الأكاديمية العربية
للعلوم الإدارية والمالية والمصرفية
كلية الدراسات العليا

تأثير الذكاء الاصطناعي على إدارة مخاطر الجريمة المالية

دراسة تطبيقية على القطاع المصرفي القطري

الباحث

نشأت جابر محمود أبو شعيشع

لاستكمال متطلبات الحصول على درجة الدكتوراه المهنية في إدارة الأعمال (DBA)

إشراف

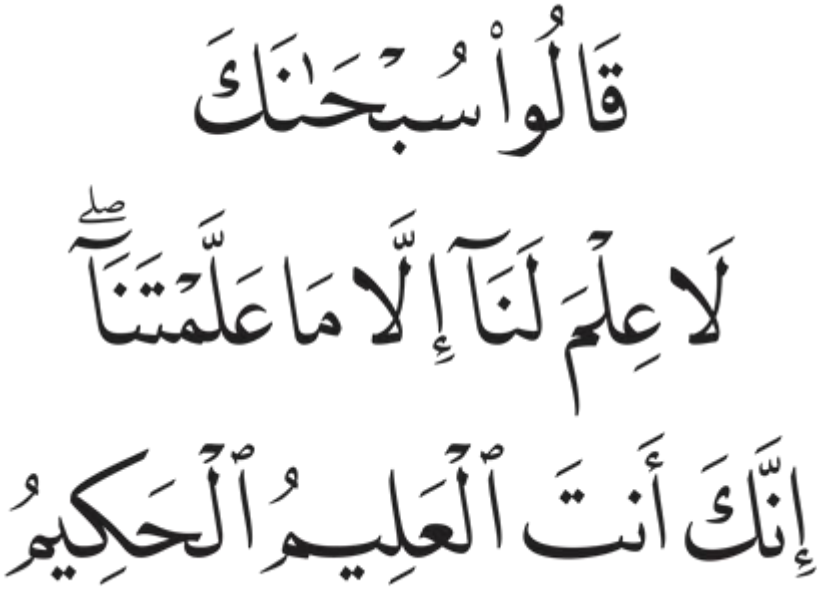
أ.د. محمد أمين شريف

أستاذ التمويل والاستثمار

كلية التجارة - جامعة القاهرة

2025م / 1447 هـ

بسم الله الرحمن الرحيم



صدق الله العظيم

سورة البقرة (32)

لجنة المناقشة والحكم

أ.د. محمد أمين شريف مشرفا ورئيسا

أستاذ التمويل والاستثمار ، كلية التجارة، جامعة القاهرة

وعميد كلية العلوم الادارية السابق، جامعة الملك سلمان

أ.د محمود محمد السيد عضوا

أستاذ ورئيس قسم التأمين والعلوم الاكتوارية، كلية التجارة، جامعة القاهرة

أ.م.د. أحمد فؤاد حسب اللّه عضوا

عميد أكاديمي - الاكاديمية العربية للعلوم والتكنولوجيا و النقل البحري

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبفضله تتحقق الإنجازات، وبعونه وتوفيقه تُذلل الصعاب وتُفتح الأبواب، نحمده حمدًا يليق بجلال وجهه وعظيم سلطانه، ونصلي ونسلم على سيدنا محمد، معلم البشرية، وقدوة السالكين، وعلى آله وصحبه أجمعين.

وبعد؛

فإن الكلمات لتقف قاصرةً عن التعبير عمّا يختلج في النفس من عرفان وامتنان لكل من كان له الفضل بعد الله تعالى في إنجاز هذا العمل العلمي، الذي لم يكن ليرى النور لولا توفيقه عزّ وجل، ثم عطاءات كريمة وتوجهات مخلصة من نخبة من أهل العلم والفضل.

بداية أتوجه بخالص الشكر وأسمى عبارات التقدير إلى أستاذي الجليل ومعلمي الفاضل **الأستاذ الدكتور/ محمد شريف، أستاذ التمويل والاستثماربكلية التجارة - جامعة القاهرة، رئيس لجنة الحكم والمناقشة و المشرف على هذه الرسالة**، الذي كان بحق منارة علم وهداية، لم يبخل بعلمه ولا بوقته ولا بتوجيهاته السديدة، فكان سندًا في كل مراحل البحث، أضاء لي دروب الحيرة، وصبر على طول المسيرة؛ فله مني خالص الدعاء، وأن يجزيه الله خير الجزاء، ويبارك له في علمه وعمره وعطائه.

كما أتقدم بجزيل الشكر وعظيم الامتنان إلى **الأستاذ الدكتور/ محمود محمد السيد، أستاذ ورئيس قسم التأمين والعلوم الاكتوارية، كلية التجارة، جامعة القاهرة**، لفضله الكريم بالموافقة على **المشاركة في لجنة الحكم والمناقشة**، وهو ما أعدّه شرفًا كبيرًا أفتخر به، وإثراءً علميًّا مميزًا لهذه الدراسة.

ولا يسعني في هذا المقام إلا أن أعبر عن بالغ امتناني **للأستاذ م. الدكتور/ أحمد فؤاد حسب الله، عميد أكاديمي، الاكاديمية العربية للعلوم والتكنولوجيا و النقل البحري**، لتفضله بالموافقة على **المشاركة في لجنة الحكم والمناقشة**، بما يشكل إثراءً وإضافةً نوعية لقيمة هذه الدراسة.

وإلى جميع أساتذتي الأفاضل في مرحلة الدكتوراه، الذين كانوا مشاعل علم ونماذج قدوة، أزجي أسمى آيات الشكر والعرفان لما غرسوه في نفسي من علمٍ وتأصيل، وما بذلوه من جهدٍ وتوجيه كريم، فجزاهم الله عني خير الجزاء.

وإلى كل أستاذ تعلّمت منه حرفًا، وكل زميلٍ ساندني في دربي، وكل صديقٍ حفّزني بكلمة صادقة، وإلى أسرتي الكريمة التي أحاطتني بالدعاء والدعم والسكينة، أتوجه بخالص الامتنان، فلكم جميعًا في القلب مكانة، وفي الدعاء نصيب.

كما لا يفوتني أن أعرب عن بالغ شكري وامتناني لكل من أسهم في إنجاز الجانب الميداني من هذه الدراسة، من مسؤولين وموظفين ومشاركين كرام، الذين تفضلوا بتخصيص وقتهم الثمين للإجابة عن الاستبانات أو تقديم المعلومات أو تسهيل إجراءات البحث، فلهم مني وافر التقدير والامتنان؛ إذ كان لعونهم أثرٌ بالغ في استكمال هذا العمل وتحقيق أهدافه البحثية.

وختامًا، أسأل الله أن يجعل هذا الجهد خالصًا لوجهه الكريم، نافعًا للعلم وأهله، وأن يجزي كل من أعانني خير الجزاء.

وآخر دعوانا أن الحمد لله رب العالمين.

إهداء

إلى من رحل بالجسد، وبقيت ذكراه حيّة في قلبي لا تغيب، إلى **أبي الغالي**، الذي علّمني معنى الصبر والرجولة، وغرس في نفسي قيم الإيمان والعلم والعمل، أسأل الله أن يتغمده برحمته الواسعة، ويسكنه فسيح جناته، وأن يجعل هذا العمل في ميزان حسناته، وفاءً وعرفانًا لما قدمه لي من دعم وحب وتضحية.

وإلى من كانت - ولا تزال - موطن الحنان ومصدر الدعاء، إلى **أمي الحبيبة**، أطال الله في عمرها ومتعها بالصحة والعافية، جزاها الله عني خير الجزاء على ما بذلته من سهر وتربية ودعاء، فكل نجاحٍ أحقّ أن يُكتب باسمها.

وإلى شريكة دربي ورفيقة روحي، **زوجتي العزيزة**، التي كانت سندًا في لحظات الضعف، ورفيقة في أوقات التعب، فكانت نعم العون في رحلة البحث، فللكِ مني كل الحب والتقدير، ما حييت.

وإلى **ابني الغالي**، وفلذة كبدي، **و ابنتيَّ الحبيبتين**، أزهار حياتي ونبض قلبي، أرجو من الله أن يجعل هذا العمل نورًا في دربهم، ودافعًا لهم لحب العلم والسعي إليه.

وإلى **أخي العزيز**، سندي بعد الله، الذي لم يبخل عليّ بمحبته ودعمه ووقفاته التي لا تنسى، فله خالص مودتي ودعائي.

وإلى **أختيّ الغاليتين**، اللتين كان دعمهما النفسي والمحبّ الصادق معينًا لي في مسيرتي، أهدي إليكما هذا الجهد المتواضع بكل مودة وامتنان.

وإلى **كل من مدّ لي يد العون، ودفعني بكلمة**، أو **ساندني بدعاء**، أو **أعانني بجهد في سبيل إتمام هذا العمل**...

إليهم جميعا... أهدي هذا العمل، تعبيرا عن الوفاء والمحبة، وذخيرة علم أسأل الله أن ينفع بها.

الباحث

مستخلص الدراسة

تهدف هذه الدراسة إلى استقصاء تأثير استخدام تقنيات الذكاء الاصطناعي في تعزيز إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي القطري، و قياس درجة تأثير الذكاء الاصطناعي على مختلف مراحل إدارة مخاطر الجرائم المالية، بدءًا من تحديدها ثم تحليلها، ومرورًا بمعالجتها، وانتهاءً بمتابعتها ومراجعتها. اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم جمع البيانات باستخدام استمارة استبانة وُزعت على عينة من العاملين في القطاع المصرفي القطري في الفترة من 1 يناير 2024 إلى 31 مايو 2025، وتم تحليل النتائج باستخدام الأساليب الإحصائية المناسبة. وقد أظهرت النتائج أن درجة استخدام الذكاء الاصطناعي في مؤسسات القطاع المصرفي القطري جاءت مرتفعة، حيث أظهرت جميع أبعاد الدراسة (التحديد، التحليل والتقييم، المعالجة، المراقبة والمراجعة) تأثيرًا ذا دلالة معنوية، كما أظهرت نتائج الانحدار وجود علاقة قوية بين الذكاء الاصطناعي وكل مرحلة من مراحل إدارة مخاطر الجريمة المالية، وهو ما يؤكد فاعلية تطبيقات الذكاء الاصطناعي في تعزيز استجابة المصارف للمخاطر المالية المتجددة والمعقدة. وتوصي الدراسة بتوسيع نطاق الاستثمار في الذكاء الاصطناعي، وتطوير الحوكمة المؤسسية للأنظمة الذكية، وضمان تكاملها مع سياسات حماية البيانات والخصوصية، وتوفير الكفاءات البشرية القادرة على إدارتها وتقييم أدائها بفعالية.

الكلمات المفتاحية:

الذكاء الاصطناعي – الجريمة المالية – إدارة المخاطر – التحليل التنبؤي – القطاع المصرفي القطري - تعلم الآلة – النظم الخبيرة

Abstract

This study aims to investigate the impact of using artificial intelligence (AI) technologies in enhancing financial crime risk management within Qatari banking institutions. It further seeks to measure the extent of AI's influence across the different stages of financial crime risk management—starting from risk identification and analysis, through mitigation, and concluding with monitoring and review. The study adopts a descriptive-analytical methodology, with data collected through a structured questionnaire distributed to a sample of employees in the Qatari banking sector during the period from January 1, 2024, to May 31, 2025. The data were analyzed using appropriate statistical methods. The findings reveal that the level of AI utilization in Qatari banking institutions is high, and that all dimensions of the study—identification, analysis and evaluation, treatment, and monitoring and review—exhibit statistically significant effects. Regression analysis further indicates a strong relationship between AI and each stage of financial crime risk management, confirming the effectiveness of AI applications in strengthening banks' responsiveness to evolving and complex financial risks. The study recommends expanding investment in AI technologies, developing institutional governance frameworks for intelligent systems, ensuring their integration with data protection and privacy policies, and providing qualified human resources capable of managing and evaluating their performance effectively.

Keywords:

Artificial Intelligence – Financial Crime – Risk Management – Predictive Analytics – Qatari Banking Sector – Machine Learning – Expert Systems

فهرس الموضوعات

م	البيان	صفحة
	شكروتقدير	د
	إهداء	هـ
	مستخلص الدراسة	و
	Abstract	ز
	فهرس الموضوعات	ح
	فهرس الجداول	ك
	فهرس الأشكال	ل
	مصطلحات الدراسة	م
	الفصل الأول: الإطار العام للدراسة	
	مقدمة	1
	أولا: مشكلة الدراسة	3
	ثانيا: الدراسات السابقة	3
	ثالثا: متغيرات وفروض الدراسة	17
	رابعا: أهداف الدراسة	19
	خامسا: أهمية الدراسة	19
	سادسا: منهجية الدراسة وإجراءاتها	21
	سابعا: حدود الدراسة	22
	ثامنا: خطة الدراسة	23
	الفصل الثاني: الإطار النظري للدراسة	
	أولاً: الإطار النظري للذكاء الاصطناعي وتطبيقاته	26
	▪ مقدمة	26
	▪ ماهية الذكاء الاصطناعي	27
	▪ مفهوم الذكاء الاصطناعي	27
	▪ مراحل تطور الذكاء الاصطناعي	28
	▪ خصائص الذكاء الاصطناعي	30
	▪ أهداف الذكاء الاصطناعي	31
	▪ أهمية الذكاء الاصطناعي	31
	▪ أنواع الذكاء الاصطناعي	32
	▪ نظم الذكاء الاصطناعي	33
	▪ مؤشرات قياس أداء الذكاء الاصطناعي	42
	▪ التحديات والعواقب المصاحبة لتبني الذكاء الاصطناعي	44

م	البيان	صفحة
	ثانيًا: الإطار النظري لإدارة مخاطر الجريمة المالية وتداعياتها في القطاع المصرفي	46
	▪ مقدمة	46
	▪ تعريف الجرائم المالية في القطاع المصرفي	47
	▪ تصنيفات الجرائم المالية في القطاع المصرفي	47
	▪ أبرز صور الجرائم المالية في القطاع المصرفي	51
	▪ الاتجاهات والتحديات الناشئة في الجرائم المالية في القطاع المصرفي	63
	▪ الآثار المترتبة على الجرائم المالية في القطاع المصرفي	64
	▪ إدارة مخاطر الجرائم المالية في القطاع المصرفي	65
	▪ إستراتيجيات إدارة مخاطر الجرائم المالية في القطاع المصرفي	72
	▪ ضوابط إدارة مخاطر الجرائم المالية في القطاع المصرفي	75
	▪ مقاييس فاعلية إدارة مخاطر الجرائم المالية في القطاع المصرفي	78
	ثالثًا: دور الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	80
	▪ مقدمة	80
	▪ نظرة على استخدامات وتطبيقات الذكاء الاصطناعي في القطاع المصرفي بشكل عام	81
	▪ تطبيقات الذكاء الاصطناعي ودورها في إدارة مخاطر الجرائم المالية	82
	▪ فوائد الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	87
	▪ التحديات المرتبطة بتبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	88
	▪ الآليات المقترحة لمعالجة تحديات تبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	90
	▪ الاتجاهات والتطورات المستقبلية لتوظيف الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	91
	▪ استعراض تطبيقات عملية للذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي	92
	رابعًا: القطاع المصرفي القطري وجهود التحول الرقمي وتبني التكنولوجيا المالية والذكاء الاصطناعي فيه	104
	▪ مقدمة	104
	▪ نبذة مختصرة عن دولة قطر	104
	▪ تطور القطاع المصرفي القطري: الخلفية التاريخية والبنية المؤسسية	105
	▪ الإطار التنظيمي والإشرافي للقطاع المصرفي القطري	106
	▪ هيكل القطاع المصرفي في دولة قطر	108
	▪ إسهام القطاع المصرفي القطري في التنمية الوطنية وتحقيق رؤية قطر 2030	110
	▪ الأداء المالي للقطاع المصرفي القطري	111
	▪ الاتجاهات الحديثة في القطاع المصرفي القطري	112
	▪ التحول الرقمي والتكنولوجيا المالية في القطاع المصرفي القطري	114
	▪ دور مصرف قطر المركزي في تعزيز نمو التكنولوجيا المالية في القطاع المصرفي القطري	116
	الفصل الثالث: منهجية ونتائج الدراسة	
	مقدمة	123
	أولا: منهجية الدراسة وإجراءاتها	124

م	البيان	صفحة
	▪ الهدف من الدراسة الميدانية	124
	▪ منهج الدراسة	124
	▪ مصادر بيانات الدراسة	124
	▪ مجتمع وعينة الدراسة وأداة القياس	125
	▪ قياس صلاحية أداة جمع البيانات	128
	ثانيا: عرض البيانات وتحليلها	130
	▪ عرض نتائج البيانات لعينة الدراسة وتحليلها	130
	▪ عرض و تحليل نتائج متغيرات الدراسة	133
	ثالثا: اختبار فروض الدراسة	144
	▪ التوزيع الطبيعي لمتغيرات الدراسة	144
	▪ اختبار فروض الدراسة	145
	الفصل الرابع: نتائج وتوصيات الدراسة	
	مقدمة	152
	أولا: نتائج الدراسة	152
	ثانيا: تحليل نتائج الدراسة	154
	ثالثا: توصيات الدراسة	155
	رابعا: صعوبات (محددات) الدراسة	158
	خامسا: دراسات مستقبلية مقترحة	158
	قائمة المصادر والمراجع	
	أولاً: قائمة المصادر والمراجع العربية	160
	ثانيًا: قائمة المصادر والمراجع الأجنبية	161
	الملاحق	

فهرس الجداول

الجدول	البيان	الصفحة
1	أبعاد المتغير المستقل (الذكاء الاصطناعي)	17
2	أبعاد المتغير التابع (إدارة مخاطر الجريمة المالية)	17
3	هيكل ومؤسسات القطاع المصرفي في دولة قطر	110
4	ملخص المفاهيم المتعلقة بمتغيرات الدراسة (المتغير المستقل و المتغير التابع)	118
5	عدد العاملين في الإدارات ذات الصلة بموضوع الدراسة في كل بنك / مصرف في القطاع المصرفي القطري	125
6	توزيع حجم عينة العاملين بمؤسسات القطاع المصرفي محل الدراسة	126
7	متغيرات البحث وعناصر قياسها ورموز أسئلتها	127
8	درجات مقياس ليكرت	127
9	مستوى الأهمية لأبعاد الدراسة	127
10	قيم معامل الثبات (طريقة ألفا كرونباخ) لأبعاد الدراسة	128
11	قيم معامل الصدق الداخلي بين فقرات أبعاد الدراسة	130
12	توزيع أفراد عينة الدراسة وفق متغير النوع	130
13	توزيع أفراد عينة الدراسة وفق متغير العمر	131
14	توزيع أفراد عينة الدراسة وفق متغير المؤهل الدراسي	132
15	توزيع أفراد عينة الدراسة وفق متغير سنوات الخبرة	132
16	المتوسطات والانحرافات المعيارية واستجابات الدراسة نحو بُعد (الذكاء الاصطناعي)	133
17	المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (تحديد مخاطر الجريمة المالية)	136
18	المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (تحليل وتقييم مخاطر الجريمة المالية)	138
19	المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (معالجة مخاطر الجريمة المالية)	140
20	المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (مراقبة ومراجعة الجريمة المالية)	142
21	اختبار التوزيع الطبيعي للبيانات	145
22	نتائج اختبارات الفرضية الفرعية الأولى لقياس تأثير الذكاء الاصطناعي على تحديد مخاطر الجريمة المالية	146
23	نتائج اختبارات الفرضية الفرعية الثانية لقياس تأثير الذكاء الاصطناعي على تحليل وتقييم مخاطر الجريمة المالية	147
24	نتائج اختبارات الفرضية الفرعية الثالثة لقياس تأثير للذكاء الاصطناعي على معالجة مخاطر الجريمة المالية	148
25	نتائج اختبارات الفرضية الفرعية الرابعة لقياس تأثيرللذكاء الاصطناعي على مراقبة ومراجعة مخاطرالجريمة المالية	149
26	توصيات الدراسة	155

