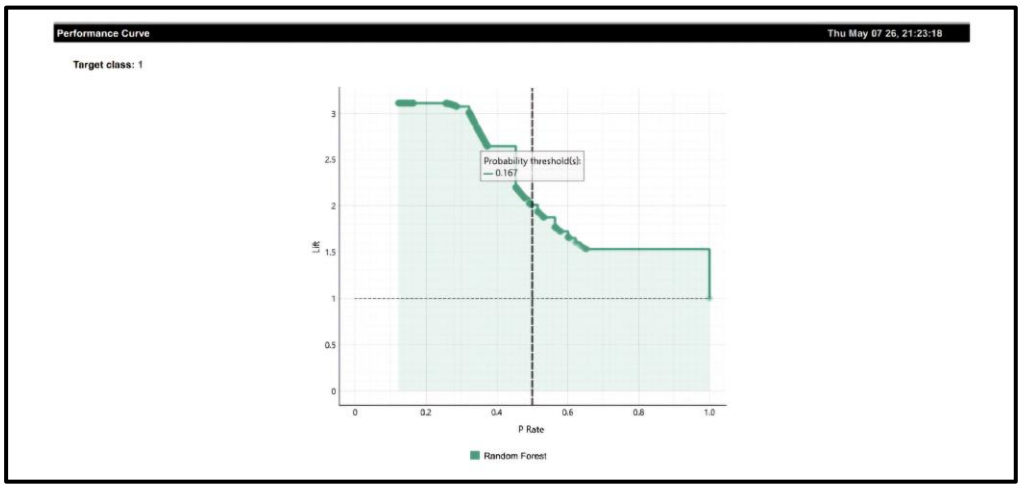
- ✓ ROC = 0.5: لا يمتلك النموذج أي قدرة تمييزية، وهو ما يعادل الصدفة.
- ✓ 0.7 ≤ ROC ≤ 0.8: يمتلك النموذج قدرة تمييزية مقبولة.
- ✓ 0.8 ≤ ROC ≤ 0.9: يتمتع النموذج بقدرة تمييز ممتازة.
- ✓ 0.9 ≤ ROC: يتمتع النموذج بقدرة تمييز فائقة.[149]

وبما ان منحنيي (ROC) في الدراسة الحالية يقتربان بشكل كبير من القيمة 1، فان نموذج الغابة العشوائية يقع ضمن فئة القدرة التمييزية الفائقة سواء بالنسبة للمعاملات الطبيعية او المعاملات الاحتيالية، مما يؤكد فعاليته في كشف الاحتيال المالي الالكتروني.

2. منحنيات الرفع (Lift curve) التابع لمنحنيات الأداء (Performance Curves):

أولا :منحنى الأداء عند فئة المعاملات الاحتيالية :

الشكل رقم 02 –46: منحنى الأداء، عند فئة المعاملات الاحتيالية



المصدر: مخرجات برنامج (Orange)

الاحظ من الشكل أعلاه ان: منحنى الأداء للفئة 1 يكشف عن قدرة عالية واضحة لنموذج الغابة العشوائية في اكتشاف الاحتيال. ففي بداية المنحنى عند النسب المنخفضة من (P Rate) يبلغ مؤشر الرفع قيمته القصوى التي تتجاوز 3.1، وهذا يعني ببساطة أن النموذج أكثر فاعلية بأكثر من ثلاثة أضعاف مقارنة بالتصنيف العشوائي حين يركز على الحالات ذات الاحتمالية المرتفعة للاحتيال.

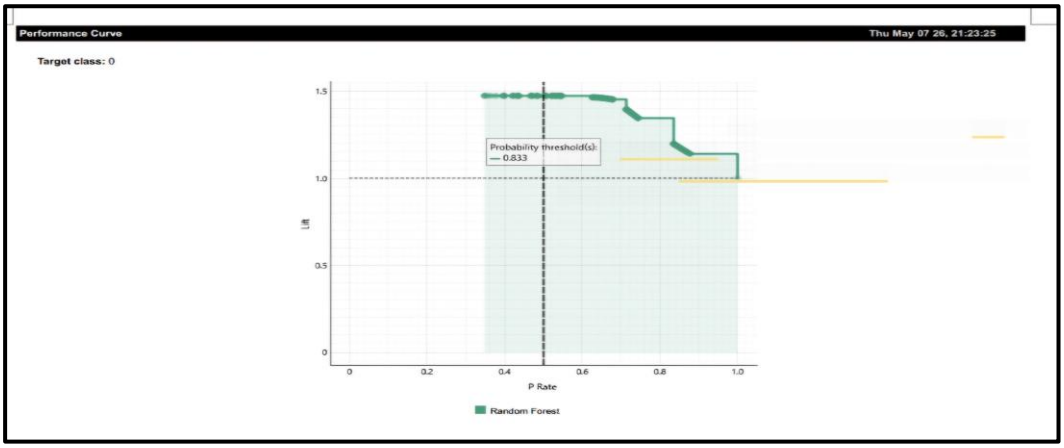
وما يثير الاهتمام أن المنحنى يحافظ على مستوى رفع مرتفع يتراوح بين 3.0 و3.1 حتى حدود 0.35 من (P Rate) قبل أن يبدأ بالانخفاض التدريجي. وعند نقطة العتبة الاحتمالية 0.167 المشار إليها بالخط المتقطع يسجل المنحنى قيمة رفع تقارب 2.0، مما يعكس أن النموذج لا يزال يتفوق بمقدار الضعف على التصنيف العشوائي

[149] BEKADDOUR FATIMA ZAHRA, STOCK PRICE CLASSIFICATION USING FINANCIAL INDICATORS FROM 10 -K REPORTS: A COMPARATIVE STUDY BETWEEN NEURAL NETWORKS (NN) AND LOGISTIC REGRESSION (LR), Op, Cit,P238 -239

حتى عند هذه العتبة المنخفضـــة. والمنحنى لا يهبط إلى مســـتوى 1.0 إلا عند اقترابه من نهاية المحور الأفقي، مما يدل على أن النموذج يحتفظ بفاعليته عبر معظم نطاق التصـــنيف، وهو ما يتوافق تماماً مع قيمة Recall الموزونة المحققة والبالغة 0.958 أي أن النموذج اكتشـــف 14،153 معاملة احتيالية من أصـــل 16،067 بمتوســـط موزون يعكس أداء الفئتين معاً.

ثانيا : منحنى الأداء عند فئة المعاملات الطبيعية:

الشكل رقم 02-47: منحنى الأداء، عند فئة المعاملات الطبيعية



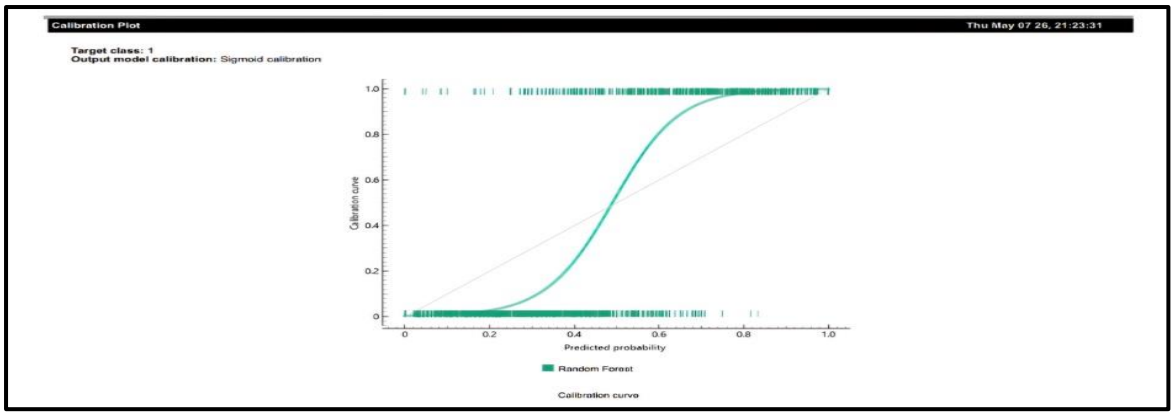
المصدر : مخرجات برنامج Orange

الاحظ من الشـــكل أعلاه ان: الصـــورة تختلف اختلافاً لافتاً في منحنى الفئة 0 فخلافاً للفئة 1 التي بدأت بقيم رفع مرتفعة جداً تبدأ الفئة 0 بقيم رفع معتدلة تتمركز حول 1.5 وتستمر بهذا المستوى على امتداد واسع من المحور الأفقي. وعند نقطة العتبة الاحتمالية 0.833 المشار إليها بالخط المتقطع يحقق النموذج قيمة رفع تبلغ 1.5 تقريباً. هذا النمط المســـتقر والمنتظم ليس ضـــعفاً في النموذج بل هو انعكاس طبيعي لحجم الفئة 0 الكبير البالغ 33،933 معاملة طبيعية. فكلما كانت الفئة أكبر حجماً كلما كان من الصـــعب تحقيق قيم رفع مرتفعة جداً لأن النموذج يجد أمامه عدداً ضخماً من الحالات يجب تصنيفها بدقة. والمؤشر الإيجابي هنا أن المنحنى يظل فوق مستوى 1.0 على مدى واسـع مما يعني أن النموذج يتفوق باسـتمرار على التصـنيف العشـوائي، وهو ما يتجلى في قيمة Specificity البالغة 0.917 والتي تعني أن النموذج صنّف 33،756 معاملة طبيعية بشكل صحيح.