فهرس الأشكال

الشكل	البيان	الصفحة
1	نموذج متغيرات الدراسة	18
2	محطات في مراحل تطور الذكاء الاصطناعي	30
3	أنواع الذكاء الاصطناعي	32
4	العلاقة بين بعض أنظمة الذكاء الاصطناعي	40
5	تصنيفات الجرائم المالية في القطاع المصرفي	48
6	مراحل جريمة غسل الأموال	52
7	مراحل جريمة تمويل الإرهاب	53
8	مراحل جريمة تمويل الانتشار	55
9	أنماط الاحتيال الداخلي أو الوظيفي / شجرة الاحتيال (العناوين الرئيسية فقط)	59
10	مراحل إدارة مخاطر الجرائم المالية في القطاع المصرفي وآلياتها المختلفة	69
11	إستراتيجيات إدارة مخاطر الجرائم المالية في القطاع المصرفي وآلياتها المختلفة	74
12	ضوابط إدارة مخاطر الجرائم المالية في القطاع المصرفي موزعة على مراحل إدارة مخاطر الجرائم المالية	77
13	الهيكل التنظيمي لمصرف قطر المركزي **QCB**	107

أهم مصطلحات الدراسة

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
المرمزات التلقائية المكدسة	Stacked Autoencoders	كشف الاحتيال القائم على الذكاء الاصطناعي	AI-based Fraud Detection
خوارزمية التعميم المكدس	Stacked Generalization	مؤشرات قياس أداء الذكاء الاصطناعي	AI Performance Metrics
خوارزمية النزول الاشتقاقي العشوائي	Stochastic Gradient Descent	خوارزمية	Algorithm
النماذج الموجهة	Supervised Models	الظلم الخوارزمي	Algorithmic Injustice
آلة المتجهات الداعمة	Support Vector Machine -SVM	تقنيات الكشف عن الحالات الشاذة	Anomaly Detection Techniques
التحليل النحوي	Syntactic Analysis	الذكاء الاصطناعي العام	Artificial General Intelligence -AGI
البيانات المصطنعة	Synthetic Data	الذكاء الاصطناعي العصبي	Artificial Neural Intelligence -NeuroAI
التصنيف	Taxonomizing	شبكة عصبية اصطناعية	Artificial Neural Network -ANN
النماذج الزمنية	Temporal Models	شبكات عصبية اصطناعية ذات انتشار مرتد	Backpropagation – Artificial Neural Network (BP-ANN)
بيانات الاختبار	Test Data	البيانات الضخمة	Big Data
توليد النصوص	Text Generation	الروبوتات البرمجية	Bots
معالجة النصوص	Text Processing	رؤية الحاسب	Computer Vision
الذكاء الاصطناعي القائم نظرية العقل	Theory- of-Mind AI	نموذج شبكة عصبية متصلة	Connected Neural Network Model
خوارزميات التدريب	Training Algorithms	الشبكات العصبية الترشيحية	Convolutional Neural Network-CNN
بيانات التدريب	Training Data	الشبكات العصبية الترشيحية	Convolutional Neural Network-CNN
نقل التعلم	Transfer Learning	أشجار القرار	Decision Trees
التأثيرات الانتقالية	Transitive Effects	التعلم العميق	Deep Learning
الشفافية	Transparency	شبكة عصبية اصطناعية متعددة الطبقات	Deep Neural Network
الثقة	Trust	شبكة المحولات العصبية العميقة	Deep Neural Network Transformers
الجدارة بالثقة / الموثوقية	Trustworthiness	النماذج القابلة للتفسير	Explainable Models
جدير بالثقة/ موثوق	Trustworthy	النظم الخبيرة	Expert Systems
الذكاء الاصطناعي الموثوق	Trustworthy Artificial Intelligence	الشبكات التوليدية التنافسية	Generative Adversarial Network - GANs
بيانات غير معلومة / غير مسماة	Unlabeled Data	الذكاء الاصطناعي التوليدي	Generative AI
الكشف غير الموجه عن الحالات الشاذة	Unsupervised Anomaly Detection	تطبيق النمذجة الشبكية	Graph Modeling
التعلم غير الموجه	Unsupervised Learning	وكيل ذكي	Intelligent Agent
البيانات غير المنظمة	Unstructured Data	غابات العزل	Isolation Forests
سلوك المستخدم	User Behavior	نماذج اللغة الكبيرة	Large Language Models – LLM
واجهات المستخدم	User Interfaces	خوارزميات الانحدار اللوجستي	Logistic Regression
بيانات تحقق	Validation Data	الشّبكة العصبية ذات الذّاكرة الطّويلة قصيرة المدى	Long-Short Term Memory- LSTM
التلاعب بالفيديو	Video Manipulation		
الوكلاء الافتراضيين	Virtual Agents	معالجة اللغات الطبيعية	Natural Language Processing
استنساخ الأصوات والصور	Voice and Image Cloning	خوارزمية الغابة العشوائية	Random Forest
تمثيل الكلمات	Word Embedding	الذكاء الاصطناعي التفاعلي	Reactive AI
التحليل النحوي	Syntactic Analysis	تصحيح التناقضات	Rectify Inconsistencies
البيانات المصطنعة	Synthetic Data	مؤشر قياس الاستدعاء	Recall Measuring Index
التصنيف	Taxonomizing	الشبكة العصبية التكرارية	Recurrent Neural Network-RNN
النماذج الزمنية	Temporal Models	خوارزميات الانحدار	Regression Algorithms
بيانات الاختبار	Test Data	أتمتة العمليات الروبوتية	Robotics Process Automation – RBA
توليد النصوص	Text Generation	النماذج شبه الموجهة	Semi-supervised Models

الفصل الأول
الإطار العام للدراسة

- **مقدمة**
- **مشكلة الدراسة**
- **الدراسات السابقة**
- **فروض و نموذج الدراسة**
- **أهداف الدراسة**
- **أهمية الدراسة**
- **منهجية الدراسة وإجراءاتها**
- **حدود الدراسة**
- **خطة الدراسة:**
  - الفصل الأول: الإطار العام للدراسة
  - الفصل الثاني: الإطار النظري للدراسة
  - الفصل الثالث: منهجية الدراسة وإجراءاتها
  - الفصل الرابع: نتائج وتوصيات الدراسة
  - قائمة المراجع والمصادر
  - ملاحق الدراسة

الفصـــــل الأول

الإطـــــار العام للدراســـــة

مقدمـــــة:

تعد مؤسسات القطاع المصرفي من أهم أعمدة الاقتصاد الوطني في أي دولة، حيث لعبت هذه المؤسسات منذ نشأتها – وما زالت – دورًا حاسمًا في نمو الاقتصادات الوطنية من خلال دورها الرئيسي المتمثل في تزويد هذه الاقتصادات بالسيولة اللازمة للقيام بالأنشطة الاقتصادية المختلفة، حتى أصبح القطاع المصرفي في أي دولة مرآة يعكس حالتها الاقتصادية بشكل عام. وقد أصبحت قوة هذا القطاع في الدولة مؤشرا حقيقيا لقوة الاقتصاد الكلي (Macroeconomics) فيها، بل تعدى تأثيره أيضا الأسواق الوطنية إلى الأسواق الخارجية ليكون أحد معززات ثقة المستثمرين الدوليين ونظرتهم الإيجابية إلى الاقتصاد الوطني، وفي المرحلة الحالية من تطور الاقتصاد العالمي، ومع التبني الواسع لمفهوم العولمة، توسع دور المؤسسات المصرفية وازداد تعقيدًا؛ إذ أصبحت هذه المؤسسات تشارك بقوة في جميع الأنشطة الاقتصادية الدولية تقريبًا عوضًا عن اقتصارها السابق على الأسواق الوطنية فقط (BIS, 2021; World Bank, 2021).

و قد شهدت العقود الثلاثة الأخيرة تطورات متسارعة في الاتصالات وتقنية المعلومات غيّرت جذريًا طريقة تفاعل البشر مع بيئاتهم، وانعكس ذلك بوضوح على القطاع المصرفي الذي شهد تحولًا كبيرًا في عملياته، فتبنّت المؤسسات المصرفية تقنيات حديثة مثل الخدمات المصرفية عبر الإنترنت (Internet Banking)، والمدفوعات الإلكترونية (E-Payments)، مما مكّنها من تقديم خدمات أعلى جودة وأكثر كفاءة، وبجهد وتكلفة أقل (Bueno et al., 2024; Litvishko et al., 2020). ومع تحوّل بيئة الأعمال المصرفية لتصبح أكثر مرونة لاستيعاب أنماطها الحديثة، ارتفع خلال العقد الأخير مستوى تبنّي هذه التقنيات في المؤسسات المصرفية واعتمادها المتزايد عليها (Sayed & Mansour, 2023; Ayinaddis et al., 2023). وفي هذا الصدد، أشارت تقارير حديثة إلى أن إنفاق المؤسسات المصرفية على تكنولوجيا المعلومات قد ارتفع بنسبة 38% خلال الفترة 2013–2022، ليصل إلى نحو 10.6% من الإيرادات وقرابة 20% من المصروفات التشغيلية، بما يعكس تحول التكنولوجيا إلى عنصر أساسي في تكلفة تشغيل الأعمال المصرفية (McKinsey, 2024) . كما بلغ الإنفاق التقني العالمي في القطاع المصرفي حوالي 650 مليار دولار عام 2023 بمعدل نمو سنوي يقارب 9%، إضافة إلى ارتفاع كبير في ميزانيات الأمن السيبراني التي بلغت مئات الملايين من الدولارات لدى البنوك الكبرى، مع توقعات بوصول الإنفاق العالمي في هذا المجال إلى 32 مليار دولار مع نهاية العام الحالي 2025 (The Guardian, 2025; Cybersecurity Advisors Network, 2025).

ونتيجة للتراكم الهائل والتوسع في التقنيات الرقمية، ظهرت موجة متسارعة من الابتكارات التي تشابكت فيما بينها عبر خوارزميات متقدمة، مُطلِقة مرحلة جديدة عُرفت **بالثورة الصناعية الرابعة (4IR) أو الصناعة 4.0** .و هي الثورة التي وصفها (Schwab, 2016) بأنها حالة تتلاشى فيها الحدود بين التطورات المادية والرقمية والبيولوجية، مع تأثير يمتد ليشمل مختلف جوانب الحياة، لا الإنتاج فقط. وتتمثل أبرز تطبيقات هذه الثورة في **الذكاء الاصطناعي** (Artificial Intelligence)، **والبيانات الضخمة** (Big Data)، و **إنترنت الأشياء** (Internet of Things)، **والأمن السيبراني** (Cyber Security)، وغيرها من التطبيقات (Meindl & Mendonça,2024; Farayola,2021).

يعرف (عزيز، 2023) الذكاء الاصطناعي (AI) بأنه أحد فروع علوم الحاسب الذي يهدف إلى تمكين الحاسب من محاكاة عمليات الذكاء البشري، بحيث يكتسب القدرة على **حل المشكلات و اتخاذ القرارات بمنطق ومنهجية مشابهة للعقل البشري** . ويتم ذلك عبر مجموعة من التطبيقات التقنية مثل **النظم الخبيرة** (Expert Systems)، **ومعالجة اللغات الطبيعية** (Natural Language Processing)، **والتعرف الآلي على الكلام** (Speech Recognition)، **والرؤية الآلية** (.Computer Vision)وتمكّن هذه

التقنيات الآلات من أداء وظائف معرفية عادةً ما ترتبط بالبشر - كالإدراك، والاستدلال، والتعلم، وحل المشكلات، وأحيانًا الإبداع - ولكن **بسرعة وكفاءة أعلى** بفضل قدرتها الكبيرة على معالجة الحسابات المعقدة والتعامل مع كمّ هائل من البيانات بسهولة، بخلاف ما يتطلبه ذلك من وقت وجهد لدى الإنسان(Grzybowski et al., 2024) .

و تماشيًا مع الانتشار الواسع والنجاح الملحوظ لتقنيات الذكاء الاصطناعي (AI) في مختلف مجالات الأعمال، ومع كون الصناعة المصرفية (Banking Industry) من أكثر القطاعات احتياجًا للابتكار المستمر، اتسع نطاق استخدام الذكاء الاصطناعي (AI) في الأنشطة المصرفية وتسارعت وتيرة تبنيه. فقد استغلت المؤسسات المصرفية القدرات الكبيرة لهذه التقنيات لتحسين كفاءة عملياتها، وزيادة الإنتاجية، ورفع رضا العملاء، إضافةً إلى تقليل الأعباء التشغيلية على الموظفين ليتفرغوا لمهام أكثر تعقيدًا، بما يسهم في تحقيق أهدافها المنشودة (Malusare, 2024; Noreen et al., 2023).

وفي إطار ممارستها لمختلف الأنشطة والعمليات المالية، تتعرض المؤسسات المصرفية لباقة واسعة من المخاطر تُصنَّف عادةً إلى أربعة أنواع رئيسية: المخاطر المالية (Financial Risks)، والمخاطر التشغيلية (Operational Risks)، ومخاطر الأعمال (Business Risks)، ومخاطر الدولة (Country Risks) (Ahmed, Hussain, Malik, & Kamran, 2024 ; إبراهيم، 2019). ويزداد حجم هذه المخاطر مع توسّع المؤسسة المصرفية وتعقّد خدماتها. وتُعد **مخاطر الجرائم المالية** Financial Crime Risks أحد أخطر مكونات المخاطر التشغيلية التي يجب على المؤسسات المصرفية إدارتها والحد من آثارها حفاظًا على نزاهتها وسلامة النظام المصرفي، لما تشكّله من تهديد مباشر للمنظومة المالية العالمية والوطنية (Ahmad N. Eddin et al., 2021; زوانب وحاج علي، 2021).

ويشير مصطلح الجرائم المالية (Financial Crimes) في سياق العمل المصرفي إلى مجموعة متنوعة من الأفعال غير القانونية التي يرتكبها أشخاص أو كيانات قانونية، والتي تهدف عامة إلى تحقيق مكاسب غير مشروعة أو تضليل المؤسسات المصرفية وأطراف العلاقة بها أو إلحاق الضرر بهم (Achim et al., 2021)، وفي هذا السياق تعد المعركة الشرسة التي تخوضها المؤسسات المصرفية لمكافحة هذه الجرائم وإدارة مخاطرها أشبه بسباق تسلح لا نهاية له؛ فالجرائم المالية - كونها بالأساس ظواهر اجتماعية - تتأثر بالتغيرات في بيئتها، وعلى رأسها التطورات المتسارعة وغير المسبوقة في تقنيات المعلومات والاتصالات، ومن هنا برز دور الذكاء الاصطناعي (AI) كتقنية يستغلها المحتالون لتسهيل أنشطتهم الاحتيالية من خلال ابتكار طرقًا جديدة لارتكاب الجرائم المالية التقليدية بأساليب متطورة ومعقدة، أو ارتكاب الجرائم المالية المتطورة المستحدثة؛ ولذلك بات يتعين على المؤسسات المصرفية أن تتبنى بدورها حلولاً مبتكرة وذكية تعتمد على تقنيات الذكاء الاصطناعي (AI) لمكافحة هذه الجرائم بفاعلية، ولاستباق خطوات المجرمين (Rouhollahi, 2021; Haya & Mishra, 2024).

وبناء على المعطيات السابقة، جاءت فكرة هذه الدراسة لرصد وتحليل تأثير الذكاء الاصطناعي (AI) على إدارة مخاطر الجريمة المالية، بالتطبيق على عينة من المؤسسات العاملة في القطاع المصرفي القطري، وجاء ذلك انطلاقا من أهمية الدور الذي تلعبه هذه المؤسسات في كلا النظامين المالي والاقتصادي بمستوياتهما الوطنية والدولية، ولما لتلك المؤسسات من تأثير جوهري علي كافة مفاصل هذين النظامين وأنشطتهما المختلفة، ونظرا لخطورة الجرائم المالية وما تحمله من آثار مدمرة اقتصاديا واجتماعيا وسياسيا على الدولة ككل، وعلى كافة الأطراف ذات الصلة بقطاعات العمل المصرفي بوجه خاص.

ولقد قام الباحث بإجراء مراجعة للمكتبتين العربية والأجنبية، وتوصل إلى وجود قلة في المكتبة العربية في الأبحاث التي تتناول تأثير الذكاء الاصطناعي (AI) في مجال إدارة مخاطر الجريمة المالية في القطاع المصرفي العربي، حيث أن الدراسة الوحيدة التي عالجت هذا الموضوع كانت دراسة (بن علي، ديسمبر 2023)، والتي ركزت على دور الذكاء الاصطناعي و تطبيقاته فقط في مرحلة الكشف عن مخاطر الجرائم السيبرانية دون التطرق إلى دور الذكاء الاصطناعي في باقي مراحل إدارة مخاطر الجرائم المالية، أو دراسة جرائم مالية أخرى، كما أن هذه الدراسة قد أجريت بالتطبيق الميداني على القطاع المصرفي الدانماركي وتحديدا بالتطبيق على بنك (Danske) الدانماركي. ويرى الباحث أن هذا النقص يعود عدة أسباب، منها: حداثة مجال الذكاء الاصطناعي

(AI) بشكل عام، وكذا التسارع الشديد في التطورات في مجال الذكاء الاصطناعي (AI) وتطبيقاته بشكل لا تكاد الدراسات العلمية التحليلية قادرة أحيانا على مواكبته من جانب، ومن جانب آخر لكون جهود تبني منظمات الأعمال المصرفية العربية لتطبيقات الذكاء الاصطناعي (AI) في مجال إدارة مخاطر الجريمة المالية في القطاع المصرفي ما زالت في مراحلها الأولى. وكان ذلك بمثابة الدافع الذي حفز الباحث للقيام بإعداد هذا البحث العلمي.

أولاً: مشكلة الدراسة:

شهد العقد الأخير توجهًا متسارعًا من المؤسسات المصرفية نحو تبنّي تقنيات وتطبيقات الذكاء الاصطناعي، مدفوعًا بالتطورات التقنية غير المسبوقة خلال العقدين الماضيين. وقد أحدث هذا التوجه تحوّلًا جوهريًا في طبيعة الخدمات المصرفية وآليات تقديمها، وفي أنماط تفاعل المؤسسات المصرفية مع عملائها، مما دفعها إلى زيادة استثماراتها في هذه التقنيات لتعزيز قدراتها التنافسية ودعم عملياتها المختلفة (نايلي وحبار، 2023). وفي الوقت نفسه، تزايد الاهتمام بتوظيف الذكاء الاصطناعي للكشف عن الجرائم المالية داخل المؤسسات المصرفية، نتيجة الارتفاع الكبير في حجم وتعقيد الجرائم المالية واتجاه مرتكبيها إلى استخدام أدوات وتطبيقات متطورة، بما في ذلك تقنيات الذكاء الاصطناعي نفسها، وهو ما أدى إلى خسائر مالية كبيرة أصابت البنوك وعملاءها على حد سواء (Mytnyk et al.,2023).

ومن جهة أخرى، أثبتت الطرق التقليدية للكشف عن الاحتيال محدوديتها في مواجهة الجرائم المالية الحديثة، نظرًا لعدم قدرتها على التكيف مع أنماط الجريمة سريعة التغير وتزايد استغلالها لثغرات الأنظمة التقليدية. ومع هذا التطور المتسارع في أساليب الجرائم المالية وتعقيداتها، ظهرت حاجة ملحّة لدى المؤسسات المصرفية إلى تبنّي **حلول أكثر ذكاءً ومرونة وتطورًا** لإدارة مخاطر الجرائم المالية والحد من آثارها (Josyula, 2023).

كان ما سبق الحافز للباحث على دراسة تأثير هذا النمط من الذكاء على إدارة مخاطر الجريمة المالية في **مؤسسات القطاع المصرفي العاملة في دولة قطر تحت إشراف مصرف قطر المركزي**، حيث تتمثل **مشكلة الدراسة في التساؤل الرئيسي** التالي:

"ما مدى تأثير الذكاء الاصطناعي على إدارة مخاطر الجريمة المالية بالتطبيق على القطاع المصرفي القطري؟".

حيث يندرج تحت هذا التساؤل الرئيسي التساؤلات الفرعية التالية:

1. ما مدي تأثير استخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري؟
2. ما مدي تأثير استخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري؟
3. ما مدي تأثير استخدام الذكاء الاصطناعي في معالجة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري؟
4. ما مدي تأثير استخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري؟

ثانيًا: الدراسات السابقة:

يشكل الإطار النظري للدراسات السابقة أساسًا مهما في الدراسة العلمية؛ ذلك أنه ينشئ إطارا نظريا قويًا، ويضمن عدم تكرار الدراسات السابقة، ويزيد من مصداقية الدراسة، كما يساعد الباحث في اختيار المنهج الصحيح، وأيضا يوجه الباحث نحو تحديد الفجوة البحثية وبناء الإطار النظري، ويزيد من المصداقية ويحدد المنهج. علاوة على ذلك تحتوي الدراسات السابقة على أدوات متنوعة تساعد على توجيه الباحث نحو المراجع المهمة وتحسين جودة الدراسة. ويمكن لهذا الجزء من الدراسة أيضا المساهمة في إنشاء إطار للأدوات والطرق المستخدمة لتحليل البيانات وزيادة قدرة الباحث على اتخاذ قرارات منطقية، إضافة إلى مساعدة الباحث في اختيار المنهجية وجمع البيانات المناسبة والحصول على نتائج موثوقة. وعملا على تحقيق هذه الأهداف، فقد راعى الباحث في هذا الجزء الالتزام بالمعايير الأساسية لمراجعة الدراسات السابقة، و التي كان من أهمها:

1. الدقة في اختيار تلك الدراسات، وهو ما يعني اختيار الدراسات ذات العلاقة بموضوع البحث.
2. تصنيف تلك الدراسات حسب متغيرات الدراسة.

3. مراعاة التسلسل الزمني من الأحدث للأقدم عند عرض الدراسات بغض النظر عن اللغة التي استخدمت في إجراء تلك الدراسات.

ومن هذا المنطلق، تناول الباحث هذا الجزء من الدراسة من خلال استعراض العناصر التالية:

1. الدراسات السابقة التي تناولت موضوع الدراسة، كما يلي:

أ. الدراسات السابقة ذات الصلة بالمتغير المستقل (الذكاء الاصطناعي).

ب. الدراسات السابقة ذات الصلة بالمتغير التابع (إدارة مخاطر الجريمة المالية).

ج. الدراسات السابقة التي تناولت العلاقة بين المتغير المستقل والمتغير التابع.

د. مجال الاستفادة من الدراسات السابقة (الدراسات العربية والأجنبية).

هـ. نقاط الاتفاق بين الدراسة الحالية والدراسات السابقة.

و. نقاط الاختلاف بين الدراسة الحالية والدراسات السابقة.

ز. ما يميز الدراسة الحالية عن الدراسات السابقة.

2. الفجوة البحثية.

1. الدراسات السابقة التي تناولت موضوع الدراسة:

بعد الاطلاع على عديد من الدراسات التي تناولت متغيرات الدراسة، سواء المتعلقة منها بالذكاء الاصطناعي أو الدراسات التي تناولت مخاطر الجريمة المالية في القطاع المصرفي، أو تلك التي تناولت العلاقة بينهما – على قلتها – أو على الأقل علاقة الذكاء الاصطناعي بأحد أنماط الجرائم المالية، فقد تم تجميع الأهم منها والأقرب إلى موضوع الدراسة، وتم ترتيبها أدناه **بادئين بالدراسات السابقة ذات الصلة بالمتغير المستقل**، يليها **الدراسات السابقة ذات الصلة بالمتغير التابع**، وأخيرا **الدراسات السابقة التي تناولت العلاقة بين المتغير المستقل والمتغير التابع** وموضوع دراساتنا، ثم ملخص لهذه الدراسات، وقد جاءت هذه الدراسات كالتالي:

أ. **الدراسات السابقة ذات الصلة بالمتغير المستقل (الذكاء الاصطناعي):**

نستهل هذه المجموعة من الدراسات السابقة **بدراسة (الأسد، 31 مارس 2023) بعنوان: (الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية)**، وهذه الدراسة ناقشت تقنيات ونظم الذكاء الاصطناعي (AI) الذي تتسابق دول العالم المتقدمة في إجراء الأبحاث حول تقنياته ونظمه المختلفة، وقد تمثل هدف الدراسة في التعرف على الفرص والمخاطر الناتجة من استخدام تقنيات الذكاء الاصطناعي، وواقع الدول العربية في هذا المجال، وتوصلت الدراسة إلى أن الذكاء الاصطناعي (AI) بنظمه وتقنياته المتعددة، يقدم فرصًا واعدة لا بد من العمل على استغلالها، وذلك بتوفير البنية العلمية ثم التقنية، أما من حيث المخاطر والتهديدات التي تشكلها بعض تقنيات الذكاء الاصطناعي (AI)، فيجب أخذها على محمل الجد وإعداد الاحتياطات والحلول اللازمة لمواجهتها والحد من أضرارها؛ إذ أنه كلما تم تطوير تقنيات ذكية لاستعمالها في الجوانب الخيّرة، طوّر "الأشرار" تقنيات منافسة لاستخدامها في تحقيق أهدافهم المختلفة، وفيما يتعلق بواقع الدول العربية في مجال الذكاء الاصطناعي، ترى الدراسة أن بعضها تقدم بخطوات عملية جيدة في هذا الشأن، بينما لا يزال بعضها في حدود تصميم إستراتيجيات نظرية لم تجد بعد طريقها للتنفيذ الفعلي، فيما الفريق الثالث لا يزال بعيد كل البُعد في مجال الذكاء الاصطناعي.

أما **دراسة (Zador et al.، 22 مارس 2023) بعنوان: (Catalyzing Next-Generation Artificial Intelligence through NeuroAI)**، فقد ناقش الباحثون فيها العلاقة بين علم الأعصاب (Neuroscience) والذكاء الاصطناعي (AI)، وأهمية علم الأعصاب (Neuroscience) في دفع التقدم في مجال الذكاء الاصطناعي (AI)، وقد هدفت هذه الدراسة إلى توفير نظرة عامة على المفاهيم الرئيسية في علم الأعصاب (Neuroscience) والذكاء الاصطناعي (AI) ومجال الذكاء الاصطناعي العصبي (NeuroAI) الناشئ، وأهمية علم الأعصاب (Neuroscience) في تقدم الذكاء الاصطناعي (AI)،

وتشجيع التفاعل المتبادل بينهما للاستفادة من ثروة المعرفة حول الدماغ وتطبيقها على أنظمة الذكاء الاصطناعي (AI)، كما هدفت هذه الدراسة أيضا إلى استكشاف إمكانية تطوير وكيل ذكي (Intelligent Agent) يتمتع بقدرات على مستوى قدرات الإنسان، وكذا تطوير نماذج اصطناعية قادرة على محاكاة سلوك الحيوانات بدقة عالية من خلال التحكم بأجساد افتراضية في بيئات افتراضية، وقد انتهت الدراسة إلى عدة نتائج مهمة، منها أن النظم الحالية للذكاء الاصطناعي (AI) لا تزال تفتقر إلى القدرات الحسية – الحركية، حيث إن جهود تطوير الذكاء الاصطناعي (AI) ونماذجه حاليا تركز بشكل كبير على تقنيات وتطبيقات تعلم الآلة (Machine Learning) دون التركيز بالقدر نفسه على تقنيات وتطبيقات الذكاء الاصطناعي العصبي (NeuroAI)، وشددت الدراسة على أنه من أجل تسريع تقدم الذكاء الاصطناعي (AI) يجب علينا الاستثمار في البحث بشكل أساسي فيما يسمى "الذكاء الاصطناعي العصبي / NeuroAI "، حيث تؤكد الدراسة على أن الاستثمار في بحوث الذكاء الاصطناعي العصبي (NeuroAI) وتطوير نماذج قادرة على اجتياز اختبار تورينج المتجسد (Embodied Turing Test) سيدفع التقدم في مجال الذكاء الاصطناعي (AI) ويقربنا من تحقيق الذكاء العام الاصطناعي (General AI).

بينما تناولت **دراسة (Simion and Kelp، 13 مارس 2023) بعنوان: (Trustworthy Artificial Intelligence)** مفهوم الذكاء الاصطناعي الموثوق (Trustworthy Artificial Intelligence)، وأبرزت فرصه في تعزيز الرفاهية وتقدم المجتمعات، إلى جانب التحديات الأخلاقية والقانونية والاجتماعية والتكنولوجية التي يواجهها، وهدف الباحثان في هذه الدراسة إلى تطوير الأدبيات العلمية من خلال تقديم تعريف واضح للذكاء الاصطناعي الموثوق باستخدام مفهوم الالتزامات الوظيفية (Functional Commitments)، موضحين أن الذكاء الاصطناعي الموثوق (Trustworthy AI) هو ذلك الذي يحقق معايير أداء التزاماته بقوة إرادة قصوى، وقد تناول الباحثان أيضًا التمييز بين كلا من الالتزامات التصميمية والوظيفية، وربطا بين مفاهيم الثقة (Trust) والجدارة بالثقة (Trustworthiness) في السياسة والصناعة والعلوم والفلسفة، مشددين على عدم جدوى استخدام معايير نفسية مثل الإرادة الحسنة أو الصفات الشخصية في تعريف الذكاء الاصطناعي الموثوق، وفي نهاية المطاف قدم الباحثان إطارا مفاهيميًا يحدد الالتزامات المرتبطة بوظائف الأنظمة الذكية.

وعلى الجانب الآخر تناولت **دراسة (Blanco and Garrido-Merch، يوليو 2022) بعنوان: (Do Artificial Intelligence Systems Understand?)** مناقشة ما إذا كانت أنظمة الذكاء الاصطناعي (AI Systems) قادرة على الفهم أم لا، ومن أجل تحقيق هذا الهدف تناولت الدراسة بالشرح والتحليل النهج الحالي للذكاء الاصطناعي (AI) وتطبيقاته المتعددة، ومنها النظم الخبيرة (Expert Systems)، وتعلم الآلة (Machine Learning)، والتعلم العميق (Deep Learning)، والذكاء الاصطناعي العصبي (NeuroAI)، والنماذج الشبكية الاحتمالية (Probabilistic Graphical Models - PGMs)، مع توضيح كيفية تمثيل هذه النماذج للمعرفة وتعلم الأنماط من البيانات، كما ناقشت الدراسة أيضا المفاهيم الفلسفية للفهم والذكاء، وقد توصلت الدراسة لعدة نتائج، منها: أن الفهم يتطلب الحدس (Intuition) والمرجعية الذاتية (Self-referential)، بينما الأنظمة الحالية من الذكاء الاصطناعي (AI) وتطبيقاته تعالج المعلومات فقط من خلال اتباع التعليمات أو الأنماط المستنتجة إحصائيًا، ومن ثم فهي لا تفهم المعاني، ومن ثمَّ تفتقد الذاتية (Subjectivity)، إذًا فعلى الرغم من أن السلوك قد يبدو ذكيًا، إلا أن التحليل يظهر عدم وجود فهم أو استيعاب داخلي (Internal Assimilation) في الآلات في الوقت الحاضر، وعلى الرغم من ذلك تؤكد الدراسة أنه لا يمكن استبعاد أن يحمل المستقبل تطويرا للأنظمة التي تتمتع بالذاتية (Subjectivity) والحالات العقلية (Mental States) من خلال التعلم الذاتي المعقد بشكل كبير.

بينما تناولت دراسة **(Birhane، يونيو 2022) بعنوان: (Automating Ambiguity: Challenges and Pitfalls of Artificial Intelligence)** التحديات العلمية والأخلاقية المتعلقة بالذكاء الاصطناعي، من خلال تحليل الافتراضات النظرية للأسس العلمية الضعيفة في التنبؤ (Predicting) والتصنيف (Sorting & Taxonomizing) للسلوك البشري،

وهدفت الدراسة إلى تعزيز العدالة (Justice) والمساواة (Equality) في مجال أنظمة تعلم الآلة (ML) عبر إجراء تحليل منهجي لأبحاثها، مما يساعد على معالجة المشكلات المقترنة بها وتحديد الاتجاهات المستقبلية، ونتج عن الدراسة ثلاثة إسهامات رئيسية، ففي جانب **الإسهام النظري (Theoretical)** أثبتت الدراسة استحالة التنبؤ الدقيق بالسلوك البشري المعقد، حيث إن البشر غير قابلين للتحديد، وتُعدّ الافتراضات الحالية في أنظمة تعلم الآلة نوعًا من (الظلم الخوارزمي/Algorithmic Injustice)، مما يؤدي إلى تشكيل صور نمطية ثابتة تضر بالفئات المهمشة مثل النساء والأقليات، بينما في جانب **الإسهام التجريبي (Empirical)** فقد كشف الدراسة عن نقص الدقة في بعض تطبيقات رؤية الحاسب (Computer Vision)، مثل التعرف على الوجوه (Face and Emotion Recognition)، مما يشكل خطرًا على المستخدمين، وتظهر مراجعة البيانات المستخدمة أنها تؤدي إلى تطبيع الصور النمطية الضارة، وأخيرا في جانب **الإسهام المنهجي (Methodological)** قدمت الدراسة تحليلاً لأكثر من 100 ورقة علمية في مجال تعلم الآلة (ML)، مع تحديد 67 قيمة أساسية، كما اقترحت الدراسة أيضا إطارا أخلاقيًا (Ethical Framework) يأخذ في الاعتبار الجوانب الاجتماعية والبيئية للذكاء الاصطناعي (AI)، مشددة على ضرورة إعادة التفكير في الهياكل الاجتماعية لتحقيق ذكاء اصطناعي عادل ومفيد (Fair and Useful AI).

أما دراسة **(Aggarwal et al.، 1 يناير 2022) بعنوان: (Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning)** فقد قدمت مراجعة شاملة لتقنيات وتطبيقات الذكاء الاصطناعي (AI) وتعلم الآلة (ML) والتعلم العميق (DL)، ودور كل منها في تحسين حياة البشر، خصوصًا في تحليل البيانات الكبيرة (Big Data Analysis)، وتطرقت الدراسة أيضا إلى الخوارزميات (Algorithms) والتطبيقات الحالية والمستقبلية في هذا المجال، وقد سعى الباحثون في هذه الدراسة لتحقيق عدة أهداف، أهمها تقديم تعريفات مبسطة للمفاهيم الأساسية في هذا المجال، وشرح كيفية عمل الأنظمة والتقنيات المستخدمة، وإبراز المجالات البحثية وتحليل وجهات النظر المختلفة في بحوث الذكاء الاصطناعي (AI) وسيناريوهات تطبيقه، ومناقشة المميزات والتحديات الحالية له، واستنتاج احتمالات النمو وآفاق المستقبل، وتعزيز فهم التقنيات وتشجيع اعتماد الذكاء الاصطناعي (AI) في مجالات متنوعة، نهاية بتوفير مرجع شامل حول الذكاء الاصطناعي، وقد خلصت الدراسة إلى أن تقنيات الذكاء الاصطناعي (AI) ستستمر في التقدم لخدمة البشرية، لكن مدى هذا التقدم غير معروف، وأوصت الدراسة باستخدام نماذج تعلم الآلة (ML) والتعلم العميق (DL) لتعزيز القدرة على التنبؤ واتخاذ القرارات، إلا أن معالجة البيانات الكبيرة قد تتطلب جهدًا بشريًا كبيرًا؛ لذا يبدأ دور الذكاء الاصطناعي (AI) في تحليل البيانات الضخمة (Big Data)، مما يساعد في تقليل التدخل البشري وتحديد أنماط صنع القرار.

بينما قدمت دراسة **(Zhang and Lu، سبتمبر 2021) بعنوان: (Study on Artificial Intelligence: The State of the Art and Future Prospects)** نظرة شاملة على مجال الذكاء الاصطناعي (AI) مع التركيز على آفاقه المستقبلية واحتمالات التطور، واستعرضت الدراسة التقنيات الأساسية والسيناريوهات التطبيقية والتحديات التي تواجه الذكاء الاصطناعي (AI) من خلال مراجعة أحدث الدراسات الحالية والمستقبلية، كما تناول الباحثون في هذه الدراسة تطبيقات الذكاء الاصطناعي (AI) في العديد من مجالاته وتطبيقاته، ومنها البرمجة التلقائية (Automated Programming)، والنظم الخبيرة (Expert Systems)، والروبوتات الذكية (Intelligent Robots)، وقد هدفت هذه الدراسة إلى تقديم مراجعة منهجية تعتمد على تكامل المعلومات الصناعية (Industry Information Integration)، مع عرض شامل لنطاق الذكاء الاصطناعي (AI) بما يتضمن الخلفية (Background)، والدوافع (Drivers)، والتقنيات (Technologies)، والتطبيقات (Applications)، وقد خلصت الدراسة إلى أن الذكاء الاصطناعي (AI) لا يتطلب فقط التفكير المنطقي (Logical Thinking)، والتقليد (Imitation)، بل يتطلب أيضًا العاطفة (emotion)، حيث إنها جزء لا غنى عنه، وأن الإنجاز الكبير

التالي في مجال الذكاء الاصطناعي (AI) يمكن أن يتجاوز قدرات الاستدلال المنطقي للحواسب (Logical Reasoning Capabilities) من خلال منحها قدرات عاطفية (Emotional Capabilities)، ومن ثمَّ فقد يتجاوز ذكاء الآلة قريبًا ذكاء الإنسان.

ونختم أخيرا **بدراسة (قمورة ومحمد وكروش، 2018) بعنوان: "الذكاء الاصطناعي بين الو اقع والمأمول، دراسة تقنية وميدانية"**، وهي الدراسة التي تناولت مفهوم الذكاء (Intelligence) عبر التاريخ، وصولاً إلى تعريف الذكاء الاصطناعي (AI)وخصائصه، وقامت بتحليل تعلم الآلة (ML) كأحد أهم فروع الذكاء الاصطناعي (AI)، مع استعراض تطبيقاته الحالية مثل التسويق الذكي (Smart Marketing)، والطائرات الذكية ذاتية التوجيه (Smart Drones)، والسيارات الذكية ذاتية التوجيه (self-driving cars)، والواقع المعزز (Augmented Reality)، والإنسان الآلي البشري "صوفيا" (Sophia Humanoid)، وقد هدفت الدراسة إلى رسم صورة واضحة لتطورات التقنيات الذكية (Smart Technologies) ومستقبلها، خاصة في الوسط الأكاديمي، مما يتيح للباحثين متابعة دراسات دقيقة حول هذا الموضوع، وقد توصلت الدراسة إلى نتائج مهمة، منها: أن المجتمعات البشرية ستتجه نحو التعايش مع الآلات، وهو ما يتضح في المدن الذكية (Smart Cities) والمنازل الذكية (Smart Homes) وإنترنت الأشياء (Internet of Things)، واستبعدت الدراسة المخاوف من تدمير البشرية بسبب الآلات أو استقلاليتها الكاملة، مستندة إلى قاعدتين: الأولى هي استحالة وضع خوارزمية مطلقة نظرًا لأن مصممها غير مطلق، والثانية هي الفارق الجوهري بين الأداء والخلق، حيث يستطيع الروبوت التفوق في مجال ما لكنه لا يستطيع ابتكار القواعد لهذا المجال.

ب. الدراسات السابقة ذات الصلة بالمتغير التابع (إدارة مخاطر الجريمة المالية):

نستهل هذا الجزء بإلقاء الضوء على **دراسة (Gao et al.، 20 أكتوبر 2023) بعنوان: (Dirty Money: How Banks Influence Financial Crime)** لكيفية تأثير المؤسسات المصرفية على الجرائم المالية، من خلال تحليل العلاقة بين ربحية المؤسسات المصرفية وتقارير النشاط المشبوه (SARs)، وسعت الدراسة بذلك للتعرف على الحوافز التي تدفع المؤسسات المصرفية للإبلاغ عن الجرائم المالية، وفهم تأثير ضغوط الربح على سياسات الإبلاغ وجذب العملاء من المجرمين، ودراسة أثر إستراتيجيات الإبلاغ على مستوى الجرائم المالية المبلغ عنها، وتوصلت الدراسة إلى أن المؤسسات المصرفية التي تواجه ضغوطًا ربحية قد تعتمد سياسات إبلاغ متساهلة أو ضعيفة، مما يجذب العملاء من المجرمين، كما أكدت الدراسة أن هناك علاقة سببية بين حوافز قبول المخاطر (Risk-taking Incentives) مثل: التنافس، والانخفاض، والزيادة في تقارير النشاط المشبوه (SARs)، وأن قوة أو ضعف معايير الإبلاغ تؤثر على النشاط الإجرامي، حيث يمكن للمجرمين استغلال ضعف نظم الإبلاغ، وبناء على ذلك قدمت الدراسة مجموعة من التوصيات لتعزيز جهود مكافحة الجرائم المالية وحماية النظام المالي؛ فقد أوصت الدراسة بضرورة تعزيز الرقابة التنظيمية من خلال تحسين التشريعات لضمان سياسات صارمة لمكافحة الجرائم المالية، كما أوصت بضرورة مراقبة ضغوط الربح (Profit-seeking Pressures) ومتابعة حوافز قبول المخاطر لضمان عدم التأثير على جهود مكافحة غسل الأموال، بالإضافة إلى أهمية الحفاظ على معايير إبلاغ صارمة (Stringent Reporting Standards) لردع الأنشطة غير المشروعة، وأكدت الدراسة أيضا على ضرورة تبني وتنفيذ ممارسات إدارة مخاطر قوية لتحديد ومعالجة الثغرات، علاوة على أهمية تعزيز التعاون بين المؤسسات المصرفية والهيئات التنظيمية (Regulators) لضمان فاعلية التدابير المتخذة، وختاما شددت الدراسة على أهمية التقييم الدوري لمراجعة سياسات مكافحة الجرائم المالية للتكيف مع التهديدات المتطورة.