3. مخطط المعايرة (Calibration Plot)

اولا: مخطط المعايرة عند المعاملات الاحتيالية

الشكل رقم 02-48: مخطط المعايرة، عند فئة المعاملات الاحتيالية



المصدر: مخرجات برنامج Orange

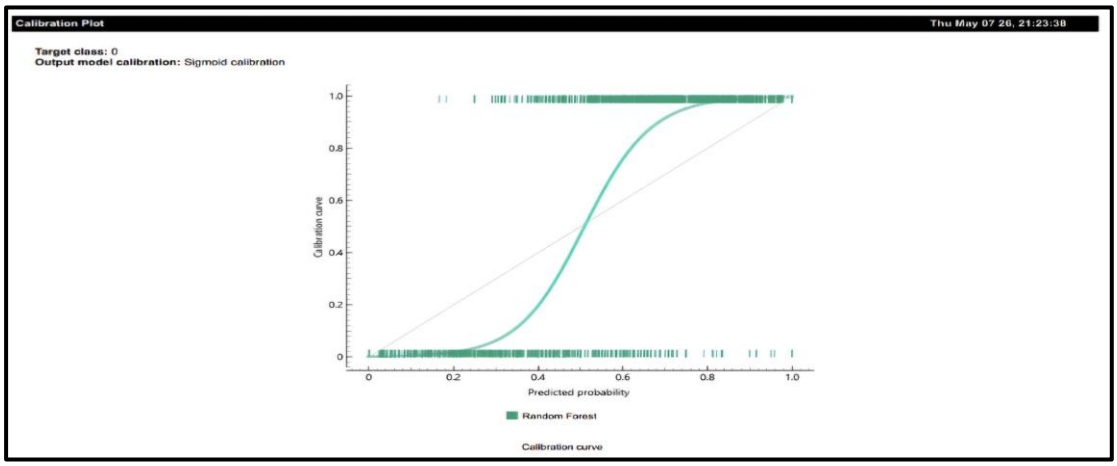
نلاحظ أن المنحنى يأخذ شكلاً سينياً نتيجة تطبيق معايرة، وهذا ليس غريباً على نماذج الغابة العشوائية التي تميل بطبيعتها لتركيز تنبؤاتها نحو القيم المتطرفة. فعلى المحور الأفقي تظهر الاحتمالات المتنبئ بها، فيما يعكس المحور العمودي قيم المعايرة الفعلية. وما يستوقف الناظر في هذا الرسم هو سلوك النموذج في المنطقة الوسطى بين 0.3 و0.65، حيث يعلو المنحنى فوق الخط المثالي بفارق ملحوظ مما يكشف عن ميل النموذج للتحفظ وإعطاء احتمالات مرتفعة نسبياً للمعاملات المشكوك فيها. وفي سياق اكتشاف الاحتيال تحديداً يُعد هذا التوجه مقبولاً بل ومرغوباً، إذ إن الإنذار الاحترازي أجدى من إغفال عملية احتيال حقيقية.

أما عند الاحتمالات التي تتجاوز 0.65 فيتقارب المنحنى مع الخط المثالي بشكل أوضح، وهنا تتمركز غالبية المعاملات الاحتيالية البالغة 14،153 معاملة مصنفة بشكل صحيح، وهو ما يتوافق مع قيمة الدقة الإيجابية 0.960 التي تعني أن النموذج حين يُصنف معاملة ما كاحتيالية فإنه يكون محقاً في 96% من الحالات.

- تكشف كثافة النقاط عند طرفي المحور الأفقي عن فصل واضح بين الفئتين، وهذا الفصل بالذات هو ما يقف خلف القيمة الاستثنائية لمساحة تحت المنحنى التي بلغت 0.996، مما يرسخ الثقة في قدرة النموذج على التمييز الدقيق بين المعاملات الاحتيالية والطبيعية.

ثانيا: مخطط المعايرة عند المعاملات الطبيعية:

الشكل رقم 02-49: مخطط المعايرة، عند فئة المعاملات الطبيعية



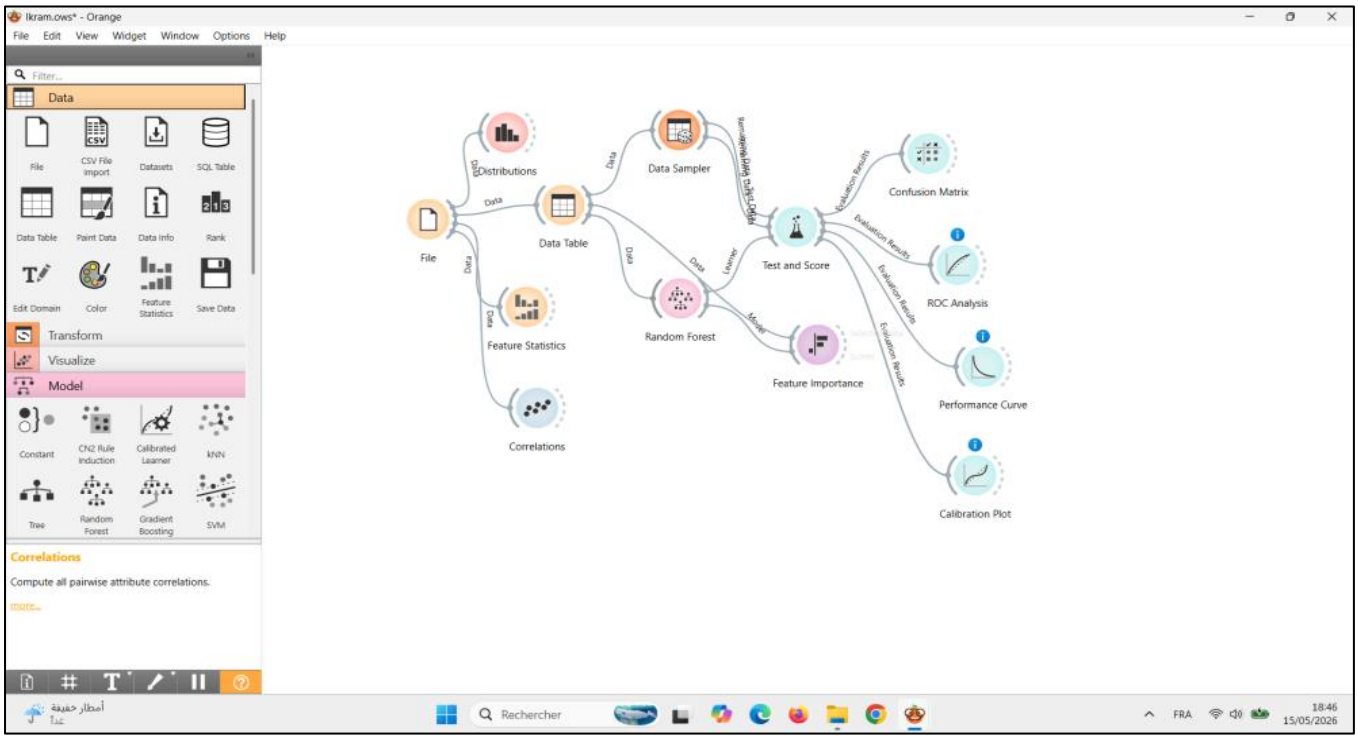
المصدر : مخرجات برنامج Orange

الاحظ من المنحنى وكما هو الحال مع الفئة 1 يأخذ المنحنى شكلاً سينياً، لكنه يحمل بعض الخصائص التي تميزه وتستحق الوقوف عندها.

- على المحور الأفقي تظهر الاحتمالات المتنبئ بها للفئة 0، فيما يعكس المحور العمودي مدى توافق هذه الاحتمالات مع القيم الفعلية. واللافت أن الارتفاع الحاد في المنحنى يبدأ من نقطة أبكر قليلاً عند حدود 0.25 مقارنة بـــ 0.3 في الفئة 1، وهذا الفارق البسيط يحمل دلالة واضحة، فالنموذج يتعرف على المعاملات الطبيعية بحسم أسرع، وهو أمر منطقي لأن أنماط المعاملات العادية أكثر اتساقاً وتكراراً في بيانات التدريب مقارنة بأنماط الاحتيال المتنوعة.
- –في المنطقة الوسطى بين 0.25 و0.65 يعلو المنحنى فوق الخط المثالي بصورة مشابهة للفئة 1، غير أن الصعود هنا أكثر انحداراً وحدة، مما يعني أن النموذج أقل تردداً حين يتعلق الأمر بالحكم على المعاملة الطبيعية.
- وعند تجاوز عتبة 0.65 تتركز غالبية المعاملات الطبيعية البالغة 33،756 معاملة مصنفة بشكل صحيح، وهو ما يتجلى في قيمة النوعية 0.917 التي حققها النموذج. وإجمالاً تكشف المقارنة بين المنحنيين عن نموذج يتعامل مع الفئتين بكفاءة متوازنة، سريع الحسم مع المعاملات الطبيعية ومتأنٍ مع حالات الاحتيال، وهي بالضبط الصفات المطلوبة في أي نظام موثوق لاكتشاف الاحتيال المالي.