أما الدراسة الثانية فهي **دراسة (Kasztelnik، 19 أكتوبر 2023) بعنوان: (The Observational Study Financial Fraud Offense Themes and Financial Fraud Risk of Money Laundering to Increase Financial Global Sustainability Compliance)**، والتي تناولت تأثير الابتكارات التكنولوجية على تطور الجرائم المالية (Financial

Crimes) ووسائل مكافحتها في المؤسسات المصرفية الأمريكية، وناقشت الدراسة ما تعانيه هذه المؤسسات من تحديات، مثل: حجم الجرائم، نقص الأدوات، وتغير السياسات، مما يعرضها للعديد من المخاطر، ومنها مخاطر السمعة (Reputation Risk)، والمخاطر التشغيلية (Operational Risk)، والمخاطر القانونية (Legal Risk)، ومخاطر التركز (Concentration Risk)، وهو ما يؤدي إلى عواقب سلبية على هذه المؤسسات، منها: زيادة تكاليف الامتثال (Compliance Costs)، والخضوع للعقوبات المالية والتنظيمية (Financial and Regulatory Penalties)، وقد هدفت الدراسة إلى استكشاف كيفية تحديد مسؤولي مكافحة الجرائم المالية لمجالات الاحتيال من أجل خفض المخاطر وزيادة الاستدامة المالية (Financial Sustainability).

وقد توصلت الدراسة إلى عدة نتائج مهمة، فعلى **مستوى الامتثال (Compliance)** خلصت الدراسة إلى أنه يجب على مسؤولي الامتثال (Compliance Officers) تحديث مجالات الجرائم المالية وفقًا لثماني مجالات ناشئة، بما يؤدي لتعزيز برامج الامتثال وتطوير مؤشرات إنذار جديدة، أما على **مستوى الممارسة (Practice)** رأت الدراسة إلى أنه يتوجب على مسؤولي الامتثال (Compliance Officers) تعديل الإجراءات التشغيلية (Operational Procedures) لجمع معلومات محدثة عن العملاء ذوي المخاطر العالية (High-Risk Customers)، مما يعزز الشفافية (Transparency) ويقلل من تعرض المؤسسات لمخاطر الجرائم، بينما على **مستوى النظرية (Theory)** تسهم الدراسة في سد الفجوة المعرفية (Knowledge Gap) حول إدارة مخاطر الجرائم المالية (Financial Crimes Risk Management)، وتدعو إلى مزيد من الأبحاث في هذا المجال، وأخيرا فعلى مستوى **التغيير الاجتماعي (Social Change)** أوضحت الدراسة إلى أنه يمكن للمؤسسات المصرفية تعزيز الوعي العام (Public Awareness) حول الجرائم المالية من خلال تثقيف عملائها وتنفيذ مبادرات التثقيف العام (Public Education).

بينما تعرضت **دراسة (Afjal et al.، 29 أغسطس 2023) بعنوان: (Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability.)**، إلى استكشاف كيفية تفاعل الاحتيال المالي (Financial Fraud) ومخاطر الائتمان (Credit Risks)، وتحديد طبيعة العلاقة بينهما، وتأثير هذه العلاقة على الاستقرار المصرفي (Banking Stability) من خلال تقييم الأثر التراكمي لهذه العلاقة على المستوى الجزئي (البنوك الفردية) والكلي (القطاع المصرفي والاقتصاد الأوسع)؛ ونظرا لنتائجها المهمة تُعدّ هذه الدراسة إسهامًا كبيرًا في الخطاب الأكاديمي (Scholarly Discourse) وتفتح آفاقًا جديدة للبحث والسياسات في مجال الاستقرار المصرفي، فعلى مستوى **سد الفجوات البحثية**، قدمت الدراسة تحليلاً شاملاً للقوى المحركة بين الاحتيال المالي (Financial Fraud) ومخاطر الائتمان (Credit Risks) والاستقرار المصرفي (Banking Stability)، ودعت لاتباع نهج أكثر تكاملية لدراسة تأثيرات هذه العوامل على الاستقرار المصرفي، من خلال تسليط الضوء على المجالات التي قد تم التغاضي عنها، مما يعزز الفهم للعلاقة المعقدة بين هذه العوامل ويضع أساسًا للدراسات التجريبية لمعالجة الثغرات الحالية ويمهد الطريق لدراسات مستقبلية لتعميق الفهم حول هذه العلاقة المعقدة، وعلى مستوى **تطوير السياسات والإجراءات**، أكدت الدراسة على الحاجة إلى أطر تنظيمية فعالة وإستراتيجيات إدارة المخاطر (Risk Management Strategies) ضد الاحتيال المالي (Financial Fraud)، حيث إن تعزيز الفهم بين الاحتيال المالي (Financial Fraud) ومخاطر الائتمان (Credit Risks) يمكن أن يؤدي إلى تدابير تنظيمية أكثر قوة، مما يعزز المرونة في مواجهة الأزمات المالية، بينما على مستوى **توجيه إستراتيجيات إدارة المخاطر** (Risk Management Strategies) يمكن للأفكار المستمدة من الدراسة أن توجه إستراتيجيات إدارة المخاطر في القطاع المصرفي، مما يساعد المؤسسات على التخفيف من المخاطر المرتبطة بالاحتيال المالي ومخاطر الائتمان، ومن ثمَّ تعزيز أمن واستقرار القطاع المصرفي.

أما دراسة (KASIE and AKUJINMA، أغسطس 2022) بعنوان: (FRAUD AND ITS EFFECT ON BANKING INDUSTRY: A STUDY OF SELECTED BANKS IN NIGERIA) فقد ناقشت تأثير جرائم الاحتيال (Fraud Crimes) والجرائم المالية (Financial Crimes) في القطاع المصرفي النيجيري على الاقتصاد والأمن والرفاهية الاجتماعية، مع التركيز على جريمة غسل الأموال (Money Laundering) وعلاقتها بجرائم الاحتيال المالي (Financial Fraud Crimes)، وضرورة اكتشاف ومنع الاحتيال للحفاظ على ثقة الجمهور في المؤسسات المالية، وقد سعت هذه الدراسة إلى تحقيق العديد من الأهداف، أهمها: تحديد تأثير الاحتيال على ربحية الصناعة المصرفية (Banking Industry Profitability)، وتقييم تأثير هذه الجرائم على ثقة العملاء، وكذا استكشاف طبيعة وطرق وقوع جرائم الاحتيال (Fraud Crimes)، وقد توصلت الدراسة إلى عدة نتائج مهمة، منها: تحديد أنواع متعددة من جرائم الاحتيال، مثل: الرشوة (Bribery)، والاختلاس (Embezzlement)، والفساد (Corruption)، التزوير والتزييف (Forgery & Counterfeiting) وانتحال الشخصية (Impersonation) وسرقة بيانات الهوية (Identity Theft)، واحتيالات القروض (Loan Fraud)، والاحتيالات على بطاقات الائتمان (Credit Card Fraud)، والاحتيالات الإلكترونية، ومنها: الاحتيالات عبر البريد الإلكتروني (E-mail Fraud)، وأكدت الدراسة أن جرائم الاحتيال لها تأثير سلبي على ربحية المؤسسات المصرفية، مما يؤدي إلى خسارة العملاء وتقليل قاعدة رأس المال، كما أن لها تأثيرًا كبيرًا على ثقة العملاء، مما قد يؤدي لفقدان الثقة وخسارة المستثمرين، وختاما قدمت هذه الدراسة عدة توصيات تسهم في حماية القطاع المصرفي النيجيري واستعادة ثقة العملاء وجذب المستثمرين الأجانب، ومنها: ضرورة اتباع نمط عالمي في الإبلاغ عن المعاملات المشبوهة (Suspicious Transactions Reporting) إلى وحدة الاستخبارات المالية (Financial Investigation Unit) في البلد المعني، وضرورة اتخاذ تدابير تنظيمية ومساءلة وشفافية بين المؤسسات المصرفية والهيئات التنظيمية، والأهمية القصوى لتنفيذ برامج لمكافحة الاحتيال والالتزام باللوائح الصارمة.

في حين ناقشت دراسة (Mahony، 4 إبريل 2022) بعنوان: (Best Practices in Combating Fraud in Financial Institutions) أهمية الحوكمة (Governance)، وثقافة الامتثال (Culture of Compliance) في مكافحة الاحتيال والجرائم المالية في المؤسسات المالية والمصرفية، مع التركيز على إنشاء إطار فعال بعد جائحة كوفيد-19، وقد هدفت الدراسة إلى تحديد الخطوات العملية لإنشاء إطار لمكافحة الاحتيال (Framework for Combating Fraud)، وتقديم توصيات لتعزيز القدرات في منع واكتشاف الجرائم المالية (Prevent and Detect Financial Crimes)، وقد توصلت هذه الدراسة إلى عدد من النتائج والتوصيات التي تسهم بشكل كبير في تعزيز دفاعات المؤسسات المالية والمصرفية وحماية سمعتها وعملائها، ففي مجال **تعزيز الحوكمة (Governance) وثقافة المساءلة (Culture of Accountability)** رأت الدراسة ضرورة تعزيز ممارسات الحوكمة (Governance) وثقافة المساءلة (Culture of Accountability) داخل المؤسسات المصرفية، من خلال تحديد هياكل المسؤولية (Responsibility Structures)، وكذلك التحديد الواضح للإجراءات التفصيلية للمساءلة (Granular Accountability Measures)، أما في مجال **تعزيز إدارة مخاطر الاحتيال والجرائم المالية (Managing Fraud and Financial Crimes Risk)** فقد أوصت الدراسة بضرورة اتخاذ تدابير موحدة للكشف عن الاحتيال بفاعلية من خلال وجود إجراءات تحديد الاحتيال المنظمة والقياسية (Formalized and Standardized Fraud Identification Measures)، وفيما يتعلق بإجراءات التحقيق، فقد شددت الدراسة على أهمية اتباع أفضل الممارسات في التحقيقات، مثل جمع الأدلة والحفاظ على سرية المعلومات، بينما في مجال **خصوصية البيانات والسرية (Confidentiality and Data Privacy)**، أكدت الدراسة على ضرورة الامتثال لقوانين خصوصية البيانات (Data Privacy) أثناء التحقيقات، أما في جانب **الاعتبارات التنظيمية (Regulatory Considerations)**، فقد أشارت الدراسة إلى حتمية مواءمة برامج مكافحة الاحتيال مع المتطلبات التنظيمية (Regulatory Requirements) لتقليل المخاطر القانونية، وفيما يتصل **بالمراجعة المستمرة**، فقد أكدت الدراسة على أهمية التقييم المستمر لإستراتيجيات مكافحة الاحتيال لمواكبة التغيرات في المخاطر.

وفي السياق نفسه ناقشت **دراسة (Pradesyah et al.، نوفمبر 2021) بعنوان: (Fraud in Financial Institutions)** جرائم الاحتيال في المؤسسات المالية والمصرفية التقليدية في إندونيسيا، مع التركيز على تحليل بيانات من تقارير الحوكمة الرشيدة (Good Corporate Governance) للفترة من 2015 إلى 2019، وهدفت هذه الدراسة إلى استكشاف اتجاهات جرائم الاحتيال (Fraud Crimes Trends) انخفاضا وارتفاعا، حيث نجحت بعض المؤسسات في تقليل عدد الحالات في حين شهدت مؤسسات أخرى زيادة وارتفاعا في عدد الحالات، كما أصبحت الاحتيالات القائمة على التكنولوجيا كالاحتيالات السيبرانية (Cyber Frauds) مصدر قلق كبير، وأكدت الدراسة على أهمية فهم مخاطر جرائم الاحتيال التي يرتكبها الموظفون، مشيرة إلى نظرية مثلث الاحتيال (Fraud Traingle) كأداة لفهم أسباب الاحتيال، ودعت الدراسة إلى ضرورة تعزيز الأنظمة والإجراءات من خلال تطوير أنظمة متخصصة لرصد ومنع الاحتيال وشددت على أهمية التعاون بين الباحثين وصانعي السياسات في سبيل معالجة الإجراءات الاحتيالية بشكل فعال، كما أشارت الدراسة إلى أهمية المراقبة المستمرة للموارد البشرية من خلال تنفيذ إجراءات وقائية وأنظمة أمنية مشددة، مع اتخاذ إجراءات قانونية عند الحاجة وذلك سعيا لتعزيز مصداقية المؤسسات المالية وبناء ثقة الجمهور.

أما **دراسة (Muminovic، يناير 2021) بعنوان: (Typologies of Financial Crimes)** فقد ناقشت الجرائم المالية ولكن من منظور آخر، حيث ناقشت هذه الدراسة الجرائم المالية في سياق العولمة وأثرها على النظام المالي والمصرفي العالمي، مع التركيز على الخلفية النظرية وخصائص هذه الجرائم وأنواع ضحاياها، وهدفت الدراسة بذلك إلى تحديد أنواع الجرائم المالية وتصنيفاتها، وتحليل خصائص الجرائم المالية وتأثيرها على المجتمع والاقتصاد، مما يستدعي إستراتيجيات فعالة لمكافحتها، وتوصلت الدراسة إلى أن الجرائم المالية تمثل تهديدًا كبيرًا للنظام المالي والاقتصاد العالمي، وتشمل أنماطًا متنوعة، مثل: الفساد (Corruption)، والاحتيال (Fraud)، والسرقة (Theft)، والتلاعب (Manipulation) وغسل الأموال (Money Laundering)، وغيرها، كما أوضحت تأثير العولمة على الجرائم المالية والذي تمثل في زيادة تعقيدها، وزيادة انتشار الشبكات الإجرامية المنظمة، مما يزيد من التحديات أمام المؤسسات المصرفية والجهات الرقابية، وبينت الدراسة أن السلطات المختصة تواجه تحديات في تعقب الجرائم المالية بسبب اختلافات القوانين الوطنية وتعقيد الأنظمة المالية الحديثة، مما يبرز الحاجة للتعاون الدولي، وأوصت الدراسة بضرورة تعزيز التعاون بين الدول لمكافحة الجرائم المالية العابرة للحدود (Cross-Border Financial Crimes) والحاجة إلى تحسين وتعزيز الإجراءات التنظيمية لمواجهة التحديات الحالية التي تفرضها الجرائم المالية.

أما دراسة **(Nyakarimi et al.، يناير 2020) بعنوان: (Risk Assessment and Fraud Prevention in Banking Sector)** فقد سلطت الضوء على أهمية عملية تقييم المخاطر (Risk Assessment Process) كأداة وقائية حيوية في مكافحة الاحتيال في القطاع المصرفي، وقامت الدراسة بذلك من خلال استعراض أنماط جرائم الاحتيال (Fraud Types) في هذا القطاع، مُركّزة على الاحتيال الداخلي (Internal or In-house Fraud) الذي يرتكبه العاملون في المؤسسات المصرفية، والاحتيال الخارجي (External Fraud) الذي يقوم به العملاء أو أطراف العلاقة الآخرين، كما ناقشت الدراسة أيضا عملية تقييم المخاطر (Risk Assessment Process) وعلاقتها بجرائم الاحتيال، خاصة مع تزايد الأنشطة الاحتيالية نتيجة للتقدم التكنولوجي، وهدفت الدراسة إلى التعرف على تأثير تقييم المخاطر على منع الاحتيال في القطاع المصرفي في كينيا، وسد الفجوة البحثية حول العلاقة بين تقييم المخاطر والاحتيال، وأثبتت نتائج الدراسة أن الاحتيال المصرفي أصبح أكثر تعقيدًا وسهولة في ارتكابه بفضل التقدم التكنولوجي، وأن هناك حاجة كبرى لتحسين الضوابط الأمنية وآليات تحديد المخاطر، وعليه أوصت الدراسة بضرورة إشراك محللي المخاطر (Risk Analysts) بشكل منتظم لتحديد مؤشرات الاحتيال مبكرًا، وكذا بضرورة تدريب الموظفين بشكل دوري لتعزيز قدراتهم في اكتشاف المخاطر والتعامل معها، مما يساعد في منع الاحتيال.

ج. الدراسات السابقة التي تناولت العلاقة بين المتغير المستقل والمتغير التابع:

نستهل هذا الجزء **بدراسة (Ahmadi، فبراير 2024) بعنوان: "Open AI and its Impact on Fraud Detection in Financial Industry"** والتي هدفت إلى مناقشة الزيادة في الأنشطة الاحتيالية في القطاع المالي والمصرفي، خاصة بعد انتشار الخدمات المصرفية الرقمية (Digital Banking) في ظل جائحة كورونا، وهو ما أدى إلى ظهور أنماط احتيالية جديدة مثل: التصيد الاحتيالي عبر البريد الإلكتروني (Phishing)، والاحتيال السيبراني (Cyber Fraud)، والذي تسبب في خسائر تصل إلى 32.34 مليار دولار في 2021، وتوصلت الدراسة إلى أن الأساليب التقليدية القائمة على القواعد (Rule-based Methods) تعاني من تحيزات بشرية (Human Bias)، ولم تعد كافية في مواجهة تقنيات الاحتيال المتطورة، وتؤدي إلى نتائج إيجابية كاذبة (False Positive Results)، وهو ما يؤدي بدوره لرفض بعض المعاملات المشروعة للعملاء نتيجة لتصنيفها الخاطئ على أنها معاملات احتيالية (False Positives) مما يضر بالمؤسسات المالية ويؤدي إلى فقدان العملاء.

وأوصت الدراسة بتبني تقنيات تعلم الآلة (Machine Learning) والذكاء الاصطناعي التوليدي (Generative AI)، كوسائل أكثر كفاءة في الكشف عن الاحتيال، كما أشارت الدراسة إلى أهمية مواكبة تقنيات الاحتيال المتطورة، وتفعيل التدابير الاستباقية التي تشمل استخدام أدوات خوارزميات الانحدار اللوجستي (Logistic Regression)، وأشجار القرار (Decision Trees)، والغابة العشوائية (Random Forest)، والشبكات العصبية (Neural Networks)، والتعلم العميق (Deep Learning)، ومعالجة اللغة الطبيعية (Natural Language Processing)، وختامًا أبرزت الدراسة فرص الشراكة بين شركة OpenAI[1] وشركات التكنولوجيا المالية (FinTech) لتعزيز الأمان وتجربة العملاء، وقدمت الدراسة أمثلة ناجحة مثل شركة Stripe وماستركارد MasterCard وكبرى شركات التكنولوجيا التي استخدمت هذه التقنيات في مكافحة الاحتيال.

أما **دراسة (بن علي، ديسمبر 2023) بعنوان: "مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي"**، فقد هدفت لمناقشة الجوانب النظرية للذكاء الاصطناعي (AI) وتأثيره في الكشف عن الاحتيال وإدارة المخاطر (Risk Management) في القطاع المصرفي، مع التركيز على تطبيقات الأمن السيبراني (Cyber Security) من خلال فهم دور الذكاء الاصطناعي في تعزيز الأمان الرقمي (Digital Security) ومكافحة الجرائم المالية، وتقديم توصيات لتحسين العمليات المصرفية وتعزيز الثقة بين المؤسسات المالية وعملائها، واستعرضت الدراسة حالة **بنك Danske** الدانماركي، وخلصت إلى عدة نتائج رئيسية، منها: أن استخدام الذكاء الاصطناعي (AI) في الأمن السيبراني (Cyber Security) قد أسهم في اكتشاف 95% من حالات الاحتيال الفعلي، مما يزيد من كفاءة إدارة المخاطر، كما أن استخدام تقنيات الذكاء الاصطناعي (AI) يؤدي لتبسيط العمليات المصرفية كتسهيل فتح الحسابات وإنشاء درجات ائتمانية، مما يحسن تجربة العملاء، وأيضا أن الذكاء الاصطناعي يمكن من معالجة قضايا مثل البطالة والتحيز في تصميم الأنظمة، ومن جانب آخر شددت الدراسة على ضرورة معالجة التحديات والمسؤوليات القانونية المرتبطة بقرارات الذكاء الاصطناعي، كما شددت أيضا على ضرورة تعزيز التعاون بين المؤسسات المالية والحكومات لتحسين استخدام الذكاء الاصطناعي (AI) في مكافحة الاحتيال وضمان تواجد الفئات الضعيفة في السوق، وختاما أوصت الدراسة بتبني إستراتيجيات متكاملة لتعزيز الأمان الرقمي (Digital Security) وتحسين الخدمات المصرفية.