1. وفي الأخير وبعد الانتهاء من مراحل تصميم أنموذج خوارزمية الغابة العشوائية، نعرض المخطط العام (Workflow) لسير العمل الكامل لأنموذج داخل بيئة الدراسة. وذلك بهدف تقديم نظرة شاملة ومتكاملة عن كيفية ترابط جميع المراحل، باستخدام أدوات Orange الوظيفية، وصولا للنتائج النهائية.

الشكل رقم 02-50: سير العمل النهائي لأنموذج خوارزمية الغابة العشوائية داخل برنامج (Orange data mining)

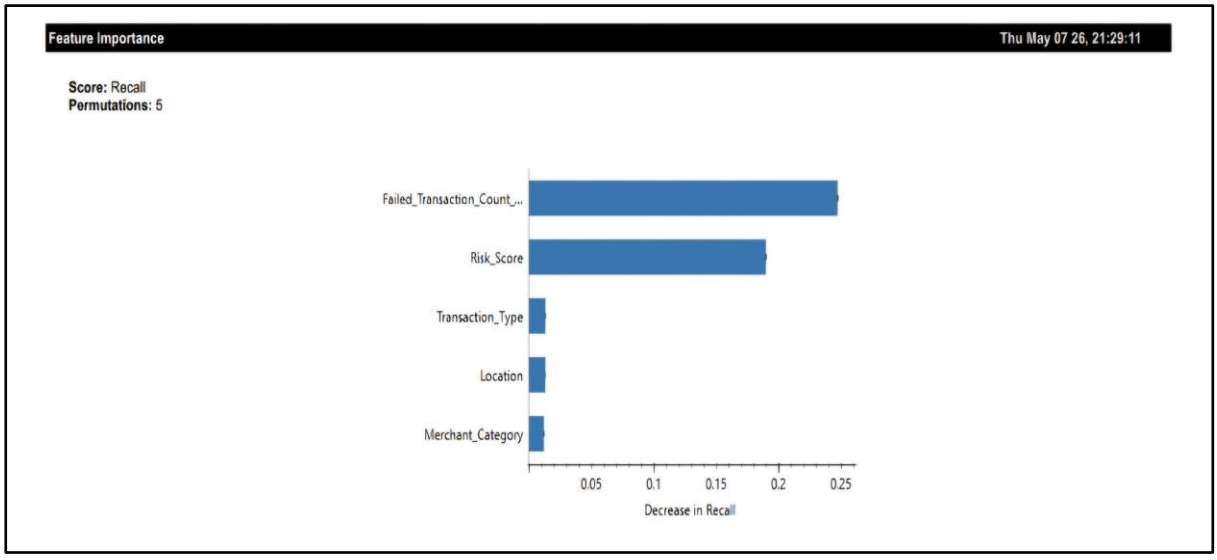


المصدر : مخرجات برنامج Orange

المطلب الرابع: تحليل المتغيرات الأكثر تأثيرا في كشف الاحتيال

تم اســـتخدام الأداة الوظيفية (widget Feature Importance) لبرامج (Orange data mining) لترتيب المتغيرات المستقلة تنازليا، حسب مساهمتها في التنبؤ بالاحتيال، حيت قمنا باستعراض أهم 5 متغيرات الأكثر تأثيرا وهو موضحة في الشكل التالي:

الشكل رقم 02-51: أهمية المتغيرات لنموذج الغابة العشوائية باستخدام مقياس (Recall) مع 5 تبديلات



المصدر : مخرجات برنامج (Orange)

يوضح هذا الشكل البياني أهمية المتغيرات لنموذج الغابة العشوائية باستخدام مقياس (Recall) مع 5 تبديلات ويهدف هدا التحليل الى تحديد مدى تأثير كل متغير على قدرة النموذج في اكتشاف حالات الاحتيال بشكل صحيح خاصة الحالات الإيجابية:

- عدد المعاملات الفاشلة خلال 7 أيام (**Failed_Transaction_Count**): تظهر النتائج ان متغير عدد المعاملات الفاشلة خلال 7 ايام يعد العامل الأكثر تأثيرا في اداء النموذج، حيث يؤدي حذف هدا المتغير الى انخفاض واضح في قيمة Recallبأكثر من 0,25، ويعكس ان هدا الدور المحوري ان تكرار فشل المعاملات خلال الفترة الزمنية قصيرة يعتبر مؤشرا قويا على السلوك الاحتيالي، اذ يحاول غالبا المحتال تنفيذ عدة محاولات فاشلة قبل نجاح عملية مشبوهة، مما يجعل هدا المتغير ذا قدرة تفسيرية عالية داخل النموذج. مما يجعله **الركيزة** الأساسية في اكتشاف الاحتيال
- درجة خطر الاحتيال المحسوبة للمعاملة (**Risk_Score**): يحتل المرتبة الثانية بانخفاض يقترب من 0.20 عند حذفه، وهو متغير مُركَّب يجمع مؤشرات المخاطرة ويُعزز قدرة النموذج على التصنيف الدقيق حيث يجمع عدة مؤشرات سلوكية ومالية، مما يجعله تلخيصا كميا لعدة انماط احتيالية محتملة، وبالتالي فهو يعزز قدرة النموذج على التعميم وتحسين الكشف عن الحالات المعقدة التي لا يمكن لمتغير واحد بسيط تفسيرها.
- **نوع المعاملة (Transaction_Type) والموقع الجغرافي للمعاملة (Location) ونوع التاجر (Merchant_Category)**: فتظهر تأثيرا اقل نسبيا، حيث لا يتجاوز الانخفاض في ال Recallعند حذفها 0.03 لكل منها ومع ذلك، فان دورها يبقى مهما على المستوى القياسي، اذ تساهم في اضافة معلومات وصفية تساعد النموذج على التمييز بين الانماط الطبيعية والغير طبيعية، خصوصا في الحالات الحدودية.

بناءا على هده النتائج يتضح ان اداء النموذج في اكتشاف الاحتيال يرتكز بشكل كبير على المتغيرات السلوكية المركزة متل عدد المعاملات الفاشلة ودرجة الخطر، في حين تؤدي المتغيرات الاخرى دورا تكميليا داعما لتحسين الاستقرار العام للنموذج. كما ان قيمة (Recall) الموزونة المحققة البالغة 0.958، تؤكد فعالية النموذج في تقليل حالات الفشل في اكتشاف الاحتيال، وهو ما يعد هدفا اساسيا في انظمة كشف الاحتيال المالي الالكتروني.

خلاصة الفصل الثاني:

في ختام هذا الفصـــل تمكنا من تصـــميم أنموذج عملي للكشـــف عن الاحتيال المالي الالكتروني باســـتخدام خوارزمية الغابة العشـــوائية (Random Forest)، عبر البيئة البرمجية (Orange data mining)، بالاعتماد على مجموعة بيانات محاكاة اصطناعية (Fraud detection Transactions Dataset) من (kaggle)، والتي تم اختيارها بطريقة قصـــدية لكونها مناســـبة لأهداف الدراســـة، حيت تم اتباع منهجية منظمة مرت بمراحل: امتدت من جمع البيانات، الى تقييم أداء انموذج الدراسة، حيت أظهرت النتائج قدرة انموذج خوارزمية تعلم الالة المصمم: على تحقيق دقة كلية 95،8% واستذكار بلغ 95،8% ودقة إيجابية بلغت 95.8% وقيمة Auc 99.6% ومعامل ارتباط ما تيوس بلغ 90،4% مما يؤكد فعاليته في كشـــف الاحتيال والتعرف على المعاملات الاحتيالية، كما اظهر تحليل (Feature Importance) المتغيرات الأكثر تأثيرا في الكشـــف عن الاحتيال، حيت يمكن اعتماد هده المنهجية كأداة مســـاعدة للمؤسـسـات المالية في أنظمة الإنذار المبكر بالاعتماد على بيانات واقعية حقيقية، وهدا ما يؤكد في النهاية موضـوع دراستنا حول دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني مما يؤدي الى دعم المؤسسات المالية ويعزز أنظمة الحماية.

الخاتمة

خاتمة عامة

من خلال دراستنا لموضوع دور خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني، واعتمادا على منهجية وصفية في الجانب النظري، ومنهج تجريبي في الجانب التطبيقي، وبالاستعانة بقاعدة بيانات اصطناعية محاكاة من منصة (kaggle)، بعنوان (Fraud detection Transactions Dataset)، وتطبيق خوارزمية الغابة العشوائية (Random Forest) عبر بيئة برنامج (orange data Mining)، وذلك بهدف تصميم أنموذج قادر على كشف العمليات الاحتيالية وتقييم اداءه.

فبعد معالجتنا وتحليلنا لمختلف جوانب الموضوع النظرية والتطبيقية، واسقاط الجانب النظري على الجانب التطبيقي الخاص بتصميم أنموذج بخوارزمية تعلم الالة، خوارزمية الغابة العشوائية للكشف عن الاحتيال المالي الالكتروني، ومن اجل الإجابة على الإشكالية الرئيسية المطروحة: كيف تساهم خوارزميات تعلم الالة في كشف الاحتيال المالي الالكتروني؟ تم التوصل الى مجموعة من النتائج، نعرضها في المستويات التالية.

أولا: نتائج اختبار فرضيات الدراسة

1.اختبار الفرضية الأولى:

- **الفرضية (H0):**

لا يحقق انموذج خوارزمية الغابة العشوائية اداء كافيا في اكتشاف الاحتيال المالي الالكتروني بناءا على مقاييس تقييم الأداء.

- **الفرضية (H1):**

يحقق انموذج خوارزمية الغابة العشوائية اداء كافيا في اكتشاف الاحتيال المالي الالكتروني بناءا على مقاييس تقييم الأداء.

❖ **النتيجة:**

تم رفض الفرضية الصفرية (H0) وقبول الفرضية البديلة (H1)، حيت اثبت المقاييس تفوق الانموذج وقدرته العالية على اكتشاف الاحتيال المالي الالكتروني. ، ودلك من خلال النتائج التطبيقية التي اظهرت ان انموذج الغابة العشوائية، حقق دقة كلية بلغت (95,8%)، وقيمة استذكار بلغت (95,8%) , وقيمة AUC (99.6%)، معامل ارتباط ما تيوس (90,4%)، وهي مقاييس تشير الى أداء عال جدا، خاصة في قدرته على اكتشاف المعاملات الاحتيالية الفعلية، مما يؤكد فعالية الخوارزمية في هدا المجال

2.اختبار الفرضية الثانية:

- **الفرضية (H0):** لا يظهر تحليل أهمية المتغيرات لنموذج الغابة العشوائية ان بعض خصائص المعاملات المالية، تؤدي دورا مهما في كشف الاحتيال المالي الالكتروني

- **الفرضـــية (H1):** يظهر تحليل أهمية المتغيرات لنموذج الغابة العشـــوائية ان بعض خصـــائص المعاملات المالية، تؤدي دورا مهما في كشف الاحتيال المالي الالكتروني.

❖ **النتيجة:**

تم رفض الفرضـية الصـفرية (H0) وقبول الفرضـية البديلة (H1)، ، فقد اظهر تحليل (Feature Importance) ان المتغيرات الأكثر تأثيرا في التنبؤ بالاحتيال هي:

1. (Failed – Transaction – Count -7 d): عدد المعاملات الفاشلة خلال 7 أيام
2. (Risk – Score): درجة خطر الاحتيال المحسوبة للمعاملة
3. (Transaction – Type): نوع المعاملة (اونلاين، المتجر، ATM...)
4. (Location): الموقع الجغرافي للمعاملة
5. (Merchant – Category): نوع التاجر (تجزئة، طعام، سفر ....)

وهدا يؤكد ان خصـائص المعاملات المالية ليست متساوية الأهمية، بل هناك خصـائص محددة يجب التركيز عليها في أنظمة الإنذار المبكر.

ثانيا: النتائج العامة للدراسة:

من خلال الدراســة التطبيقية وتصــميم أنموذج لكشــف الاحتيال المالي الالكتروني باســتخدام خوارزمية الغابة العشوائية، توصلنا الى النتائج التالية:

1. تمكن نموذج خوارزمية الغابة العشوائية من تحقيق دقة تمييز عالية بين المعاملات السليمة والاحتيالية، مما يجعله أداة فعالة وموثوقة يمكن الاعتماد عليها كأداة مساعدة في أنظمة كشف الاحتيال المالي الالكتروني.

2. ساهمت بيئة برنامج (orange data Mining) بشكل كبير في تبسيط عملية بناء النموذج وتقييمه، بفضل واجهته الرسومية وادواته الوظيفية المتكاملة (widgets) التي غنتنا عن كتابة اكواد برمجية معقدة.

3. كشف تحليل أهمية المتغيرات (Feature Importance) ان متغيرات: عدد المعاملات الفاشلة خلال 7 أيام، درجة خطر الاحتيال المحســوبة للمعاملة، نوع المعاملة (اونلاين، المتجر، ATM...)، الموقع الجغرافي للمعاملة، نوع التاجر (تجزئة، طعام، سفر ....) .

4. التحقق المتقاطع ب 5 طيات (Fould Cross-5) أسـهم في الحصـول على تقييم اكتر دقة وواقعية لأداء النموذج، مقارنة بالاعتماد على تقسيم عشواءي واحد للبيانات.

5. رغم ان البيانات المستخدمة اصطناعية الا ان نتائج النموذج كانت مشجعة للغاية، مما يفتح المجال لتطبيق نفس المنهجية على بيانات حقيقية بعد توفيرها.

6. اثبت الدراسـة ان خوارزميات تعلم الالة لا تقتصـر فائدتها على كشـف الاحتيال فحسـب، بل تمتد الى تحليل وفهم أنماط الاحتيال من خلال تحديد اهم المتغيرات المرتبطة به، مما يساعد في تطوير سياسات وقائية اكتر فعالية.

7. أنموذج تعلم الالة المصـــمم يمتل اثباتا علميا يبرز إمكانية توظيف خوارزميات تعلم الالة ودورها في كشـــف الاحتيال المالي الالكتروني في كشف الاحتيال المالي الالكتروني، ورغم النتائج المرتفعة تبقى هذه النتائج مرتبطة بطبيعة بيانات الدراســـة المســـتخدمة، لذلك لا يمكن تعميمها بشـــكل كامل على البيئات المالية الحقيقية الا بعد اختبار النموذج على بيانات واقعية اكتر تعقيدا.

ثالثا: الاقتراحات

من خلال النتائج المتوصل اليها يمكن صياغة الاقتراحات التالية:

1. اعتماد نموذج خوارزمية الغابة العشـوائية كنظام مسـاعد في المؤسـسـات المالية الجزائرية (البنوك، شـركات الدفع الالكتروني، التجارة الالكترونية) للكشـــف الاولي عن المعاملات المشـــبوهة، على ان تفحص التنبيهات يدويا قبل اتخاذ أي اجراء.

2. تطوير قاعدة بيانات وطنية للمعاملات المالية الالكترونية (مع الحفاظ على الخصـوصـية والسرية) لتغذية متل هده النماذج ببيانات حقيقية، مما يزيد من دقتها وفعاليتها في البيئة الجزائرية.

3. تشـجيع المؤسسـات المالية على الاستثمار في أدوات تعلم الالة مفتوحة المصـدر متل:(Orange), نظرا لانخفاض تكلفتها وسهولة استخدامها مقارنة بالحلول المبرمجة من الصفر .

4. ادراج موضـــوع كشـــف الاحتيال المالي الالكتروني باســـتخدام تعلم الالة في المناهج الجامعية خاصـــة في كليات العلوم الاقتصـــادية والتجارية وعلوم التسـيير، بالإضـــافة الى تعلم تقنيات الذكاء الاصـــطناعي وتعلم الالة، للإعداد كوادر وطنية قادرة على مواجهة هده التهديدات في ظل تزايد المعاملات المالية الرقمية والتكنولوجيا المالية.

5. التنسيق بين البنوك وهيئات الرقابة المالية لا نشاء نظام انذار مبكر موحد يعتمد على خوارزميات تعلم الالة، مما يسمح بتبادل المعلومات حول أنماط الاحتيال المكتشفة.

رابعا: افاق الدراسة (النظرة المستقبلية)

حاولنا من خلال هده الدراســـة الالمام بجوانب الموضـــوع النظرية والتطبيقية قدر الإمكان، ومن اجل مواصـــلة البحت في هدا الموضوع نقترح بعض المواضيع كأفاق مستقبلية للدراسة واهمها:

1. الاختبار على بيانات حقيقية: تطبيق نفس المنهجية على بيانات حقيقية من احدى المؤسـسـات المالية الجزائرية (بنك، شركة دفع الكتروني) بعد التنسيق معها، وقياس الفجوة بين الأداء على البيانات الاصطناعية والحقيقية.

2. بناء نظام انذار مبكر في الوقت الفعلي (Real -time Detection): تطوير نموذج يعمل بشـــكل مباشـــر على تدفق المعاملات (Streaming Data) واصدار تنبيهات فورية عند اكتشاف معاملات مالية مشبوهة.

3. تطبيق تقنيات شرح النماذج (EXplainable AI): استخدام أدوات متل (SHAP) أو (LIME) لتفسير سبب تصنيف معاملة معينة كاحتيالية، مما يزيد من شفافية النموذج وقبوله من قبل المؤسسات المالية.

4. **دمج المزيد من الميزات (Feature Engineering):** انشـاء متغيرات مركبة جديدة متل: تكرار المعاملات خلال السـاعة او الانحراف المعياري لمبالغ المعاملات السـابقة او نسـبة المبلغ الى متوسـط الرصـيد لتعزيز قدرة النموذج على التمييز والكشف على المعاملات الاحتيالية.
5. **معالجة عدم توازن البيانات (Imbalanced data):** من خلال استخدام تقنيات متل: (SMOTE) (Synthetic Minority Over −Sampling Technique) داخل بيئـة (orange) أو (python) لتحسين قدرة النموذج على اكتشاف المعاملات الاحتيالية النادرة.
6. **تطبيق خوارزميات تعلم الة أخرى:** ومقارنة اداءها مع خوارزمية الغابة العشوائية.
7. **توسـيع نطاق الدراسـة ليشـمل أنواعا أخرى من الاحتيال:** متل الاحتيال في قطاع التامين، الاحتيال في العملات المشفرة، او الاحتيال عبر منصات التمويل الجماعي، مع تكييف المتغيرات حسب كل مجال.