بينما تناولت **دراسة (Mytnyk et al.، مايو 2023) بعنوان: "Application of Artificial Intelligence for Banking Operations Recognition Fraudulent"** إمكانات الذكاء الاصطناعي (AI) في تحسين اكتشاف جرائم الاحتيال في المؤسسات المصرفية، خاصة في ظل زيادة هذه الجرائم بعد جائحة كورونا والحرب في أوكرانيا، وهدفت الدراسة إلى فهم كيفية استخدام تطبيقات الذكاء الاصطناعي (AI Applications) في التعرف على المعاملات المصرفية الاحتيالية، مع

[1] OpenAI هي منظمة أبحاث أمريكية في مجال الذكاء الاصطناعي (AI) تتكون من كيانين، أولاهما: OpenAI Inc، وهي قطاع بحثي غير ربحي، والأخرى: OpenAI Global LLC، وهي شركة فرعية هادفة للربح تأسست لتسويق تقنيات وتطبيقات الذكاء الاصطناعي الخاصة بها، وقد تأسست OpenAI في عام 2015 من قبل مجموعة من الباحثين والعلماء ورجال الأعمال، ومن بين المؤسسين الأكثر شهرة: سام ألتمان، وجريج بروكمان، وبيتر ثيل، وإيلون ماسك (https://www.britannica.com/money/OpenAI).

التركيز على تطوير خوارزميات آلية موثوقة (Reliable Automated Algorithms)، وقد توصلت الدراسة إلى عدة نتائج مهمة، أولها: أن خوارزميات تعلم الآلة (Machine Learning Algorithms) التي تعتمد على خوارزميات الشبكات العصبية الاصطناعية (Artificial Neural Network -ANN) خاصة خوارزميات التصنيف (Classification Algorithms)، مثل (شجرة القرار Decision Tree والانحدار اللوجستي Logistic Regression)، قد أثبتت فاعليتها في تحسين دقة اكتشاف الاحتيال؛ إذ تمكنت من تصنيف المعاملات بناءً على خصائص محددة، وثاني هذه النتائج: أن خوارزمية التعميم المكدس (Stacked Generalization) قد أظهرت نتائج أفضل مقارنة بالخوارزميات الفردية، مما يعزز القدرة على كشف الاحتيال، وفي ثالث هذه النتائج: أكدت الدراسة على ضرورة الوصول إلى بيانات تاريخية شاملة وعالية الجودة لتدريب نماذج تعلم الآلة (Machine Learning Models) بفاعلية، مشيرة إلى أن البيانات غير الكاملة قد تؤدي إلى نتائج إيجابية كاذبة (False Positive Results)، أما النتيجة الرابعة ففيها: اعترفت الدراسة بتحديات مثل عدم الشفافية وعدم القابلية للتفسير لدى الخوارزميات (Lack of Transparency and Interpretability of Algorithms)، والمخاوف المتعلقة بالخصوصية (Privacy Concerns)، والتحيز في تحليل البيانات (Bias in Data Analysis)، مشددة على ضرورة التعامل مع هذه القضايا وعلاجها لضمان عمل أنظمة كشف الاحتيال بشكل آمن وفعال، وفي النهاية أوصت الدراسة بتبني تقنيات الذكاء الاصطناعي مع التركيز على معالجة التحديات لضمان تحقيق نتائج دقيقة في الكشف عن الاحتيال المصرفي.

في حين سلطت **دراسة (Piao and Xiao، ديسمبر 2022) بعنوان: Risk Management Analysis of Modern Commercial Banks"Using Behavioral Finance Theory and Artificial Neural Networks"** الضوء على المخاطر التي تواجه مؤسسات القطاع المصرفي مع التركيز على مخاطر الائتمان (Credit Risks) كأهم هذه المخاطر، ففي ظل العولمة الاقتصادية وزيادة تقلبات الأسواق، أصبحت مخاطر الائتمان (Credit Risks) في أعلى مستوياتها، مما يستدعي تحسين أساليب إدارة المخاطر (Risk Management)، وقد تناولت الدراسة تقييم مخاطر الائتمان في البنوك التجارية، واقترحت نموذجًا يعتمد على خوارزميات الذكاء الاصطناعي (AI Algorithms) لتحسين عملية اتخاذ القرار وتقليل المخاطر، واستخدمت الدراسة بيانات حقيقية من بنوك في الصين، وخلصت إلى عدة نتائج ذات دلالة وأهمية كبرى لمؤسسات القطاع المصرفي خاصة ومؤسسات القطاع المالي عامة؛ فقد أكدت الدراسة أن مخاطر الائتمان (Credit Risks) تتسم بطبيعتها غير المتماثلة (Asymmetric Nature) وغير الخطية (Nonlinear Characteristics)، مما يتطلب تقييمًا دقيقًا وشاملاً، وأشارت الدراسة إلى أن العواطف والتحيزات الشخصية (Emotions and Biases) لمديري المخاطر قد تؤثر سلبًا على إدارة المخاطر، كما أوضحت الدراسة أن النماذج التقليدية المستخدمة في تقييم المخاطر لم تعد كافية، مما يستدعي استخدام تقنيات متقدمة مثل نظرية التمويل السلوكي (Behavioral Finance Theory) والشبكات العصبية الاصطناعية (Artificial Neural Networks-ANN)، وفي هذا الصدد بينت الدراسة بالدليل أن استخدام خوارزميات مثل خوارزمية الشبكات العصبية الاصطناعية ذات الانتشار المُرتد أو العكسي (BP-ANN) Backpropagation – Artificial Neural Network، وخوارزمية آلة المتجهات Vector Machine قد أثبت فاعليته في تحسين دقة تصنيف البيانات (Data Classification Accuracy) وتوفير أسس تنبؤية أفضل لقرارات القروض، وختاما أوصت الدراسة بتبني نماذج تقييم مخاطر الائتمان المتقدمة لتحسين ربحية المؤسسات المصرفية وتقليل القروض المتعثرة وتعزيز القدرة على تحديد المخاطر وإدارتها.

أما **دراسة (Awasthi، أكتوبر 2022) بعنوان: "Using Artificial Intelligence to Prevent Banking Fraud"** فقد تناولت استخدام تطبيقات الذكاء الاصطناعي (AI Apps) وتقنيات تعلم الآلة (ML) لمواجهة تحديات الاحتيال المصرفي وتعزيز الإجراءات الأمنية في القطاع المصرفي، وهدفت الدراسة إلى استكشاف كيفية استخدام الذكاء الاصطناعي (AI)لمنع الاحتيال المصرفي، مع التركيز على نوعين شائعين من الجرائم المالية، وهما: سرقة الهوية (Identity Theft)، والتصيد الاحتيالي عبر البريد الإلكتروني (Phishing Fraud)، وقدمت الدراسة أمثلة واقعية على ذلك، ومنها خسارة بنك **"Crelan"**

البلجيكي نحو 75.8 مليون دولار نتيجة التصيد الاحتيالي عبر البريد الإلكتروني (Phishing Fraud)، وقد خلصت الدراسة إلى أن الذكاء الاصطناعي (AI) وتعلم الآلة (ML) يساعدان المؤسسات المصرفية في حماية أموالها وبيانات عملائها من خلال تطوير حلول تشمل مصادقة العملاء (Customer Authentication) وفحوصات أمنية متعددة المستويات، وفي مجال مكافحة التصيد الاحتيالي، تقوم التطبيقات بتحليل البيانات التعريفية (Metadata) وسلوك المستخدم (User Behavior) لتحديد التهديدات المحتملة، أما في مجال سرقة الهوية (Identity Theft)، فقد تم تطوير حلول تتضمن معايير لمصادقة الهوية (Authentication Parameters for Identity)، مثل التحقق من صحة الوثائق والحبر (Validation of Special Paper and Ink)، والتعرف على الوجه (Facial Recognition)، وشددت الدراسة على أهمية البحث والتطوير المستمر في الذكاء الاصطناعي (AI) وتعلم الآلة (ML)، نظرًا لتطور أساليب المحتالين؛ فالابتكار المستمر يعد ضروريًا لمكافحة الاحتيال وضمان أمن الأنظمة المالية.

وفي السياق نفسه ناقشت **دراسة (Hilal et al.، مايو 2022) بعنوان: "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances"** التحديات المرتبطة باكتشاف جرائم الاحتيال المالي (Financial Fraud) في المؤسسات المالية، وقدمت الدراسة مسحًا شاملاً لتقنيات اكتشاف الشذوذ في البيانات (Anomaly Detection Techniques)، مع التركيز على احتيالات بطاقات الائتمان (Credit Card Fraud)، الاحتيال في التأمين (Insurance Fraud)، وغسل الأموال (Money Laundering)، وهدفت الدراسة إلى تحديد عمليات الاحتيال الشائعة في الصناعة المصرفية وكيفية ارتكابها، ومناقشة تأثير الاحتيال على الشركات والأفراد والاقتصادات، ورصد التقنيات المستخدمة في اكتشاف الاحتيال، وتحديد تحديات تلك التقنيات وقياس فاعليتها، وتوصلت الدراسة إلى مجموعة من النتائج ذات الأثر فيما يتعلق بتقنيات الكشف عن الاحتيال المالي (Financial Fraud Detection Technologies)، فقد أوضحت نتائج الدراسة قيام المحتالين بتطوير أساليبهم لاستغلال نقاط الضعف، وهو ما يستلزم أنظمة متقدمة للكشف عن الاحتيال، وفيما يتعلق بأنماط الاحتيال الشائعة، أوضحت الدراسة أن احتيالات الشيكات ومعاملات المقاصة (Checks and ACH Fraud) والمدفوعات الإلكترونية (E-Payments Fraud) يعدان من أكثر أنواع الاحتيالات شيوعًا في المعاملات، كما يحظى اكتشاف الاحتيال في بطاقات الائتمان (Credit Card Fraud)، والاحتيال في التأمين (Insurance Fraud) بأكبر قدر من الاهتمام البحثي، بالتوازي مع ارتفاع معدل الأبحاث المتعلقة بالكشف عن غسل الأموال (Money Laundering) مؤخرًا، في حين ما تزال الأبحاث فيما يتعلق بأنماط الاحتيال الأخرى محدودة، وخاصة الاحتيال في مجالات ومعاملات الرهن العقاري والأوراق المالية والسلع (Mortgage, Securities, and Commodities Fraud)، وفي جانب أساليب الكشف عن الاحتيال، بينت الدراسة أن أبحاث الاحتيال في بطاقات الائتمان (Credit Card Fraud) تعتمد على تحليل الملفات الشخصية (Profile Analysis) وسلوكيات الإنفاق، بينما تهيمن أساليب تحليل المطالبات (Claim Analysis) في مجال التأمين، وبينت الدراسة أنه فيما سبق كانت الأساليب الموجهة، مثل نماذج التعلم الموجه (SVMs) والشبكات العصبية (NNs) وأشجار القرار (DTs)، هي الشائعة والأكثر استخداما على نطاق واسع في كشف الاحتيال، ولكن بدأت الأساليب غير الموجهة، مثل التجميع (Clustering) والغابات المعزولة (Forests Isolation)، تكتسب الاهتمام البحثي مؤخرًا؛ وذلك لمعالجة القيود المفروضة على النماذج الموجهة (Limitations of Supervised Models)، كما أشارت الدراسة إلى أنه لا تزال هناك فجوات في الأدبيات المتعلقة بأنواع الاحتيال الأخرى، والنماذج القابلة للتفسير (Explainable Models)، واكتشاف الاحتيال عبر الإنترنت (Online Fraud Detection).

أما **دراسة (Zhu et al.، أكتوبر 2021) بعنوان: "Intelligent Financial Fraud Detection Practices in Post-Pandemic Era"** فقد قدمت مراجعة شاملة لطرق الكشف عن الاحتيال المالي (Financial Fraud)، مركزة على التحديات التي أفرزها وباء (كوفيد-19 -Covid)، وهدفت الدراسة لتحديد الإستراتيجيات والتقنيات المبتكرة لمواجهة تحديات الاحتيال

المالي فيما بعد الوباء، وتقديم توصيات لتعزيز ممارسات الكشف الذكي عن الاحتيال المالي (Intelligent Financial Fraud)، وأظهرت الدراسة عدة نتائج، من أهمها: أن عقبات دمج البيانات (Integrating Data) من مصادر متعددة ومعالجة كميات كبيرة من المعلومات تظل قائمة مما يؤثر على قدرة الكشف عن الأنشطة الاحتيالية، وتوصلت الدراسة أيضا إلى أن تقنيات الذكاء الاصطناعي (AI) مثل تعلم الآلة (Machine Learning) والنظم القائمة على قاعدة معرفية (Knowledge-based Systems)، والشبكات المعرفية (knowledge Graphs) لديها قدرات كبيرة على دمج (Consolidate) المعلومات حول الكيانات المتورطة في الاحتيال، مما يسهل عملية أتمتة الكشف (Automate Detection Process) عن الاحتيال وتحديد الأنماط المشبوهة، كما أن نظم الذكاء الاصطناعي يمكنها استخدام البيانات المنظمة وغير المنظمة (Structured and Unstructured Data) للكشف عن الحالات الشاذة (Anomalies) وتحليل العلاقات السرية بين الكيانات المرتبطة بالاحتيال، كما أوضحت الدراسة أن هناك حاجة ملحة لنماذج كشف قابلة للتفسير (Interpretability) لمواجهة التحديات المتعلقة بتحيز النموذج (Model Bias)، وقوته (Robustness) وقابلية تفسيره (Interpretability)، ولكن نبهت الدراسة إلى أن عدم توازن الفئات (Class Imbalance) الناتج عن تفوق عدد المحتالين بشكل كبير على عدد المستخدمين العاديين، يؤدي إلى تفاقم مشكلات تحيز النماذج (Model Bias)، وهو ما يستدعي تطوير نماذج غير متحيزة، وختاما أكدت الدراسة على أهمية البحث المستمر في تطوير أنظمة فعالة وموثوقة للكشف عن الاحتيال، مما يمهد الطريق لممارسات أكثر فاعلية ومرونة في المستقبل.

وفي الختام، نستعرض **دراسة (Rouhollahi et al.، مايو 2021) بعنوان: "Towards Artificial Intelligence Enabled Financial Crime Detection"** التي ناقشت الجرائم المالية التي تواجه المؤسسات المصرفية، مع التركيز على التحديات المتزايدة في اكتشاف ومنع هذه الجرائم؛ وذلك بهدف تحسين قدرة المؤسسات على اكتشاف ومنع جرائم الاحتيال المالي (Financial Fraud)، وغسل الأموال (Money Laundering)، وتطوير نموذج جديد لاكتشاف وتوقع جرائم غسل الأموال (Money Laundering) بالحد الأدنى من التدخل البشري، ولتحقيق هذه الأهداف قامت هذه الدراسة بتحليل الأساليب الحديثة في الكشف عن الجرائم المالية، ومنها على سبيل المثال أساليب النماذج القائمة على القواعد (Rule-based Models)، والتجميع (Clustering)، والتصنيف (Classification)، وكذا الكشف عن الشذوذ (Anomaly Detection)، كما ناقشت الدراسة أيضا أهمية تصنيف البيانات (Data Labeling) واستخدام التقنيات الذكية لتسمية مجموعات البيانات الكبيرة (Label Large Datasets).

وطبقا لنتائج الدراسة فقد قدم نموذج الشبكة العصبية المتصلة بالكامل (Fully Connected Neural Network) أعلى مستوى للدقة بين نماذج التصنيف المختلفة، كما حققت طريقة غابة العزل (iForest) أفضل أداء في الكشف عن الحالات الشاذة (Anomaly Detection)، مما يدل على فاعليتهما في هذا المجال، واقترحت الدراسة منهجية تجمع بين التصنيف الموجه (Supervised Classification) والكشف عن الحالات الشاذة غير الموجه (Unsupervised Anomaly Detection)، وهي منهجية تقدم تحسينات كبيرة في دقة النتائج، حيث يمكنها كشف المعاملات المشبوهة بفاعلية مما يقلل الحاجة إلى التدخلات البشرية، كما يمكنها تقليل النتائج الإيجابية الكاذبة (False Positive Results)، وأوصت الدراسة بتوسيع نطاق البحث والتطوير، بما في ذلك دمج خصائص العملاء (Incorporating Customer Features)، وتطوير تقنيات هندسة الخصائص الذكية (Intelligent Feature Engineering Techniques)، وأوصت الدراسة أيضا بتطبيق النمذجة الشبكية (Graph Modeling) وتقنيات التجميع (Clustering Techniques) لتوفير لوحة تحكم ديناميكية (Dynamic Dashboard) للمحللين المصرفيين، كما أوصت الدراسة بضرورة تعزيز الامتثال للمتطلبات التنظيمية وزيادة اليقظة في تحديد المعاملات المشبوهة.

د. مجال الاستفادة من الدراسات السابقة (الدراسات العربية والأجنبية):

أظهرت الدراسات السابقة بشكل عام ثراءً وتنوعًا في الإطار المعرفي والمنهجي ومجتمعات تطبيقها، كما أبرزت هذه الدراسات توجهات الأكاديميين والخبراء المهنيين والممارسين على حد سواء نحو تبني استخدام تطبيقات الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية بشكل عام وتأثيراتها المحتملة وقيود ومحددات استخدامها الحالية ومجالات تطورها المستقبلية، وبقدر ما تكون الدراسات السابقة حجر أساس لما بعدها بما تتوصل إليه من نتائج، بقدر ما تكون هناك بعض الملاحظات وأحيانا الانتقادات من خلال ما تطرحه من توصيات؛ لذلك جاءت الدراسة الحالية مبنية على ما قدمته هذه الدراسات من استنتاجات وما طرحته من توصيات، ومن ثمَّ يتمحور مجال الاستفادة من هذه الدراسات في النقاط التالية:

1. كانت الدراسات السابقة هي نقطة الانطلاق للباحث لبناء خطة أولية لموضوع الدراسة الحالية.
2. تم اعتماد الدراسات السابقة كأساس لتحديد المشكلة البحثية الرئيسية للدراسة الحالية وبلورتها.
3. دعمت الدراسات السابقة بناء نموذج الدراسة الحالية حول رسم علاقة المتغير المستقل بالمتغير التابع واختبار فرضياتها.
4. شكلت الدراسات السابقة قاعدة جيدة للباحث لاقتناء مراجع ومصادر الدراسة الخاصة به.
5. دعمت الدراسات السابقة الإطار النظري للدراسة الحالية حول الذكاء الاصطناعي وتطبيقاته المختلفة، ومخاطر الجرائم المالية بأنماطها المتعددة، وتأثير تطبيقات الذكاء الاصطناعي على إدارة هذه المخاطر في القطاع المصرفي.
6. كانت الدراسات السابقة المرجع المرشد للباحث لصياغة أسئلة الاستبانة.

هـ. نقاط الاتفاق بين الدراسة الحالية والدراسات السابقة:

1. تتفق الدراسة الحالية مع الدراسات السابقة في موضوعها الرئيسي وهدفها العام، وبالنظر أيضا إلى منهجية الدراسة نلاحظ أنها جميعا قد استخدمت المنهج الوصفي.
2. تتفق الدراسة الحالية مع الدراسات السابقة في العديد من الأمور، منها ما هو في جوهر المحتوى العلمي، وخاصة مناقشة تأثير الذكاء الاصطناعي على إدارة مخاطر الجرائم المالية، حيث اتفقت جميعها في الدور الحيوي الذي يلعبه حاليا، والمتوقع مستقبلا، للذكاء الاصطناعي وتطبيقاته المختلفة في إدارة مخاطر هذه الجرائم في القطاع المصرفي، وكشفها ومكافحتها على اختلاف أشكالها وأنماطها والقائمين بها.
3. تتفق الدراسة الحالية مع الدراسات السابقة في تكييف مختلف تطبيقات الذكاء الاصطناعي بما يتلاءم وأنماط وخصائص الجرائم المالية المختلفة في القطاع المصرفي، بدءا من الجرائم المالية التي كان يتم ارتكابها غالبا بالأساليب التقليدية، مثل غسل الأموال، ومرورا بأنماط الاحتيالات التي تختلف وتتنوع باختلاف المنتجات والخدمات المصرفية، ووصولا إلى الجرائم المالية التي يتم ارتكابها بالوسائل الإلكترونية المستحدثة، مثل سرقة الهوية واختراق الحسابات المصرفية، الخ.
4. تتفق الدراسة الحالية مع الدراسات السابقة في وصولها جميعا إلى إجابة نهائية عن مشكلة الدراسة وإشكاليتها، بحيث انعكست مفاهيم المتغيرات على الواقع الفعلي للمؤسسات التي أسقطت عليها ما درسته نظريًا.