قائمة المصادر والمراجع

- **المراجع باللغة العربية:**

1. أبو بكر التواتي، الياس مالك قرادي، **جرائم النصب والاحتيال الإلكتروني في التشريع الجزائري**، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، المركز الجامعي المقاوم الشيخ آمود بن مختار –إيليزي– 2025.
2. اسية بن بوعزيز ميلود بن عبد العزيز، **جريمة الاحتيال المالي في ظل تكنولوجيا المعلومات**، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد6،1 / 2024.
3. بشرى فاضل الطائي، حسين فخري سلمان، **دور التخصص المهني لشركات التدقيق في الكشف عن الاحتيال في القوائم المالية**، مجلة العلوم الاقتصادية والإدارية، المجلد 25، العدد 114، سنة 2019.
4. بن خضرة حميدة، بضياف صالح، **دور الذكاء الاصطناعي في الكشف والحد من الاحتيال على البطاقات الائتمانية البنكية على المستوى الدولي**، مجلة الابداع، المجلد 14، العدد 2، 07\2024.
5. تامر السيد احمد السيد قناوي، **اتر استخدام العملات المشفرة على جريمة الاحتيال الالكتروني**، المجلة القانونية الاقتصادية، المجلد 37، العدد53، ديسمبر2025.
6. جمال الدين عباس، **اليات الحد من الانحرافات في الأسواق المالية دراسة تحليلية تقييمية لعدد من الأسواق المختارة**، أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في علوم التسيير تخصص إدارة مالية، جامعة البشير الإبراهيمي برج بوعريريج، 2024.
7. حياة هراكي، **واقع جريمة الاحتيال الالكتروني في التجارة الالكترونية**، مجلة التغير الاجتماعي، المجلد 8، العدد 02، 2023/02.
8. حمز خضري، عشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري, مجلة الدارسات القانونية و السياسية,المجلد,6العدد ,20جوان ,2020.
9. خراز عبد الحق، شاربي بلقاسم، **الذكاء الاصطناعي وتطوير الأداء الرياضي: من التحليل البدني والتكتيكي الى الاعداد الفني والذهني**، مجلة روافد للدراسات والابحاث في علوم الرياضة، المجلد 6، العدد 1، 2026.
10. خير الدين بوزرب، عبد الرؤف عباسي، **الذكاء الاصطناعي كأداة استراتيجية في مكافحة غسيل الأموال في البنوك: عرض تجربة بنك (hsbc) وبنك (Danske)**، مجلة دراسات اقتصادية، المجلد 19، العدد 3، 2025.
11. خيرة حنش، احمد بن الشين، **الذكاء الاصطناعي بين الابتكار والمسؤولية الأخلاقية في البحت العلمي**، مجلة العلوم الإسلامية والحضارة، المجلد 10، العدد 2، 2025.
12. دعاء المحيتاوي، وآخرون، **نموذج محسن في مسالة كشف الاحتيال لبطاقات الائتمان باستخدام خورزميات تعلم الالة، منشورات المعهد العالي للعلوم التطبيقية والتكنولوجيا**، دمشق، 2019/7.
13. نصيف جاسم الجبوري، صلاح هادي محمد الخالدي، **دور المحاسبة القضائية في اكتشاف عمليات الاحتيال المالي**، مجلة العلوم الاقتصادية والإدارية، المجلد: 19، العدد 70، سنة 2013.
14. ريم محمد محمود عبد المنعم واخرون، **اثر التنبؤ بالأرباح المستقبلية باستخدام خوارزميات تعلم الالة كإحدى تقنيات الذكاء الاصطناعي على تعزيز ثقة المستثمرين– دراسة تطبيقية**، مجلة الشروق للعلوم التجارية، العدد17، ماي 2025.

15. زهواني مروة، **تطبيقات نماذج الذكاء الاصطناعي للتنبؤ بمخاطر التعثر المالي في المؤسسة الاقتصادية – دراسة حالة–**، أطروحة مقدمة لاستكمال متطلبات نيل شهادة الدكتوراه في العلوم الاقتصادية تخصص نقدي وبنكي، جامعة غرداية، جوان 2022.

16. سامر هايل الصباغ، حسين احمد دحدوح، **مدى التزام مدققي الحسابات بتقييم عوامل مخاطر الأخطاء الجوهرية الناجمة عن الاحتيال (دراسة ميدانية في هيئة الأوراق والأسواق المالية السورية)**، 12 العدد 2، سنة 2016.

17. سامية بوضياف، فيصل بهلولي، **استخدام الذكاء الاصطناعي لدراسة علاقة أسعار النفط، الصرف، الذهب، بالتضخم والتنبؤ به في الفترة الممتدة من جوان 2006 –أفريل 2020**، مجلة (les cahiers du cread), المجلد 39 ، العدد 1، 2023.

18. عبد الكافي مريم، بورابابة صورية، **جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية**، مجلة القانون والعلوم السياسية، المجلد: 08، العدد01، 2022/02.

19. عبد الكريم حرز الله، **التعلم الالي كجزء من الذكاء الاصطناعي**، مجلة العلوم والتكنولوجيا، العدد التجريبي، ماي 2019.

20. علي بن الضب، **دور الذكاء الاصطناعي وتعلم الالة في تعزيز كشف الاحتيال على البطاقات الائتمانية**، صندوق النقد العربي، العدد 23، 2023.

21. علي لؤي ياسين، **استخدام طرائق التعلم الالي لاكتشاف الشذوذ في مجموعة البيانات**، مذكرة ماجيستير في هندسة البرمجيات ونظم المعلومات، كلية الهندسة المعلوماتية، جامعة البحت، سوريا.

22. عون الله سعاد، عامري رضوان، **مخاطر وتداعيات تداول العملات المشفرة على استقرار القطاع المالي خلال الفترة 2017–2021**، مجلة اقتصاديات شمال افريقيا، المجلد 19، العدد 31, 2023/3.

23. فراحي فضيلة، **نموذج تعلم الي لكشف الاحتيال في بطاقة الائتمان– تطبيق عملي على منصة تفاعلية**، مجلة دفاتر اقتصادية، المجلد 16، العدد1. 2025.

24. فرحاني رزيقة، بالرايس زينب، **ضحايا النصب والاحتيال في ظل انتشار وتوسع التجارة الالكترونية دراسة ميدانية على عينة من الوسط الجامعي**، جامعة الشيخ العربي التبسي، مرجع سبق دكره، ص 51–52

25. قاسمي زهيرة، **موقف القانون الجزائري من التعامل بالعملات الرقمية بين الضرورة والمخاطر**، مجلة افاق علمية، المجلد 16، العدد 2، 2024/10.

26. كريم محمد محافظ حافظ توفيق القاضي، **اتر تطبيق تقنيات التعلم الالي على مراحل عملية المراجعة الخارجية للكشف عن الاحتيال المحاسبي – دليل عملي من الشركات المقيدة بالبورصة المصرية –** , المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد17 , العدد 1, 2025/3.

27. لمى عدنان عوكل، **دور استخدام خوارزميات الذكاء الصنعي في عمليات ضبط الجودة دراسة حالة –** مصنع الميسور للصناعات البلاستكية– سوريا– ريف دمشق، بحث مقدم لنيل درجة الماجيستير في إدارة الجودة، الجامعة الافتراضية السورية، 2021.

28. مرزوق آمال، **العملات المشفرة: فرص وتحديات استخدامها**، مجلة البشائر الاقتصادية، المجلد 6، العدد 2، ديسمبر، 2020.

29. مزاري نصر الدين، **دور خوارزميات التعلم الالي في استهداف الإعلانات: تهديد للخصوصية ام ضرورة تجارية؟ دراسة حالة (Facebook abs)**، مجلة التشريع الإعلامي، المجلد 3، العدد 1، 2024.

30. مناصرة يوسف، **الاحتيال المالي السيبراني باستخدام الأصول المشفرة**، مجلة صوت القانون، المجلد 10، العدد1، 2024/1/24.

31. ميلاد وزان، **تعلم الالة وعلم البيانات – الأساسيات والمفاهيم والخورزميات والادوات**، (ترجمة علاء طعيمة)، عمان: دار المناهج للنشر والتوزيع، 2024.

32. وائل محمد نصيرات، غادة عبد الرحمن الطريف، **" جريمة الاحتيال عبر شبكة المعلومات الدولية: دراسة مقارنة النظام السعودي والقانون الأردني**، مجلة دفاتر السياسية والقانون، العدد 19، جوان 2018، ص 98

2. المرجع باللغة الأجنبية:

1. ABDULLAHI RABI 'U, NOORHAYATI MANSOR. "FRAUD TRIANGLE THEORY AND FRAUD DIAMOND THEORY. UNDERSTANDING THE CONVERGENT AND DIVERGENT FOR FUTURE RESARCHE." INTERNATIONAL JOURNAL OF ACADEMIC RESARCH IN ACCOUNTING, FINANCE AND MANAGMENT SCIENCES, VOL5, NO4 ,2015
2. ANTONIE BOUVERET, CYBER RISK FOR THE FINANCIAL SECTOR: A FRAMEWORK FOR QUANTITATIVE ASSESSMENT, IMF WORKING PAPER, INTERNATIONAL MONETARY FUND, WP /18/143. JUNE 2018
3. ASSOCIATION OF SUPERVISORS OF BANKS OF THE AMERICAS (ASBA). DIGITAL FRAUD IN BANKING .TRENDS AND PRACTICES FOR MITIGATION. EXECUTIVE SUMMARY
4. ABAS KADAR, AI-POWERED PHISHING DEEPFAKE AND THE NEW DATA GOVERNANCE IMPERATIVE,21/01/2026, RETRIEDAT:18/02/2026FROM [https://www.researchgate.net/publicati /399984480_aipowered_phishing_ deepfakes_ and_the_new_data_governance_imperative]
5. AMER F.A.H. ALNUAIMI, ET AL, AN OVERVIEW OF MACHINE LEARNING CLSSIFICATION TECHNIQUES, JOURNAL BIO WEB OF CONFERENCES, VOL 97
6. A.C.Y. HONG, ET AL, PREDICTION OF US AIRLINE PASSENGER SATISFACTION USING MACHINE LEARNING ALGORITHMS, DATA ANALYTICS AND APPLIED MATHEMATICS (DAAM), VOL 4, N 1,2023
7. ALEX SMOLA, S.V.N. VISHWANATHAN, INTRODUCTION TO MACHINE LEARNING, CAMBRIDGE UNIVERSITY PRESS,2008
8. ANTHONY OWEN, SARAH TEMPLER, INTELLIGENT FRAUD DETECTION: DESIGN A MACHINE LEARNING FRAMEWORK FOR REAL-TIME FRAUD PREVENTION IN TRANSACTIONS, RESARCHGATE ,7/2022
9. ANAVENA RAJKUMAR, MACHINE LEARNING TECHNIQUES FOR REAL-TIME FRAUD DETECTION IN FINANCIAL, LLOYD BUSINESS REVIEW, VOL 4, N1
10. ARIMONDO SCRIVANO, FRAUD DETECTION PIPELINE USING MACHINE LEARNING: METHODS, APPLICATIONS AND FUTURE DIRECTIONS, RESACHGATE, 7/2025
11. AHMAD ABUASHOUR, ET AL, COMPARATIVE STUDY OF CLASSIFICATION MECHANISMS OF MACHINE LEARNING ON MULTIPLE DATA MINING TOOL KITS, AMERICAN JOURNAL OF BIOMEDICAL SCIENCE & RESEARCH, VOL 22, N 1, ISSN :2642 -1747,4 /2024
12. BASEL COMMITTEE ON BANKING SUPERVISION, DIGITAL FRAUD AND BANKING: SUPERVISORY AND FINANCIAL STABILITY IMPLICATIONS, DISCUSSION PAPER, BANK OF INTERNATIONAL SETTLEMENTS, NOVEMBER 2023, P1, ISBAN 92-9197- 978-92-9259-709-2 (online)
13. BADIAA CHIFA, KERROM NESRINE, THE LEGAL REGULATION OF ELECTRONIC BANKING HOW DOES THE MONETARY AND BANKING LOW 09 23 ENHANCE TRUST IN DIGITAL TRANSACTIONS, JOURNAL OF LEGAL AND ECONOMIC RESEARCH, VOLUME 08, ISSUE: 02, 6/ 2025
14. BEAKCHEOL JANG, ET AL,Q-LEARNING ALGORITHMS: A COMPREHENSIVE CLASSIFICATION AND APPLICATIONS,IEEE ACCESS,VOL7,2019,DOI : 10.1109/access.2019.2941229

15. BIN GU, ET AL, NEW INCREMENTAL LEARNING ALGORITHM FOR SEMI -SUPERVISED SUPPORT VECTOR MACHINE, KDD 2018, LONDON ,8 /2018
16. BEKADDOUR FATIMA ZAHRA, STOCK PRICE CLASSIFICATION USING FINANCIAL INDICATORS FROM 10 -K REPORTS: A COMPARATIVE STUDY BETWEEN NEURAL NETWORKS (NN) AND LOGISTIC REGRESSION (LR), JOURNAL OF FINANCE, INVESTMENT AND SUSTAINABLE DEVELOPMENT, VOLUME :10, NEMBER :01, JUNE 2025
17. C. MALLESHA, M. HYMAVATHI, A REVIEW ON AI AND FRAUD DETECTION IN ACCOUNTIN: REDUCING RISKS AND ENHANCING FINANCIAL SECURITY, ACADEMY OF ACCOUNTING AND FINANCIAL STUDIES JOURNAL, VOLUME 28, ISSUE 2, 2024
18. CHRISTOPHER.M. BISHOP, PATTERN RECOGNITION AND MACHINE LEARNING, INFORMATIQUE SCIENCE AND STATISTICS, NEW YORK: SPRINGER -VERLAG ,2006
19. CHIE IKEDA, A NEW FEATURE ENGINEERING FRAMEWORK FOR FINANCIAL CYBER FRAUD DETECTION USING MACHINE LEARNING AND DEEP LEARNING, PHD DISSERTATION, SCHOOL OF COMPUTING AND DIGITAL MEDIA, LONDON METROPOLITAN UNIVERSITY, 9/2022
20. DIMOSTHENIS CHRYSIKOS ,INTERNATIONAL LEGAL FRAMEWORKS FOR COMBATING CYBERCRIME:THE UNODC PERSPECTIVE ,PRESENTATION NINTH MEETING OF OAS REMJA WORKING GROUP ON CYBERCRIME,WASHINGTON D.C,DECEMBER 2016,FROM : https://www.oas.org/juridico/pdfs/cyb9-unodc-dec16 -v1.pdf
21. D.DIVAY, ET AL, ARTIFICIAL INTELLIGENCE IN FINANCE, CONFERENCE PAPER ON INNOVATION AND TRANSFORMATION: REVOLUTIONIZING THE BUSINESS WORLD WITH BREAKTHROUGH CREATIVITY, SRI RAMAKRISHNA COLLEGE OF ARTS AND SCIENCE, COIMBATORE, INDIA,2 /2024
22. DAL POZZOLO, ADAPTIVE MACHINE LEARNING FOR CREDIT CARD FRAUD DETECTION, A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR BHD DEGREE IN COMPUTER SCIENCE, MACHINE LEARNING GROUP, UNIVERSITE LIBRE DE BRUXELLES, 12 /2015
23. FATF, EGMONT GROUP, INTERPOL, ILLICITE FINANCIAL FLOWS FROM CYBER -ENABLED FRAUD, PARIS, NOVEMBER 2023
24. FAIZ RAHMAN SIDDIQ, BAMBANG SUTOPO, THE FRAUD HEXAGON AS AN ANALYTICAL FRAMEWORK FOR PREDICTING FINANCIAL STATEMENT FRAUD: A SYSTEMATIC LITERATURE REVIEW, JOURNAL OF RESEARCH TRENDS IN SOCIAL SCIENCES AND HUMANITIES, VOL 3, NO 2,2024
25. FARAH AICHA, FINANCIAL FRAUD IN THE ERA OF DIGITAL TRANSFORMATION, JOURNAL OF LEGAL AND POLICITICAL SCIENCE, VOL 62, N2, 07 /2025
26. FRANK ADELMAANN, ET AL, CYBER RISK AND FINANCIAL STABILITY:IT S A SMALL WORLD AFTER ALL, IMF STAFF DISCUSSION NOTE, SDN /20/07, DECEMBER 2020, FROM: https://www.imf.org/-/media/files/publications/sdn/2020/english/sdnea2020007.pdf
27. FAKHRA AKHTAR, ET AL, CREDIT CARD FRAUD DETECTION THROUGH MODEL TESTING USING ORANGE TOOL, INTERNATIONAL JOURNAL OF LATEST ENGINEERING AND MANAGEMENT RESEARCH, VOLUME 5, N 6, JUNE 2020
28. GEORGIOS L, VOUSINAS, ADVANCING THEORY OF FRAUD: THES.C.O.R.E. MODEL. JOURNAL OF FINANCIAL CRIME, VOL 26, NO 1,2019
29. GIUSEPPE VECCHIETTI, GAJENDRA LIYANAARACHCHI, GIAMPAOLO VIGLIA ,MANAGING DEEPFAKE WITH ARTIFICIAL INTELLIGENCE :INTRODUCING THE BUSINESS PRIVACY CALCULES,JOURNALOFBUSINESSRESARCHE,14/08/2024 ,doi .org : https://doi.org/10.1016/j.jbusres.2024.115010
30. GENNARO CORDASCO, LUISA GARGANO, COMMUNITY DETECTION VIA SEMI - SYNCHRONOUS LABEL PROPAGATION ALGORITHMS, IN 2010 IEEE INTERNATIONAL WORKSHOP ON BUSSINESS APPLICATION OF SOCIAL NETWORK ANALYSIS,2011,
31. GANESH KHEKARE, ET AL, A COMPREHENSIVE PERFORMANCE COMPARISON OF TRADITIONAL AND ENSEMBLE MACHINE LEARNING MODELS FOR ONLINE FRAUD DETECTION, ARXIV PREPRINT ARXIV: A COMPREHENSIVE PERFORMANCE :2509.17176 ,2025,
32. HESHAN GUAN, SIYING LI, QIAN WANG, OLEKSII LYULYOV, TETYANA PIMONENKO, « FINANCIAL FRAUD IDENTIFICTION OF THE COMPANIES BASED ON THE LOGISTIC REGRESSION MODEL." JOURNAL OF COMPETITIVENESS, VOL 14, NO 4,04/ 2022
33. HAO JIANG, ET AL, AN IMPROVED SARSA (λ) REINFORCEMENT LEARNING ALGORITHM FOR WIRELESS COMMUNICATION SYSTEMS, IEEE ACCESS, VOL7,2019, DOI: 10.1109/access.2019.2935255