و. نقاط الاختلاف بين الدراسة الحالية والدراسات السابقة:

1. تختلف هذه الدراسة عن الدراسات السابقة في أن كل دراسة من الدراسات السابقة قد عالجت بشكل جزئي فقط أبعاد متغيريْ الدراسة المتمثلين في: "الذكاء الاصطناعي" كمتغير مستقل، و"إدارة مخاطر الجريمة المالية" كمتغير تابع، فمن ناحية ركزت كل دراسة من هذه الدراسات على استعراض عدد محدود - كان أحيانا تطبيقا واحدا فقط - من تطبيقات الذكاء الاصطناعي، ومن ثم اختبار تأثير هذه التطبيقات أيضا على بُعد واحد فقط من أبعاد إدارة مخاطر الجرائم المالية، وهو بُعد تحديد خطر الجرائم المالية من خلال كشف وجود هذا الخطر، كما أن الدراسات السابقة - من ناحية أخرى - في أثناء قيامها بذلك، ركزت فقط إما على نمط واحد فقط أو عدد محدود من أنماط الجرائم المالية، دون التطرق لبحث ومناقشة تأثير هذه التطبيقات على باقي أبعاد أو مراحل عملية إدارة المخاطر ذاتها.
2. تختلف هذه الدراسة عن الدراسات السابقة أيضا في مكان إجراء الدراسة الميدانية، حيث إنها من الدراسات القليلة التي تم إجراؤها في دولة عربية، علاوة على كونها الدراسة الأولى التي يتم إجراؤها في دولة قطر في هذا المجال، بما للدول العربية عامة ولدولة قطر تحديدا، من طبيعة خاصة تنبع من الخصائص الجغرافية والاقتصادية والاجتماعية والديموغرافية لبيئة الدراسة الميدانية فيها،

كما أن معظم الدراسات السابقة في هذا المجال - في حدود اطلاع الباحث - قد أجريت الدراسة الميدانية فيها خارج المنطقة العربية، ومنها على سبيل المثال **دراسة (بن علي، ديسمبر 2023)** والتي أجريت الدراسة الميدانية فيها في القطاع المصرفي الدنماركي بالتطبيق على بنك **(Danske)**، وركزت فقط على مخاطر الأمن السيبراني.

ز. ما يميز الدراسة الحالية عن الدراسات السابقة:

1. تتميز هذه الدراسة بتناولها بشكل أشمل العلاقة المباشرة بين الذكاء الاصطناعي وأبعاده وتطبيقاته المختلفة كمتغير مستقل، على الأبعاد المختلفة لعملية إدارة مخاطر الجرائم المالية المختلفة كمتغير تابع، ومدى تأثير الذكاء الاصطناعي وأبعاده وتطبيقاته على عملية إدارة هذه المخاطر في القطاع المصرفي، وذلك على عكس معظم الدراسات السابقة التي تناولت تأثير أحد تطبيقات أو مجموعة محدودة من تطبيقات الذكاء الاصطناعي على واحدة أو مجموعة محدودة فقط من الجرائم المالية فقط، دون التطرق لبحث ومناقشة تأثير هذه التطبيقات على باقي أبعاد أو مراحل عملية إدارة المخاطر ذاتها.
2. كما تتميز هذه الدراسة بأنه سيتم تطبيق الدراسة الميدانية لها في بيئة جغرافية وعملية مختلفة، لم يتم إجراء مثل هذه الدراسة فيها من قبل، مما يتيح لنا الكشف عن جوانب غير مسبوقة عن تأثير تطبيق تقنيات الذكاء الاصطناعي على إدارة مخاطر الجرائم المالية في القطاع المصرفي في هذه البيئة، وأيضا التعرف على التحديات التي تواجه تطبيق الذكاء الاصطناعي في هذا المجال.
3. وأيضا تتميز هذه الدراسة بأن نتائجها وتوصياتها ستكون مرجعا لمنظمات الأعمال المصرفية العربية التي ترغب في تحديث وتعزيز عملية إدارة مخاطر الجرائم المالية في ظل التغيرات العلمية والتكنولوجية السريعة من خلال استخدام تطبيقات الذكاء الاصطناعي؛ كونها الدراسة الأولى من نوعها التي تتم في هذا المجال في بيئة العمل الجغرافية نفسها التي تنتمي إليها هذه المنظمات.

2. الفجوة البحثية:

في حدود اطلاع الباحث على الدراسات والمجهودات البحثية السابقة في موضوع الدراسة نفسه، توصل الباحث إلى قلة الدراسات الأجنبية أو العربية التي تجمع بشكل شامل بين كافة أبعاد كل من "**الذكاء الاصطناعي" كمتغير مستقل**، و"**إدارة مخاطر الجريمة المالية**" كمتغير تابع؛ إذ تركزت معظم الدراسات السابقة على دراسة إما بُعد واحد فقط من أبعاد المتغير المستقل "**الذكاء الاصطناعي**" أو عدد محدود من أبعاده، واستكشاف تأثير هذا البُعد أو هذه الأبعاد المحدودة على بُعد واحد فقط من أبعاد المتغير التابع "**إدارة مخاطر الجريمة المالية**"، ألا وهو بُعد "**تحديد الخطر**"، والمتمثل عمليا في تحديد وكشف الجريمة المالية فقط، دون التطرق إلى مناقشة **تأثير الذكاء الاصطناعي وتطبيقاته المختلفة على كافة أبعاد ومراحل عملية إدارة مخاطر الجريمة المالية**، وبالإضافة إلى ذلك فإن الدراسات العربية في هذا المجال قليلة إن لم تكن نادرة، وهو ما دفع الباحث لتبني موضوع الدراسة للإسهام في سد الفجوة البحثية، وتعزيز المعرفة في هذا المجال.

ثالثا: متغيرات و فروض الدراسة:

1. المتغير المستقل: الذكاء الاصطناعي:

قام الباحث باعتماد الأبعاد التالية (**النظم الخبيرة، تعلم الآلة، التعلم العميق، الذكاء الاصطناعي التوليدي، معالجة اللغات الطبيعية، رؤية الحاسب، و أتمتة العمليات الروبوتية**) كأبعاد للمتغير المستقل (**الذكاء الاصطناعي**)، وذلك بناء على الدراسات السابقة، كما هو موضح بالجدول رقم (1) أدناه:

جدول رقم (1) أبعاد المتغير المستقل (الذكاء الاصطناعي)

الدراسات السابقة	النظم الخبيرة	تعلم الآلة	التعلم العميق	الذكاء الاصطناعي التوليدي	اللغات الطبيعية	رؤية الحاسب	أتمتة العمليات الروبوتية
دراسة (Ahmadi، 2024)	✓	✓	✓	✓	✓	✓	✓
دراسة (بن علي، 2023)	✓	✓	✓	X	✓	X	✓
دراسة (الأسد، 2023)	✓	✓	✓	X	✓	✓	✓

دراسة (Mytnyk et al.، 2023)	X	✓	✓	X	X	X	X
دراسة (Zador et al.، 2023)	X	✓	✓	✓	✓	✓	✓
دراسة (Blanco & Garrido، 2022)	✓	✓	✓	✓	✓	✓	X
دراسة (Birhane، 2022)	✓	✓	✓	✓	✓	✓	X
دراسة (Aggarwal et al.، 2022)	X	✓	✓	✓	✓	✓	X
دراسة (Zhu et al.، 2021)	✓	✓	✓	X	✓	✓	X
دراسة (Rouhollahi et al.، 2021)	✓	✓	✓	X	✓	X	✓
المجموع	7	10	10	5	9	7	5
نسبة التكرار	%70	%100	%100	%50	%90	%70	%50

المصدر: من إعداد الباحث بالاعتماد على دراسات سابقة

2. المتغير التابع: إدارة مخاطر الجريمة المالية:

اعتمد الباحث الأبعاد التالية (**تحديد المخاطر، تحليل وتقييم مستوى المخاطر، معالجة المخاطر، مر اقبة ومراجعة المخاطر**) كأبعاد للمتغير التابع (**إدارة مخاطر الجريمة المالية**)، وذلك بناء على الدراسات السابقة، كما هو موضح بالجدول رقم (2) أدناه:

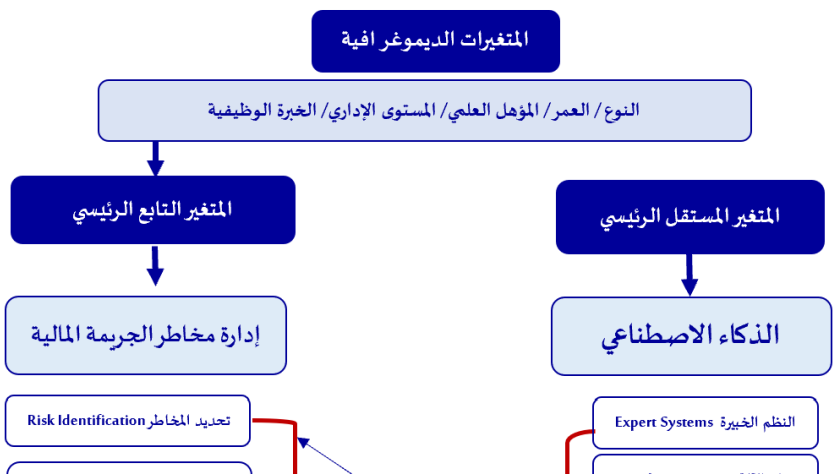
جدول رقم (2) أبعاد المتغير التابع (إدارة مخاطر الجريمة المالية)

الدراسات السابقة	تحديد المخاطر	تحليل وتقييم مستوى المخاطر	معالجة المخاطر	مر اقبة ومراجعة المخاطر
دراسة (Kasztelnik، 2023)	✓	✓	✓	✓
دراسة (Afjal et al.، 2023)	✓	✓	✓	✓
دراسة (KASIE & AKUJINMA، 2022)	✓	✓	✓	✓
دراسة (Mahony، 2022)	✓	✓	✓	✓
دراسة (Pradesyah et al.، 2021)	✓	✓	✓	✓
دراسة (Muminovic، 2021)	✓	✓	✓	✓
دراسة (Gao et al.، 2023)	✓	✓	✓	✓
دراسة (Nyakarimi et al.، 2020)	✓	✓	✓	✓
المجموع	8	8	8	8
نسبة التكرار	%100	%100	%100	%100

المصدر: من إعداد الباحث بالاعتماد على الدراسات السابقة

3. نموذج متغيرات الدراسة:

في ضوء مراجعة الدراسات السابقة، واعتمادًا على المرجعيات ذات العلاقة، تم بناء نموذج الدراسة الذي يوضح العلاقة بين متغيرات الدراسة، والذي يحتوي على **المتغير المستقل** (**الذكاء الاصطناعي**) و**المتغير التابع** (**إدارة مخاطر الجريمة المالية**)، كما هو موضح في **الشكل رقم (3)**:



شكل رقم (1): نموذج متغيرات الدراسية

المصدر: من إعداد الباحث بالاعتماد على الدراسات السابقة

4. فروض الدراسة:

أ. **الفرضية الرئيسية:** في ضوء نموذج متغيرات الدراسة، يمكن صياغة الفرضية الرئيسية للدراسة كما يلي:

"يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري".

ب. **الفرضيات الفرعية:** يتفرع من هذه الفرضية الرئيسية الفرضيات الفرعية التالية:

1. **يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.**
2. **يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.**
3. **يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في معالجة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.**
4. **يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.**

رابعا: أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

الهدف الرئيسي:

التعرف على درجة تأثير استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي القطري.

الأهداف الفرعية:

1. التعرّف على درجة تأثير استخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية من خلال استقصاء قدرة الأنظمة الذكية على الكشف المبكر عن الأنماط والسلوكيات المشبوهة.
2. التعرّف على درجة تأثير استخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية من خلال استقصاء دقة نماذج التحليل والتنبؤ وتصنيف المخاطر الناتجة عن تقنيات الذكاء الاصطناعي.
3. التعرّف على درجة تأثير استخدام الذكاء الاصطناعي في معالجة مخاطر الجريمة المالية من خلال استقصاء كفاءة وسرعة استجابة الأنظمة الذكية في اتخاذ إجراءات الحد من المخاطر وتقليل الأخطاء البشرية.

4. التعرّف على درجة تأثير استخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية من خلال استقصاء قدرة الأنظمة الذكية على الرقابة المستمرة، وإصدار تقارير المراقبة والمراجعة الدورية.
5. تقديم نتائج وتوصيات الدراسة المتعلقة بتأثير الذكاء الاصطناعي و أنظمته و تقنياته المتنوعة على إدارة مخاطر الجريمة المالية، بما يتيح للباحثين والعاملين بالقطاع المصرفي القطري والعربي الاطلاع عليها و الاستفادة منها، سواء ارتبطت هذه التوصيات بالجوانب التنظيمية أو التشغيلية أو التقنية.

خامسا: أهمية الدراسة

تكمن أهمية الدراسة الحالية في أهمية موضوعها الرئيسي، والمتمثل **في تأثير الذكاء الاصطناعي على إدارة مخاطر الجريمة المالية وخاصة في مؤسسات القطاع المصرفي**، حيث تُعدّ ظاهرة الجرائم المالية عامة، والجرائم المالية في مؤسسات القطاع المصرفي على وجه الخصوص، من الظواهر شديدة الضرر على الدول ومؤسسات القطاع المصرفي وأطراف العلاقة بها على حد سواء، وهذه الجرائم تزايدت خطورتها مؤخرا في ظل ظروف الجائحة الصحية لفيروس كورونا (كوفيد -19) والتي أدت لتزايد الاعتماد على إجراء المعاملات والعمليات في القطاع المصرفي عن بُعد (Online) وباستخدام وسائل تقنية، وهو ما ضاعف من معدلات ارتكاب هذه الجرائم وحجم الخسائر الناتجة عنها على حد سواء، ومن ثم تتجلى أهمية هذه الدراسة في محاولة إيجاد حلول مبتكرة لإدارة مخاطر هذه الجرائم المالية، ويمكن تلخيص أهمية الدراسة في **المحاور الثلاثة الآتية**:

أ-الأهمية العلمية للدراسة:

1. تسهم هذه الدراسة في توضيح أهمية الذكاء الاصطناعي في تحقيق تحولات جوهرية في القطاع المصرفي بصفة خاصة، وفي جميع مجالات الأعمال والحياة بصفه عامة.
2. تسهم هذه الدراسة في علاج الفجوة البحثية وسد الفراغ المعرفي الناتج عن قلة الدراسات التي تناولت العلاقة بين الذكاء الاصطناعي وتأثيره علي إدارة مخاطر الجريمة المالية في القطاع المصرفي، وهي الفجوة الناتجة عن حداثة موضوع الذكاء الاصطناعي وعلاقته بإدارة مخاطر الجريمة المالية من جانب، و قلة المراجع العربية التي تناولت هذا الموضوع عامة، أو التي ربطت ما بين المتغيرين وتناولت العلاقة بينهما بشكل واف وشامل من جانب آخر، ومن ثمَّ ستمثل هذه الدراسة إضافة علمية جديدة لحقل مكافحة الجرائم المالية وإدارة المخاطر المرتبطة بها لسد جزء من الفجوة في هذا الجانب، وإثراء المكتبة المالية والاقتصادية من خلال الربط بين تطبيقات وتقنيات الذكاء الاصطناعي وإدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي العربي عامة والقطري خاصة.
3. تأتي هذه الدراسة استجابة لمتطلبات المستقبل في التوسع في استخدام الذكاء الاصطناعي وتطبيقاته في جميع مجالات الأعمال والحياة، ومنها مجال إدارة مخاطر الجريمة المالية بشكل عام، وإدارة مخاطر هذه الجريمة في القطاع المصرفي بشكل خاص، خاصة مع تزايد الاهتمام بتقنيات الذكاء الاصطناعي كأحد التقنيات الحديثة في هذا المجال، وأهمية أن تواكب المؤسسات العاملة في القطاع المصرفي العربي التطورات الحديثة والمتمثلة في تقنيات الذكاء الاصطناعي، ومحاولة الاستفادة منها بأكبر قدر ممكن في إدارة مخاطر الجريمة المالية.
4. تحاول الدراسة توجيه أنظار الباحثين للاهتمام بالبحث في مجال تطبيقات الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية، كما يمكن الاستفادة من أدواتها ونتائجها وتوصياتها في إجراء دراسات وبحوث أخرى تتكامل مع نتائج الدراسة الحالية.

ب- الأهمية العملية الدراسة:

1. يمس هذا الموضوع قطاعًا مهمًا وحيويًا في اقتصاد أي دولة، ألا وهو القطاع المصرفي، والذي يُعدّ القلب النابض للنظام المالي للدولة، والمسئول الأول عن توفير رؤوس الأموال لاقتصادها الوطني، ومن ثمَّ فمن الأهمية ضرورة مسايرة التحولات التكنولوجية الرقمية من أجل تعزيز كفاءة هذا القطاع بشكل عام، وحماية أصوله وموجوداته ومؤسساته وأطراف العلاقة فيه من الجرائم المالية التي قد ترتكب ضدهم، ومن ثمَّ زيادة تأمين هذا القطاع والمؤسسات العاملة فيه، وعملياتها ومعاملاتها، وتعظيم ربحيتها وتقليل خسائرها، والحد مما تتعرض له من مخاطر أخرى مختلفة ومتنوعة ناتجة عن مخاطر الجريمة المالية، مثل مخاطر السمعة، ومخاطر التركز، والمخاطر القانونية والتنظيمية، وغيرها.

2. تساعد هذه الدراسة على جذب انتباه منظمات الأعمال عامة، والمؤسسات المصرفية خاصة، ومسئولي إدارة المخاطر ومكافحي الجريمة المالية بها إلى الاستفادة من المميزات التي تقدمها تقنيات و أنظمة الذكاء الاصطناعي في تعزيز وتقوية ممارستها في مجال إدارة مخاطر الجريمة المالية، من حيث السرعة والدقة والقدرة التخزينية للبيانات والمعلومات، ومعالجة الكم الهائل من المعلومات والبيانات أولاً، ومدى كفاءة وفاعلية هذه التقنيات في هذا المجال ثانيًا، ومن ثمَّ تساعد هذه الأنظمة والتقنيات مؤسسات القطاع المصرفي ومسئولي إدارة المخاطر ومكافحي الجريمة المالية بها على تخطي الكثير من المعوقات والضغوطات المختلفة التي تحيط بعملية إدارة مخاطر الجريمة المالية، وتتيح لهم استخدام هذه الأنظمة والتقنيات في بيئة الأعمال المصرفية المعاصرة، والتي أصبحت تتضمن تفاصيل كثيرة تتسم بالتعقيد وتحتاج إلى تركيز عقلي وحضور ذهني متواصل، وقرارات حساسة وسريعة لا تحتمل التأخير أو الخطأ، وما يترتب على ذلك من تحقيق عوائد مرضية ومكانة سوقية عالية وميزة تنافسية كبيرة، ويمهد لرفع مستوى هذه المؤسسات المصرفية بما يتيح لها دخول حيز المنافسة العالمية.

3. يأمل الباحث أن يكون للدراسة الحالية دور كبير في زيادة فاعلية وكفاءة عملية إدارة مخاطر الجريمة المالية بالقطاع المصرفي العربي والعالمي ومخرجات هذه العملية، ويأمل كذلك أن يتم ذلك من خلال التعرف على الدور الذي يلعبه الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي، وتوضيح متطلبات استخدام تقنيات الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية، وكذا مناقشة المعوقات أو المشكلات المحتملة التي قد تحد من قدرة المؤسسات المصرفية على استخدام تقنيات الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية، خاصة بعد تنوع أنماط هذه الجريمة والزيادة الكبيرة في معدل ارتكابها في العقد الأخير. كما يأمل الباحث - في هذا السياق - أن توفر هذه الدراسة وبياناتها وأدواتها والنتائج والتوصيات التي خلصت إليها قاعدة معرفية ودليل عملي للمؤسسات المصرفية، ومكافحي الجريمة المالية فيها حول تحقيق الاستخدام الأمثل لتقنيات الذكاء الاصطناعي وتعظيم الاستفادة منها في إدارة مخاطر الجريمة المالية ومكافحة هذه الجرائم.