34. HONGFANG ZHOUA, ET AL, A DEEP LEARNING HYBRID RNN-LSTM MODEL FOR CREDIT CARD FRAUD DETECTION, GOOGLE SCHOLAR, 12/2025, DOI: HTTPS://doi.org/10.21203/rs.3.rs-8327749/v1
35. INTERPOL, INTERPOL GLOBAL FINANCIAL FRAUD ASSESSMENT, MAY 2024
36. ISRAT JAHAN, ET AL, COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR SENTIMENT CLASSIFICATION IN SOCIAL MEDIA TEXT, WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS, VOL 23, N3
37. IOSCO, IOSCO STATEMENT ON ONLINE HARM,15 /12/ 2023, FROM: https:// www.iosco.org /library/pubdocs /pdf / ioscopd 752.pdf
38. JUN TAMURA, ET AL, STATISTICAL INFERENCE OF THE MATTHEWS CORRELATION COEFFICIENT FOR MULTICLASS CLASSIFICATION, ARXIV:2503.06450v1 [stat.ME] , 3/2025
39. JONATHAN KLESS, ET AL, PROBABILISTIC LABEL SPREADING: EFFICIENT AND CONSISTENT ESTIMATION OF SOFT LABELS WITH EPISTEMIC UNCERTAINTY ON GRAPHS, ARIVEX PREPRINT: 2602.04574 ,2026
40. JYOTHI. G, PAVANKUMAR G KULKARNI, ARTIFICIAL INTELLIGENCE IN FINANCE ;A LITERATURE REVIEW ,REVISTA DE CIENCIAS DE GESTION ;360,N10
41. JASELLA SAKWI YANTI, YOSSI DIANTIMALA, NURAINI A TESTING THE CROWES PENTAGON THEORY OF FRAUD ON FINANCIAL STATEMENT FRAUD, INTERNATIONAL JOURNAL OF MANAGEMENT, ACCOUNTING AND ECONOMICS, VOL 11,NO 3, 2024
42. KAREN ANN GILL, INSURANCE FRAUD: CAUSES CHARACTERISTICS AND PREVENTION THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY AT THE UNIVERSITY OF LEICESTER, ,9/2001
43. KHALIFA ALSENAANI, FRAUD DETECTION IN FINANCIAL SERVICES USING MACHINE LEARNING, DEGREE OF MASTER OF SCIENCE IN PROFESSIONAL STUDIES: DATA ANALYTICS, DEPARTMENT OF GRADUATE PROGRAMS & RESEARCH, ROCHESTER INSTITUTE OF TECHNOLOGY, 2022
44. LINA FERNANDES, FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES, ASIA PACIFIC JOURNAL OF MARKETING & MANAGEMENT REVIEW. VOL2, NO 3, MARCH 2013
45. LUDIVIA HERNANDEZ AROS, LUISA XIMENA BUSTAMANTE MOLANO, ET AL, FINANCIAL FRAUD DETECTION THROUGH THE APPLICATION OF MACHINE LEARNING TECHNIQUES: A LITERATURE REVIEW, JOURNAL HUMANITIES & SOCIAL SCIENCES COMMUNICATIONS, 3/09/2024, VOL11, ARTICLE NUMBRE 1130, DOI: https://doi.org/10.1057/s41599-024-03606−0
46. LARRY M. MANEVITZ, MALIK YOUSEF, ONE -CLASS SVMS FOR DOCUMENT CLASSIFICATION, JOURNAL OF MACHINE LEARNING RESARCH, VOL 2,12/2001
47. LEO BRIMANE, RANDOM FORESTS, MACHINE LEARNING, VOL 45, N 1, ,2001
48. MANURUNG, DANIEL T.H, NIKI HADIAN. "DETECTION FRAUD OF FINANCIAL STATEMENT WITH FRAUD OF FINANCIAL STATEMENT WITH FRAUD TRIANGLE." PROCEEDINGS OF 23RD INTERNATIONAL. BUSINESS *RESARCH CONFERENCE*, MARRIOTT HOTEL, MELBOURNE, AUSTRlIA. 18-20 NOV. 2013
49. MAMENE BESMA, IMAGES AND MANIFESTATIONS OF ELECTRONIC FRAUD ON PERSONS AND FUNDS THROUGH DIGITAL DATA, JOURNAL OF LAW, SOCIETY AND AUTHORITY, VOLUME 14, ISSUE 1, MARCH 2025
50. MOZAN. "10 COMMON TYPES OF BANK ACCOUNT FRAUD +PROTECTION TIPS.NOVEMBER 23, 2023. ACCESSED: /112/2026.AVAIBLE AT: http://www.getfocal.ai/
51. MARCOS R. MACHADO, IOANA FLORINA COITA, ET AL , 3D SYSTEMATIC LITERATURE REVIEW : AI,NETWORKS AND HUMANS TO DETECT CROWDFUNDING FRAUD ,10/2024
52. MARCOS R. MACHADO, IOANA FLORINA COITA, ET AL, CROWDFUNDING FRAUD DETECTION: A SYSTEMATIC REVIEW HIGHLIGHTS AI AND BLOCKCHAIN USING TOPIC MODELING, 9/2024
53. MARC SCHMITT, IVAN FLECHAIS, DIGITAL DECEPTION: GENERATIVE ARTIFICIAL INTELLIGENCE IN SOCIAL ENGINEERING AND PHISHING, JOURNAL ARTIFICIAL INTELLIGENCE REVIEW, VOL.57, NO 324 ,12. OCTOBER2024
54. MUSTAPHA M. HOBALLAH, ZAHRAA L. HAMMOUDA, HABIB M , AWADA ,ELECTRONIC FINANCIAL FRAUD:ABSTRACT ,DEFINATIONS,VULNERABILITIES, ISSUSES AND CAUSES,PROCEEDINGS OF POM BEIRUT 2019 ,06/2019, doi : http://dx.doi.org/10.14236/ewic/pom19.2
55. MERYEM TOUIL, LEGAL PROTECTION OF ELECTRONIC PAYMENT METHODES, JOURNAL OF LAW AND POLICITICAL SCIENCE, KHENCHELA UNIVERSITY, VOLUME 12, ISSUE 02,07/2025