4. تحاول الدراسة جذب انتباه المشرعين وهيئات الإشراف والرقابة إلى أهميَّة وضرورة صياغة أطر تشريعية وقواعد تنظيمية توجه وتحكم عملية تبني واستخدام الذكاء الاصطناعي وتطبيقاته في إدارة مخاطر الجريمة المالية بالقطاع المصرفي؛ ذلك أن التحول من أنظمة إدارة مخاطر الجريمة المالية القائمة على استخدام القواعد التقليدية والبشر إلى أنظمة قائمة على استخدام الذكاء الاصطناعي، يحتم على المشرعين وهيئات الرقابة التنظيمية، ليس فقط تبني مبادئ حوكمة الذكاء الاصطناعي الناشئة حديثًا، بل أيضًا ضرورة وضع أطر تشريعية وتنظيمية متوازنة ومنسجمة تصاحب هذا التحول غير المسبوق.

ت- أهمية الدراسة للباحث:

1. تنبع أهمية هذه الدراسة للباحث من ارتباطها بواقع عملي متقدم تشهده دولة قطر – حيث تم اجراء الدراسة الميدانية - في المجالين المصرفي والتقني، حيث حققت المؤسسات المصرفية القطرية تقدمًا ملحوظًا في تبني الحلول الرقمية والذكاء الاصطناعي ضمن **رؤية قطر الوطنية 2030**. وبناءً على ذلك، تسهم هذه الدراسة في دعم هذا التوجه من خلال توضيح كيفية توظيف الذكاء الاصطناعي بكفاءة في إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي القطري، بما يعزز قوة المنظومة الرقابية ويكرّس مكانة دولة قطر كمركز مالي متطور وموثوق إقليميًا ودوليًا.

سادسا: منهجية الدراسة وإجراءاتها:

في سبيل تحقيق أهداف الدراسة وتقييم فرضياتها، تم تصميم منهجية لضمان أعلى مستويات الدقة والموثوقية ، وذلك على النحو التالي:

1. **منهجية الدراسة المعتمدة (Adopted Methodology)**:

اعتمدت الدراسة على **المنهج الوصفي التحليلي Descriptive-Analytical Approach**، وهو المنهج الأمثل للتعمق في دراسة العلاقة السببية بين متغيرات البحث. وقد تم تطبيق هذا المنهج عبر **دراسة ميدانية (Field Study)** شاملة في بيئة القطاع المصرفي القطري، بهدف:

أ. **التحليل التشخيصي**: وصف واقع تطبيق تقنيات الذكاء الاصطناعي في المؤسسات المصرفية محل الدراسة.

ب. **التحليل التفسيري**: تقييم وتحليل مدى تأثير استخدام هذه التقنيات على الأبعاد المختلفة لعملية إدارة مخاطر الجريمة المالية (التحديد، التحليل والتقييم، المعالجة، والمتابعة والمراجعة).

ج. **الاستنتاج القائم على البيانات:** استخلاص نتائج مدعومة إحصائياً حول فاعلية الذكاء الاصطناعي في تعزيز كفاءة الأنظمة الرقابية.

2. **الأهداف الإجرائية للدراسة الميدانية (Operational Objectives of the Field Study) :**

تجاوزت الأهداف الإجرائية للدراسة الميدانية في دولة قطر مجرد القياس الكمي لتشمل أبعاداً استراتيجية وتطبيقية، أهمها:

أ. **تحديد الأثر الوظيفي:** تحديد وتأكيد الأثر المباشر لاستخدام الذكاء الاصطناعي في الكشف المبكر عن الأنماط غير الاعتيادية (Anomaly Detection) في العمليات المصرفية.

ب. **تعزيز القدرات الاستباقية:** تقييم مدى مساهمة الذكاء الاصطناعي في تطوير القدرات التنبؤية (Predictive Capabilities) لمخاطر الجرائم المالية المحتملة.

ج. **التطوير الاستراتيجي:** تقديم مجموعة من التوصيات والمقترحات العملية التي تُسهم في صياغة استراتيجيات أكثر كفاءة ومرونة لإدارة مخاطر الجرائم المالية، بما يضمن الالتزام بمتطلبات الامتثال التنظيمي.

3. **مصادر البيانات واستراتيجية جمعها (Data Sources and Acquisition Strategy) :**

تم تطبيق استراتيجية متكاملة لجمع البيانات، شملت مسارين رئيسيين:

أ. **البيانات الثانوية Secondary Data** : في إطار معالجة الإطار النظري للدراسة، اعتمد الباحث على مراجعة نقدية معمقة للإطار النظري (Theoretical Framework) والدراسات السابقة، من خلال الرجوع إلى الكتب والمراجع العربية والأجنبية ذات العلاقة، والدوريات والمقالات والتقارير، والأبحاث والدراسات السابقة التي تناولت موضوع الدارسة، وعلى البحث والمطالعة في مواقع الإنترنت المختلفة، بالإضافة إلى البيانات والمعلومات ذات الصلة بموضوع الدراسة من خلال النشرات والإحصائيات والتقارير الصادرة عن الجهات المختصة الدولية والإقليمية والمحلية المنشورة في الفترة من يناير **2020** إلى مايو **2025**.

ب. **البيانات الأولية (Primary Data) :** تم جمعها ميدانياً من خلال استخدام استمارة استبانة (Structured Questionnaire) تم تصميمها خصيصا لقياس متغيرات الدراسة، حيث تم توزيعها على عينة على أفراد العينة العشوائية لجمع بيانات نوعية وكمية عن الخبرات والتطبيقات الفعلية.

4. **مجتمع وعينة الدراسة (Study Population and Sample):**

يضم **مجتمع الدراسة (Study Population)** العاملين في الإدارات المحورية المسؤولة عن إدارة المخاطر والالتزام في المؤسسات المصرفية القطرية الخاضعة لرقابة مصرف قطر المركزي. وقد تم التركيز على الإدارات ذات الصلة المباشرة بالموضوع وهي: إدارة الامتثال/الالتزام، إدارة المخاطر، إدارة مكافحة الجرائم المالية، وإدارة التدقيق الداخلي و إدارة الأمن السيبراني.

وفيما يتعلق **بعينة الدراسة (Study Sample)** و دراسة مفرداتها، و نظرا لكبر عدد العاملين في هذا القطاع محل الدراسة والذي يقدر بحوالي **(1017)** موظفًا تقريبًا، فقد تم اختيار عينة عشوائية **(Random Sample)** من مجتمع الدراسة لضمان تمثيل إحصائي موضوعي وآراء متنوعة تغطي الخبرات المختلفة داخل هذا القطاع.

5. **طرق وأساليب جمع البيانات و التحليل الاحصائي (Methods and Techniques of Data Collection Statistical Analysis)**

قام الباحث بإعداد استمارة استبانة تم توجيهها من خلال طرح مجموعة من أسئلة الاختيار من متعدد، كما استخدم الباحث في تصميمه لاستمارة الاستبانة "**مقياس ليكرت الخماسي / Five-Point Likert Scale**" وذلك لما يوفره هذا المقياس من نتائج قابلة للتحليل الإحصائي، وقدرته على قياس درجة اتفاق أو اختلاف المبحوثين مع العبارات المطروحة، مما يتيح التعرف بشكل كمي على مستوى تأثير استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي، وكذلك مقارنة وجهات نظر المبحوثين واستخلاص استنتاجات علمية مبنية على بيانات موضوعية. ولتحقيق الدقة في اختبار الفرضيات، تم استخدام حزمة متقدمة من الأساليب الإحصائية كان أبرزها **تحليل الوصف الإحصائي** من خلال **حساب المتوسطات الحسابية** (Means) والانحرافات المعيارية (Standard Deviations) لوصف اتجاهات الاستجابات.

سابعا: حدود الدراسة:

تُعدّ حدود الدراسة الإطار العملي الذي تتم من خلاله معالجة موضوع الدراسة والتحليل الجيد والواقعي له، وتتمثل حدود هذه الدراسة فيما يلي:

1. الحدود الموضوعية:

تقتصر هذه الدراسة على دراسة تقنيات وتطبيقات الذكاء الاصطناعي المختلفة، وبيان مدى تأثيرها على إدارة مخاطر الجريمة المالية بما يشمل كلا من جريمة غسل الأموال، جريمة تمويل الإرهاب، جريمة تمويل انتشار أسلحة الدمار الشامل، جريمة خرق قرارات العقوبات أو الجزاءات المالية المستهدفة، جرائم الاحتيال المالي بأنماطها المختلفة ومنها الفساد، و اختلاس الأصول و الاحتيال في البيانات المالية والجرائم الالكترونية أو السيبرانية وما يندرج تحت كل نمط من جرائم فرعية أخرى، وذلك عبر الأبعاد المختلفة لإدارة محاطر الجريمة المالية و المتمثلة في: تحديد المخاطر، وتحليل وتقييم المخاطر، ومعالجة المخاطر، مراقبة ومراجعة المخاطر، مع الاعتماد على الأساليب الإحصائية الملائمة التي تسهم في تحقيق أغراضها التحليلية.

2. الحدود المكانية:

تقتصر هذه الدراسة على مؤسسات القطاع المصرفي القطري الخاضعة لإشراف مصرف قطر المركزي فقط، **وعددها ستة عشر (16) بنكًا ومصرفًا**، تشمل **أربعة (4) مصارف إسلامية و اثني عشر (12) بنكًا تجاريًا تقليديًا**. ويعود اختيار هذه الفئة إلى أن المؤسسات المصرفية القطرية الخاضعة لإشراف المصرف المركزي قد حققت تقدمًا ملموسًا في تبني الحلول الرقمية وتقنيات الذكاء الاصطناعي في إطار دعم تنفيذ **رؤية قطر الوطنية 2030**. كما تزامن ذلك مع **قيام مصرف قطر المركزي** في عام **2024** بإصدار **إرشادات تنظيم استخدام الذكاء الاصطناعي في القطاع المالي**، اتساقًا مع **الاستراتيجية الثالثة للقطاع المالي (2024 – 2030) الصادرة عن مصرف قطر المركزي**، وتبني **الاستراتيجية الوطنية للتكنولوجيا المالية في دولة قطر (2023 – 2027)**.

3. الحدود الزمنية:

تم إجراء الدراسة وفق الحدود الزمنية التالية:

أ. دراسة مصادر البيانات الثانوية المنشورة في الفترة من 1 يناير **2020** إلى **31** مايو **2025**.

ب. الدراسة الميدانية والبيانات الأولية في الفترة من **1 يناير 2024** إلى **31 مايو 2025**.

4. الحدود البشرية:

تقتصر الحدود البشرية للدراسة على عينة عشوائية لمجموعة من العاملين في الإدارات والوظائف ذات الصلة بموضوع الدراسة في مؤسسات القطاع المصرفي القطري الخاضعة لإشراف مصرف قطر المركزي، والمكونة لمجتمع الدراسة وحجمه **1017 مفردة** تقريبًا كما تم توضيحه مسبقا، وقد تم توزيع عدد **278** استمارة استبانة وتم الحصول علي **270** استمارة صالحة للتحليل أي بنسبة استجابة **97%**.

ثامنا: خطة الدراسة:

تم تقسيم الدراسة إلى **أربعة (4) فصول**، كالتالي:

1. الفصل الأول: الإطار العام للدراسة:

يشتمل هذا الفصل على مقدمة عامة عن الدراسة، ومشكلة الدراسة، و الدراسات السابقة، و متغيرات وفروض الدراسة، و أهداف الدراسة، و أهمية الدراسة، ومنهجية الدراسة وإجراءاتها، و حدود الدراسة، وأخيرًا خطة الدراسة.

2. الفصل الثاني: الإطار النظري للدراسة:

ويشمل هذا الفصل على **أربعة (4) أجزاء**، كالتالي:

أ. الجزء الأول: الإطار النظري للذكاء الاصطناعي وتطبيقاته:

يتضمن هذا الجزء إلقاء الضوء - بشكل موجز - على بعض الجوانب ذات الصلة بالذكاء الاصطناعي، ومنها مفهوم الذكاء الاصطناعي، تاريخ الذكاء الاصطناعي، أنواع الذكاء الاصطناعي، إمكانات الذكاء الاصطناعي، العوامل الدافعة لاعتماد الذكاء الاصطناعي، مفردات ومكونات الذكاء الاصطناعي، فوائد وتحديات وسلبيات الذكاء الاصطناعي، مستقبل الذكاء الاصطناعي، وأهم أدوار الذكاء الاصطناعي ومجالات توظيفه في القطاع المصرفية وأنشطته ومعاملاته.

ب. الجزء الثاني: مخاطر الجريمة المالية وتداعياتها على مؤسسات القطاع المصرفي:

يتضمن هذا الجزء استعراضًا سريعًا لمفهوم وأنواع المخاطر في القطاع المصرفي، وتعريف الجريمة المالية في القطاع المصرفي، وتعريف مخاطر الجريمة المالية في القطاع المصرفي، وأنواع وأنماط الجريمة المالية في القطاع المصرفي، وتأثير مخاطر الجريمة المالية على أداء المصارف والاستقرار المالي، والإطار التنظيمي والقانوني لإدارة مخاطر الجريمة المالية في القطاع المصرفي، وخطوات ومراحل إدارة مخاطر الجريمة المالية في القطاع المصرفي، وإستراتيجيات إدارة مخاطر الجريمة المالية.

ج. الجزء الثالث: دور الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في القطاع المصرفي:

يتناول هذا الجزء مناقشة كيف يمكن للذكاء الاصطناعي مساعدة مؤسسات القطاع المصرفي على إدارة مخاطر الجريمة المالية، من خلال استعراض أهم نماذج هذه التطبيقات المستخدمة في الواقع العملي، وخصائص كل منها، ومجالات تميز كل منها عن الطرق التقليدية المستخدمة حاليا في إدارة مخاطر الجريمة المالية، وكذا الصعوبات أو التحديات المختلفة التي تواجه تبني واستخدام هذه التطبيقات والتقنيات في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي.

د. الجزء الرابع: القطاع المصرفي القطري وجهود التحول الرقمي وتبني التكنولوجيا المالية والذكاء الاصطناعي فيه:

يقدم هذا الجزء استعراضًا عامًا للقطاع المصرفي القطري وتطوره عبر المراحل التاريخية المختلفة، والإطار التنظيمي والإشرافي للقطاع المصرفي القطري، وهيكل القطاع المصرفي في دولة قطر، وإسهام القطاع المصرفي القطري في التنمية الوطنية وتحقيق رؤية قطر **2030**، والأداء المالي للقطاع المصرفي القطري، والاتجاهات الحديثة في القطاع المصرفي القطري، وجهود التحول الرقمي والتكنولوجيا المالية في القطاع المصرفي القطري، ودور مصرف قطر المركزي في تعزيز نمو التكنولوجيا المالية في القطاع المصرفي القطري.

3. الفصل الثالث: منهجية الدراسة وإجراءاتها:

يتناول هذا الفصل المنهجية العلمية والإجرائية التي استندت إليها الدراسة في مراحلها المختلفة، ابتداءً من تحديد الإطار المنهجي ووصولاً إلى عرض النتائج الميدانية واختبار الفروض. ويستعرض الفصل في محوره الأول الهدف من الدراسة، والمنهج البحثي المُعتمد، ومصادر بيانات الدراسة، إضافةً إلى تحديد مجتمع البحث وعينته، وشرح خصائص أداة جمع البيانات وطرق التحقق من صلاحيتها. أما المحور الثاني فيركّز على عرض البيانات الميدانية لعينة الدراسة وتحليلها باستخدام الأساليب الإحصائية الملائمة، مع تقديم تحليل تفصيلي لمتغيرات الدراسة الرئيسة. وفي المحور الثالث، يتم فحص التوزيع الطبيعي للمتغيرات وإجراء الاختبارات الإحصائية اللازمة للتحقق من فروض الدراسة.

4. الفصل الرابع: نتائج وتوصيات الدراسة:

يتضمن هذا الفصل ملخصا لنتائج الدراسة، و تحليل نتائج الدراسة لاستخلاص الدلالات العلمية والعملية لهذه النتائج، كما يحتوي على أهم المحددات أو الصعوبات التي واجهها الباحث في أثناء الدراسة، بالإضافة إلى تقديم مجموعة من التوصيات المتعلقة بالدراسة، ويختتم هذا الفصل بعدد من الدراسات المستقبلية المقترحة في مجال الدراسة نفسها.

5. قائمة المراجع والمصادر.

6. ملاحق الدراسة.

الفصل الثاني

الإطار النظري للدراسة

- مقدمة
- الإطار النظري للذكاء الاصطناعي وتطبيقاته
- إدارة مخاطر الجريمة المالية وتداعياتها في القطاع المصرفي
- دور الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي
- القطاع المصرفي القطري وجهود التحول الرقمي وتبني التكنولوجيا المالية والذكاء الاصطناعي فيه
- المفاهيم الأساسية للدراسة

الفصل الثاني
الإطار النظري للدراسة
أولاً: الإطار النظري للذكاء الاصطناعي

مقدمة:

في العقد الأخير أصبح الذكاء الاصطناعي (Artificial Intelligence - AI) أحد أبرز المجالات التي تثير اهتمام الباحثين والمطورين وصناع القرار في جميع أنحاء العالم، ويُعرف الذكاء الاصطناعي بأنه: "**قدرة الأنظمة الحاسوبية على أداء مهام تتطلب عادةً ذكاء بشريًا، مثل الفهم والتعلم، والتفكير النقدي، والتفاعل مع البيئة**"، ويتضمن هذا المجال مجموعة واسعة من التقنيات، بما في ذلك تعلم الآلة Machine Learning، ومعالجة اللغة الطبيعية Natural Language Processing، والرؤية الحاسوبية Computer Vision، والشبكات العصبية Neural Networks (Arsenyan & Piepenbrink, 2023; Stryker & Kavlakoglu, 2024).

ويعود التاريخ الفعلي لنشأة الذكاء الاصطناعي (AI) إلى بدايات القرن العشرين، عندما بدأ العلماء في محاولة محاكاة القدرات العقلية للإنسان، ومنذ ذلك الحين شهد هذا المجال تطورات هائلة، بداية من الأنظمة البسيطة التي تعتمد على القواعد الثابتة، وصولا إلى الأنظمة المتقدمة التي تستخدم خوارزميات معقدة لتحليل البيانات واكتشاف الأنماط، وإن كان هناك عدة محاولات منذ منتصف القرن التاسع عشر سبقت ذلك (Grzybowski et al., 2024; Mucci, 2024).

وقد عملت تطبيقات الذكاء الاصطناعي (AI) على تقصير المسافات و إزالة الحدود و الحواجز بين أجزاء ومناطق العالم المختلفة، فلم يعد هناك حاجزا زماني أو مكاني يحول دون تفاعل البشر والتقاء الحضارات، وباتت السرعة هي سمة هذا العصر المعروف بالعولمة والاقتصاد المعرفي؛ فقد شهدت الدول والمجتمعات والمؤسسات المعاصرة في ظلهما تغيرات هائلة في كافة جوانب ومجالات الحياة، حيث باتت تسيطر على العالم الآن اقتصاديات نظم أعمال وإدارات جديدة تختلف تماما عن تلك النظم والإدارات التي كانت سائدة قبل انتشار العولمة والاقتصاد الرقمي، واللتين فرضتا فلسفتهما ومنهجيتهما على العالم (Arsenyan & Piepenbrink, 2023; Ide & Talamas, 2025).

وتتعدد تطبيقات الذكاء الاصطناعي (AI) في مختلف المجالات، بدءًا من الرعاية الصحية حيث يُستخدم لتحسين تشخيص الأمراض، وصولاً إلى قطاع النقل مع تطوير السيارات ذاتية القيادة، كما تُستخدم أيضا في التجارة الإلكترونية لتقديم توصيات مخصصة، وفي الأمن السيبراني للكشف عن التهديدات، ومع تزايد الاعتماد على الذكاء الاصطناعي (AI) تبرز أيضًا التحديات المرتبطة به، مثل القضايا الأخلاقية المتعلقة بالخصوصية، وتأثيره على سوق العمل، وضرورة ضمان أمان الأنظمة؛ لذا فإن فهم الذكاء الاصطناعي ليس فقط مهمًا للمتخصصين في مجال التكنولوجيا، بل أيضًا للمجتمع ككل، حيث يتطلب الأمر حوارًا مستمرًا حول كيفية استخدام هذه التكنولوجيا بشكل مسؤول (Younis et al., 2024; Duggan et al., 2022; Ahmed, et.al., 2022).