56. MATTHEW N. O. SADIKU, ET AL, MACHINE LEARNING: AN OVERVIEW, INTERNATIONAL JOURNAL OF TREND IN SCIENTIFIC RESARCHE AND DEVELOPMENT, VOL 9, N 5, 9 /2025
57. M.VALVAN, S. RITA, PREDIACTIVE -ANALYSIS -BASED MACHINE LERNING MODEL FOR FRAUD DETECTION WITH BOOSTING CLASSIFICATION, JOURNAL COMPUTER SYSTEM SCIENCE AND ENGINEERING, VOL 45, N 1
58. MATTHEW N. O. SADIKU, ET AL, MACHINE LEARNING IN MEDIA AND ENTERTAINMENT, INTERNATIONAL JOURNAL OF TREND IN SCIENTIFIC RESARCH AND DEVELOPMENT, VOL 9, ISSUE 6, NOV -DEC 2025
59. MARKUS M. BREUNIG, ET AL, LOF: IDENTIFYING DENSITY -BASED LOCAL OUTLIERS, IN PROCEEDINGS OF THE 2000 ACM SIGMOD INTERNATIONAL CONFERENCE ON MANAGMENT OF DATA, DALLAS, TEXAS.USA,2000
60. MASSIH -REZA AMINI, ET AL, SELF -TRAINING: A SURVEY, NEUROCOMPUTING, VOL 616, N 128904,2025
61. MATTHIAS LEHMANN, THE DEFINITIVE GUIDE TO POLICY GRADIENTS IN DEEP REINFORCEMENT LEARNING: THEORY, ALGORITHMS AND IMPLEMENTATIONS, ARIVEX PREPRINT, ARIVEX: 2401.13662.,2024
62. MOHAMMED NAJIM UDDIN, FRAUDULENT TRANSACTION DETECTION AND PREVENTION USING DEEP NEURAL NETWORKS, THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF RESEARCH CENTRAL QUEENSLAND UNIVERSITY, SCHOOL OF ENGINEERING AND TECHNOLOGY, AUSTRALIA, 2؛ /2024
63. MOHAMED KAMEL ALDIN ISMAIL, HARNESSING AI FOR NEXT -GENERATION FINANCIAL FRAUD DETECTION: A DATA-DRIVEN REVOLUTION, JOURNAL OF ECOHUMANISM, VOL 3,N 7,2024
64. MOHAMMED MAABDEH, RUBA OBIEDAT, DEVELOPING A MODEL TO PREDICT DEFAULTING CREDIT CARD CLIENTS USING BUSINESS INTELLIGENCE TECHNIQUES, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON ADVANCED RESEARCH IN MANAGEMENT BUSINESS AND FINANCE, Vol. 1, ISSUE. 1, 2024
65. OLIVIER COLLIOT, MACHINE LEARNING FOR BRAIN DISORDERS, NEUROMETHODS, VOL 197, HUMAN PRESS, NEW YORK ,2023
66. PEI SHYUAN LEE, MAJDI OWDA, KEELEY CROCKETT, THE DETECTION OF FRAUD ACTIVITIES ON THE STOCK MARKET THROUGH FORWARD ANALYSIS METHODOLOGY OF FINANCIAL DISCUSSION BOARDS, THE MANCHESTER METROPOLITAN UNIVERSITY
67. POOGA KAUSHIK, ET AL," FINANCIAL FRAUD AND MANIPULATION: THE MALICIOUS USE OF DEEPFAKE IN BUSINESS, "DEEPFAKES AND THEIR IMPACT ON BUSINESS, EDITED BY GAURAV GUPTA ET AL, IGA GLOBAL, 2025
68. PRATYUSH SHARMA, ET AL, MACHINE LERNING MODEL FOR CREDIT CARD FRUD DETECTION -A COMPARATIVE ANALYSIS, THE INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY, VOL 18, NO 6,11/2021
69. PALAK GUPTA, ET AL, UNBALANCED CREDIT CARD FRAUD DETECTION DATA: A MACHINE LEARNING -ORIENTED COMPARATIVE STUDY OF BALANCIG TECHNIQUES, PROCEDIA COMPUTER SCIENCE, VOL 218,2023
70. REJWAN BIN SULAIMAN, VITALY SCHETININ, PAUL SANT, REVIEW OF MACHINE LEARNING APPROACH ON CREDIT CARD FRAUD DETECTION, HUMAN -CENTRIC INTELLIGENT SYSTEMS, VOL 1, N 2 ,5/2022
71. RAMIRO DANIEL CAMINO, MACHINE LEARNING TECHNIQUES FOR SUSPICIOUS TRANSACTION DETECTION AND ANALYSIS, PHD DISSERTION, THE FACULTY OF SCIENCE, TECHNOLOGY AND MEDICINE, UNIVERSITE DU LUXEMBOURG EN INFORMATIQUE,10 /2020,
72. REJWAN BIN SULAIMAN, ET AL, REVIEW OF MACHINE LEARNING APPROACH ON CREDIT CARD FRAUD DETECTION, HUMAN -CENTRIC INTELLIGENT SYSTEMS, VOL 2, 5/2022
73. ROBIN M. SCHMIDT, RECURRENT NEURAL NETWORKS (RNNs): A GENTLE INTRODUCTION AND OVERVIEW, ARIVEX PREPRINT, ARIVEX: 1912. 05911v1 [cs. lg],11/2019
74. RICHARD OLIVER LANE, A COMPREHENSIVE REVIEW OF CLASSIFIER PROBABILITY CALIBRATION METRICS, ARIVEX:2504 .18278, 4/2025
75. STOGANOVIC BRANKA, ET AL, "FOLLOW THE TRAIL: MACHINE LEARNING FOR FRAUD DETECTION IN FINTECH APPLICATIONS SENSORS «, VOL 21, NO.5, 02/2021, P2
76. SHEWANGU DZOMIRA, ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, ZIMBABWE, RISK GOVERNANCE & CONTROL: FINANCIAL MARKETS & INSTITUTIONS, VOLUME 4, ISSUE 2, 2014

77. SALMAN BAHOO, ET AL, ARTIFICIAL INTELLIGENCE IN FINANCE: A COMPREHENSIVE REVIEW THROUGH BIBLIOMETRIC AND CONTENT ANALYSIS, SN BUSINESS AND ECONOMICS A SPRINGER NATURE JOURNAL, VOL 4, N23,2024
78. SEBRI ABDERAHIM, COURS OF MACHINE LEARNING IA, UNIVERSITY OF SAVOIE -FRANCE, 2022‹ -2023‹P13 ‹FROM: https://cel.hal.science/hal-03906387
79. SHAHNAWAZ KHAN, ET AL, DEVELOPING A CREDIT CARD FRAUD DETECTION MODEL USING MACHINE LEARNING APPROACHES, INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, VOL 13, N 3, 2022
80. SANGWON JUNG, ET AL, A REVIEW OF T -SNE, IMAGE PROCESSING ON LINE, VOL 14,2024
81. SAHID TUFAIL, HUGO RIGGS, ET Al, AVANCEMENTS AND CHALLENGES IN MACHINE LEARNING : A COMPREHENSIVE REVIEW OF MODELS, LIBRARIES, APPLICATIONS, AND ALGORITHMS, JOURNAL ELECTRONICS, VOL12, N8‹4/2023
82. TAUFIQUL AZIZ, RITA YUNIARTI, FRAUD PENTAGON THEORY FOR DETECTION OF FRAUDULENT FINANCIAL REPORTS: A PRELIMINARY STUDY IN MANUFACTURING ENTERPRISES IN INDONESIA, DINASTI INTERNATIONAL JOURNAL OF ECONOMICS, FINANCE & ACCOUNTING, VOL .4, No.1,2023
83. TIANQI CHEN, CARLOS GUESTRIN, XGBOOST: A SCALABLE TREE BOOSTING SYSTEM, IN PROCEEDINGS CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING,2016‹https://doi.org/10.1145/2939672.2939785
84. V.S.RAJ KUMAR, T. KUMARESAN, A COMPARATIVE STUDY ON MACHINE LEARNING APPROACHES FOR SENTIMENT ANALYSIS, INTERNATIONAL RESEARCH JOURNAL ON ADVANCED ENGINEERING HUB (IRJAEH), VOL 2, N 2,2/2024
85. VIKAS THAMMANNA GOWDA, CREDIT CARD FRAUD DETECTION USING SUPERVISED LEARNING, IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY, VOL 11, N1
86. VIJAY R. KONDA, JOHN N. TSITSIKLIS, ACTOR -CRITIC ALGORITHMS, ADVANCE IN NEURAL INFORMATION PROCESSING SYSTEMS, VOL 12, 1999
87. VAISHNAVI NATH DORNADULA, GEETHA SA, CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS, PROCEDIA COMPUTER SCIENCE, Vol 165,2019
88. WOLFE DAVID. T, HERMANSON DANAR, THE FRAUD DIAMOND: CONSIDERING THE FOUR ELEMENTS OF FRAUD.THE CPA JOURNAL, NEW YORK STATE SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS. VOL 174.NO (12),2004
89. XIN ZHANG, ET AL, A MACHINE LEARNING MODEL THE PREDICTION OF ATHLETE ENGAGEMENT BASED ON COHESION, PASSION AND MENTAL TOUGHNESS, VOL 15, N 3220,2025
90. XUETONG LI, ET AL, GAUSSIAN MIXTURE MODELS WITH RARE EVENTS, JOURNAL OF MACHINE LEARNING RESEARCH, VOL 25, 1245 ,2024
91. YANBEI CHEN, ET AL, SEMI -SUPERVISED AND UNSUPERVISED DEEP VISUAL LEARNING: A SURVEY, ARVIEX, ARVIEX :2208. 1 1296v1 [cs.CV]
92. YOGITA RANI, HARISH ROHIL, A STUDY OF HIERARCHICAL CLUSTERING ALGORITM, INTERNATIONAL JOURNAL OF INFORMATION AND COMPUTATION TECHNOLOGY, VOL 3, N11,2013

المواقع الإلكترونية:

1. https://support.kaspersky.com/kisa/android_11.98/ar-ae/248822.htm.
2. https://www.interpol.int.
3. https://orangedatamining.com/widget-catalog.
4. www.iosco.org /library/pubdocs /pdf / ioscopd 752.pdf
5. http://dx.doi.org/10.14236/ewic/pom19.2
6. http://www.getfocal.ai/
7. https:// www.iosco.org
8. https://www.imf.org/-/media/files/publications/sdn/2020/english/sdnea2020007.pdf
9. https://www.oas.org/juridico/pdfs/cyb9-unodc-dec16-
10. http://e-space.mmu.ac.uk/619559.
11. https://www.kaggle.com/datasets/samayashar/fraud-detection-transactions-dataset

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Ghardaïa
Faculté des Sciences Economiques, Commerciales et Sciences de Gestion
Département .....

وزارة التعليم العالي و البحث العلمي
جامعة غرداية
كلية العلوم الاقتصادية و التجارية و علوم التسيير
قسم .....

غرداية في: .....

شهادة تصحيح

يشهد الأستاذ (ة) : أستاذ مريم ..... الصفة في لجنة المناقشة: ... مشرفا و مقررا ...

بصفته عضوا في لجنة مناقشة الطالب (ة) : ..... إكرام معطا الله .....

شعبة : مالية و محاسبة ..... تخصص : ... تكنولوجيا مالية .....

بعنوان : دور خوارزميات تعلم الآلة في كشف الاحتيال المالي الإلكتروني (تصميم انموذج) .....

.....

.....

تاريخ المناقشة : ..... 2026/06/01 .....

أن الطالب (ة) إلتزم (ت) بجميع الملاحظات المقدمة من طرف اللجنة وأن المذكرة قابلة للإيداع النهائي

إمضاء الأستاذ(ة) المكلف(ة) بمتابعة التصحيح

د. أستاذ مريم

رئيس القسم