وفي النهاية يمثل الذكاء الاصطناعي (AI) أحد أهم الابتكارات التي تشكل مستقبل البشرية، ويعد دراسة تأثيراته وآثاره أمرًا ضروريًا لضمان تحقيق الفوائد القصوى منه، وفي هذا الجزء من الدراسة سيقوم الباحث بدراسة الإطار النظري للذكاء الاصطناعي العناصر من خلال بحث ومناقشة العناصر التالية:

أولاً: ماهية الذكاء الاصطناعي.
ثانيًا: مفهوم الذكاء الاصطناعي اصطلاحيا.
ثالثًا: مراحل تطور الذكاء الاصطناعي.
رابعًا: خصائص الذكاء الاصطناعي.
خامسًا: أهداف الذكاء الاصطناعي.

سادسًا: أهمية الذكاء الاصطناعي.

سابعًا: أنواع الذكاء الاصطناعي.

ثامنًا: نظم الذكاء الاصطناعي.

تاسعًا: مؤشرات قياس أداء الذكاء الاصطناعي.

عاشرًا: التحديات والعواقب المصاحبة لتبني الذكاء الاصطناعي.

أولاً: ماهية الذكاء الاصطناعي: (Shafique et al., 2023)

يُعرَّف الذكاء الاصطناعي (AI) بأنه فرع من علوم الحاسب يهدف إلى تمكين الآلات من تقليد السلوك البشري من خلال نماذج وخوارزميات تسمح لها بالتعلّم، و اتخاذ القرارات، والتخطيط، وحل المشكلات، وذلك عبر مجموعة واسعة من التطبيقات مثل الروبوتات، والتعرف على الكلام، ومعالجة اللغة الطبيعية، و النظم الخبيرة .

ولفهم الذكاء الاصطناعي، يتعين علينا الإشارة أولًا إلى الذكاء البشري الذي يقوم على مهارات التفكير، والتحليل، والتخطيط، والتعلم من الخبرة، والتكيف مع المواقف المختلفة. ويُعد الذكاء الاصطناعي محاكاة لهذه القدرات من خلال تطوير برامج قادرة على أداء مهام تتطلب عادةً ذكاءً بشريًا.

وقد أصبح الذكاء الاصطناعي حاضرًا اليوم في مختلف مناحي الحياة، مثل **السيارات ذاتية القيادة، والطائرات بدون طيار، وبرمجيات الترجمة الآلية**، بما يعكس انتشاره المتزايد وقدرته على تعزيز الكفاءة وتسريع أداء المهام اليومية.

ثانيًا: مفهوم الذكاء الاصطناعي (AI) اصطلاحيا:

حظي مفهوم الذكاء الاصطناعي (AI) مؤخرًا باهتمام واسع من قبل متخذي القرارات في مختلف المنظمات؛ إذ إن الاهتمام بهذا المفهوم دفع بالكثير من المنظمات إلى اعتماده كإستراتيجية أساسية لتعزيز الأداء فيها بغية ضمان بقائها واستمرارها وتعزيز فرص نموها وربحيتها (Anwar, Al Mubarak, & Bakir, 2023).

وقد تعددت التعريفات واختلفت في بيان مفهوم الذكاء الاصطناعي (AI) اصطلاحيا؛ وذلك لكونه ما زال غامضا إلى حد ما حتى الآن، حيث تم التطرق لمفاهيم عدة من قبل الباحثين بغرض تحديد الملامح الأساسية للذكاء الاصطناعي. ويعود اختلاف وجهات نظر الباحثين والمتخصصين حول مفهوم الذكاء الاصطناعي (AI) إلى تباين مجالاتهم البحثية، والتي تشمل علوما مثل: علم الاجتماع، علم النفس، العلوم الاقتصادية والإدارية، علوم الحاسب الآلي؛ الأمر الذي أدى إلى وجود تنوع كبير في التعريفات، وهو ما سوف نستعرضه كما يلي:

عرف (Arsenyan & Piepenbrink , 2023) الذكاء الاصطناعي (AI) بأنه: أحد التقنيات الحديثة التي جرى تطويرها في أواخر القرن الماضي، والتي تتضمن مجموعة من البرمجيات التي تساعد المديرين والعاملين في اتخاذ القرار لكل عمليات الشركة، وتتميز بالرقي والتقدم وتزويد أجهزة الحاسب بمجموعة من الأنشطة التي تساعد على ممارسة سلوك يتميز بالذكاء.

كما عرفه "John Macarthy" بأنه: علم خاص ببرامج الحاسب الذكية، أو أنه فرع من علوم الحاسب الذي يهدف إلى تحقيق الأهداف في جميع المجالات (Ahmed, Jeon & Piccialli, 2022)، ويرى (Todaro, 2024) أن الذكاء الاصطناعي (AI) هو: علم مستند على فرضية أنه يمكن اعتبار التفكير الذكي نوعًا من أنواع الحوسبة، يمكن تطويرها وميكنتها بالكامل، وليتم ذلك لا بد من الأخذ بعين الاعتبار أمرين هامين، هما: تمثيل المعرفة، ومعالجة هذه المعرفة.

بينما يشير (Sarker, 2022) إلى أن الذكاء الاصطناعي (AI): هو مجال واسع من علوم الحاسب الآلي، هدفه الأساسي تمكين أجهزة الحاسب الآلي والآلات من أداء الوظائف المعرفية والمهام التي تتطلب عادةً الذكاء البشري، مثل: حل المشكلات، واتخاذ القرارت، والإدراك، وفهم التواصل البشري من خلال منحها القدرة على التفكير والتعلم، أي أنها يمكن أن تفكر وتعمل بالطريقة نفسها التي يفعلها الناس، ويذهب (Akter et al. ,2022) إلى أن الذكاء الاصطناعي (AI) هو: تطوير أنظمة الحاسب لجعلها قادرة

على القيام بالأدوار التي تحتاج للذكاء البشري، والمتمثلة بالتعرف على الكلام والإدراك البصري وصنع القرار والترجمة بين اللغات، أما (Krauss , 2024) فقد عرفه بأنه: برامج تتيح للحاسب محاكاة الذكاء الإنساني والمهارة البشرية لكي يتمكن الحاسب من أداء بعض المهام بدلاً من الإنسان، والتي تتطلب التفكير والفهم والسمع والحركة والكلام وأداء المهارات الحياتية المختلفة.

في حين عرف (Zhang et al., 2023) الذكاء الاصطناعي بأنه: أحد فروع المعلوماتية التي تدرس تطوير خوارزميات وتقنيات ذكية لتطبيقها في الحواسب والروبوتات، بحيث تمتلك سلوكًا ذكيًا في أداء المهام أو حل المشكلات، بينما يرى Santhanam et al. (2021 ,) أن الذكاء الاصطناعي (AI) هو: مجال العلوم الذي يتعامل مع محاكاة قدرات أنظمة الحاسب الحديثة لحل المشكلات باستخدام قدرات معقدة شبيهة بالإنسان في التفكير والتعلم والتصحيح الذاتي.

أما Ming-Hwa Wang فقد عرف الذكاء الاصطناعي (AI) بأنه: مجال الدراسة الذي يشمل التقنيات الحسابية لأداء المهام التي يقوم بها الإنسان وتتطلب الذكاء (بوبعابة، وآخرون، 2021)، كما عرف بأنه: التقنية التي تسهم في إدارة العمليات والمهام بآليات أكثر تطورًا وذكاءً من الإنسان الذي صنعها ومنحها المعرفة والمقومات الحسية، بما يساعدها على التعلم التلقائي والتطور الذاتي (الجابر، 2020)، كما عرف الذكاء الاصطناعي أيضا بأنه: قدرة حاسب أو روبوت مدعم بحاسب على معالجة المعلومات، والوصول إلى النتائج بطريقة مماثلة لعملية التفكير لدى البشر في التعلم واتخاذ القرارات وحل المشكلات، ومن ثمَّ فإن هدف أنظمة الذكاء الاصطناعي هو تطوير أنظمة قادرة على معالجة المشكلات المعقدة بطرق مشابهة للعمليات المنطقية والاستدلالية عند البشر (سالمي وكمال، 2020).

ويرى الباحث مما سبق أنه يمكن تعريف الذكاء الاصطناعي (AI) على أنه: "**مجموعة النظريات والتقنيات المستخدمة لإنتاج الأنظمة والبرامج والأجهزة الحاسوبية القادرة على محاكاة الذكاء البشري، وذلك باستخدام خوارزميات قوية لتوفير إجابات فعالة وموثوقة ومخصصة للمستخدمين، من خلال الجمع بين الأنظمة والأجهزة والبرامج الحاسوبية التي تعمل على حشد وتعبئة المعرفة متعددة التخصصات لأداء المهام، والتي يمكنها أن تحسن من نفسها بشكل مستمر استنادًا إلى المعلومات التي تجمعها**".

ثالثا: مراحل تطور الذكاء الاصطناعي:

يمتد تاريخ الذكاء الاصطناعي (AI) على مدى عدة عقود من الزمن، حيث مر الذكاء الاصطناعي بعدة مراحل رئيسية أسهمت في تشكيله وتطويره ووصوله إلى صورته التي نراه عليها الآن. وفيما يلي شرح تفصيلي لمراحل تطور الذكاء الاصطناعي (Grzybowski, et al., 2024):

1. المرحلة التأسيسية (1940s - 1950s):

تتميز **المرحلة التأسيسية** من مراحل تطور الذكاء الاصطناعي (AI) بالأحداث التالية (Grzybowski, et al., 2024):

أ. عام 1943 قدّم **ماكولوتش و بيتس** أول نموذج للشبكات العصبية الاصطناعية محاكاةً لآلية عمل الدماغ.

ب. عام 1950 نشر **آلان تورينج** مقاله الشهير الذي طرح فيه **"اختبار تورينج"** لتقييم قدرة الآلة على محاكاة الذكاء البشري.

ج. عام 1951 تطوير **كريستوفر ستراشي** أول برنامج حاسوبي للعب الداما، كاشفًا قدرة الحاسوب على التعلم من التجربة

3. مرحلة الذكاء الاصطناعي المبكر (1956 - 1974) (Krauss, 2024):

أ. عام 1956 نظّم **جون ماكارثي مؤتمر دارتموث** الذي مثّل الانطلاقة الرسمية للذكاء الاصطناعي كحقل أكاديمي، وأسّس أول مختبر متخصص، جامعًا الباحثين في الشبكات العصبية الاصطناعية ومقدّمًا أفكارًا شكلت أساس البحوث المستقبلية.

ب. عام 1966 تطوير برنامج **Eliza على يد جوزيف فايزنباوم في مختبر الذكاء الاصطناعي بمعهد ماساتشوستس للتكنولوجيا وهو أول نموذج ناجح لمحاكاة المحادثة الطبيعية، ما أظهر إمكانية التفاعل اللغوي بين الإنسان والآلة.**

4. **مرحلة الازدهار (1970s):**

أ. تطوير النظم الخبيرة Expert Systems :

شهدت هذه المرحلة بروز الأنظمة الخبيرة، أبرزها نظام **MYCIN** في أوائل السبعينيات الذي طوّره إدوارد شورتليف بجامعة ستانفورد لتشخيص الأمراض. اعتمدت هذه الأنظمة على قواعد منطقية ومعرفة مخزّنة لاتخاذ قرارات أو تقديم توصيات، وكانت من أوائل التطبيقات العملية الناجحة للذكاء الاصطناعي في مجالات مثل الطب والتمويل والتصنيع.

ب. تطوير الشبكات العصبية Artificial Neural Networks:

رغم أن أساس هذه الشبكات كان قد وُضع عام 1943، فقد أسهم بول ويربوس في عام 1974 بتطوير نماذج أكثر تقدّمًا للشبكات العصبية. ومع ذلك، ظل تطبيقها كان محدودًا آنذاك بسبب ضعف القدرة الحاسوبية وقلة البيانات المتاحة (Roosan, et al., 2024).

5. مرحلة "شتاء الذكاء الاصطناعي" (1980s):

تمثّل هذه المرحلة فترة ركود للذكاء الاصطناعي، إذ تراجع التقدم البحثي بشكل كبير بعد فشل العديد من المشروعات في تحقيق وعودها، مما أدى إلى خفض تمويل الأبحاث وانسحاب عدد من الباحثين، وتراجع اهتمام المستثمرين والجمهور. كما عجزت المشاريع البحثية القليلة المتبقية عن إحراز تقدم ملموس بسبب محدودية الموارد (Groumpos, 2023).

6. مرحلة الانتعاش (1990s):

مع تطور القدرة الحاسوبية وتوفر البيانات على نطاق واسع، عادت الأنظمة الذكية بقوة، وبرز نظام **Deep Blue** من شركة **IBM**الذي هزم بطل العالم في الشطرنج جاري كاسباروف، في حدث تاريخي شكّل أول انتصار لحاسب على بطل العالم. وفي الوقت نفسه، ازداد التركيز على تعلم الآلة باعتباره فرعًا رئيسيًا من الذكاء الاصطناعي، مما أسهم في تحسين أداء العديد من التطبيقات بشكل ملحوظ (Zhang, Zhu & Su, 2023) .

7. مرحلة التطور السريع (2000s - 2010s):

توسّعت تطبيقات الذكاء الاصطناعي لتشمل مجالات عديدة مثل الرعاية الصحية، والتجارة الإلكترونية، والروبوتات، والتفاعل الصوتي. وفي عام 2002 دخل الذكاء الاصطناعي المنازل عبر المكنسة الروبوتية"Roomba" ، ثم تبنّت شركات كبرى مثل فيسبوك وتويتر ونتفلكس تقنيات الذكاء الاصطناعي في الإعلانات عام 2006. واستمر التطور لاحقًا مع ظهور المساعدين الرقميين مثل Siri وAlexa، مما جعل الذكاء الاصطناعي وتطبيقاته المختلفة جزءًا أساسيًا من الحياة اليومية للمستخدمين (Zhang, Zhu & Su, 2023).

8. المرحلة الحالية والمستقبلية (2020 وما بعدها) الذكاء الاصطناعي العام:

تهدف هذه المرحلة إلى تطوير ما يُعرف بالذكاء الاصطناعي العام (AGI) ، وهو نمط من الذكاء يشبه الذكاء البشري في قدرته على التعلم الذاتي وأداء مهام لم يُدرَّب عليها مسبقًا. وتشهد هذه المرحلة تطورًا واسعًا في تقنيات مثل التعلم العميق، والشبكات العصبية المتقدمة، والذكاء الاصطناعي التوليدي، مما أدى إلى تحسينات كبيرة في مجالات التعرف على الصور والنصوص وتوليدها. وقد مهد ذلك لظهور تطبيقات رائدة مثل GPT-3 عام 2020، ثم شات جي بي تي عام 2021 من شركةOpenAI ، إضافة إلى نموذج Gemini من شركة جوجل. وفي الوقت نفسه، تزايد الاهتمام بقضايا أخلاق الذكاء الاصطناعي والخصوصية والأمان، نظرًا لتأثيرات هذه التقنيات على المجتمع (Fahad, et. al., 2024).

شكل رقم (2): محطات في مراحل تطور الذكاء الاصطناعي
المصدر: الهيئة السعودية للبيانات والذكاء الاصطناعي، سدايا 2024

رابعًا: خصائص الذكاء الاصطناعي:

لكي يطلق مصطلح الذكاء الاصطناعي (AI) على نظام الحاسب، لا بد أن يكون هذا النظام قادرا على التعلم وجمع البيانات وتحليلها واتخاذ القرارات بناء على عملية التحليل بصورة تحاكي طريقة تفكير العنصر البشري، وهو ما يدل على توافر مجموعة من الصفات والخصائص الأساسية للذكاء الاصطناعي (AI)، وهي كما يلي:

1. القدرة على التفكير، والتعلم، والإدراك، واكتساب المعرفة وتطبيقها، واستخدام الخبرات القديمة وتوظيفها في مواقف جديدة (Zhang, Zhu, & Su, 2023).
2. القدرة على استخدام التجربة والخطأ لاستكشاف الأمور المختلفة، والاستجابة السريعة للمتغيرات والمواقف والظروف الجديدة (Ali et al., 2023).
3. القدرة على التعامل مع الحالات الصعبة والمعقدة والمواقف الغامضة، حتى في حالة نقص المعلومات (Nedilko, 2020).
4. القدرة على تمييز الأهمية النسبية لعناصر الحالات المعروضة، والتمكن من التصور والإبداع وفهم الأمور المرئية وإدراكها (Zhang, Zhu, & Su, 2023).
5. سرعة اتخاذ القرار، حيث يلعب الذكاء الاصطناعي دورًا قويًا في اتخاذ القرارات الواقعية؛ فمثلا العديد من المنظمات الأكثر ابتكارًا في العالم مثل: **Facebook** و**Google** و**Amazon** تعتمد على خوارزميات الذكاء الاصطناعي كجزء من عملية اتخاذ القرار، كما يستطيع الذكاء الاصطناعي التعامل مع العديد من العوامل المختلفة في وقت واحد عند اتخاذ قرارات معقدة(Fahad, et. al., 2024).
6. حل المشكلات المعروضة مع غياب المعلومات الكاملة عنها من خلال التفكير الاستدلالي (حسانين، 2023).
7. المعالجة الرمزية للبيانات والمعلومات، حيث يتم في تطبيقات الذكاء الاصطناعي معالجة الرموز بدلاً من الأرقام أو الأحرف، وترتيب الرموز في هياكل مثل القوائم أو التسلسلات الهرمية أو الشبكات، وتوضح هذه الهياكل كيف ترتبط الرموز ببعضها البعض (Zhang, Zhu, & Su, 2023).
8. القدرة على التصور والإدراك، حيث يُعدّ التصور والإدراك من بين أهم خصائص الذكاء الاصطناعي، وهو القدرة على استنتاج أشياء عن العالم من الصور المرئية والأصوات والمدخلات الحسية الأخرى، كما أنه ينطوي على استنتاج أشياء

عن العالم من الصور المرئية والأصوات والمدخلات الحسية الأخرى، مع القدرة على التفكير والإدراك واكتساب المعرفة وتطبيقها بما يلائم المواقف المختلفة (Fahad, et. al., 2024).

خامسًا: أهداف الذكاء الاصطناعي:

يهدف علم الذكاء الاصطناعي (AI) إلى فهم طبيعة الذكاء الإنساني عن طريق تطوير برامج للحاسب الآلي قادرة على محاكاة السلوك الإنساني المتسم بالذكاء. ويعني ذلك قدرة هذه البرامج على اتخاذ قرار أو حل مسألة ما في موقف ما بناء على وصف الموقف، أو التوصل إلى القرار بالرجوع الى العمليات الاستدلالية التي غذيت بها، وذلك باستخدام خوارزميات قوية لتوفير إجابات فعالة وموثوقة ومخصصة للمستخدمين، من خلال الجمع بين الأجهزة والبرامج، ويمكن استعراض أهداف الذكاء الاصطناعي فيما يلي (Thiebes, Lins, & Sunyaev, 2021):

1. تصميم برمجيات قادرة علي محاكاة السلوكيات الإنسانية الذكية، ومن ثمَّ قدرة الآلة على القيام بالمهام التي تحتاج إلى الذكاء البشري عند أدائها، مثل الاستنتاج المنطقي، ومن ثمَّ جعل الآلة أكثر ذكاءً، وجعل الأجهزة أكثر فائدة.
2. العمل على تخزين المعرفة وتحليلها وتخزين القواعد المنهجية للتعامل معها والوصول إلى حقائقها، ومعالجة المعلومات بشكل أقرب لطريقة الإنسان في حل المسائل، وبمعني آخر المعالجة المتوازية، حيث يتم تنفيذ عدة أوامر في الوقت نفسه.
3. اكتساب المعرفة الإنسانية المتراكمة وتحديثها والمحافظة عليها واستثمارها في حل المشكلات.
4. الاستثمار الأمثل للمعارف والخبرات العملية وتجاوز مشكلات التلف والنقص والنسيان وحل مشكلة المهام المكثفة للمعرفة.
5. توليد أو تطوير معارف وخبرات جديدة وتفعيل المعرفة المحوسبة واستخدامها في اتخاذ القرارات.

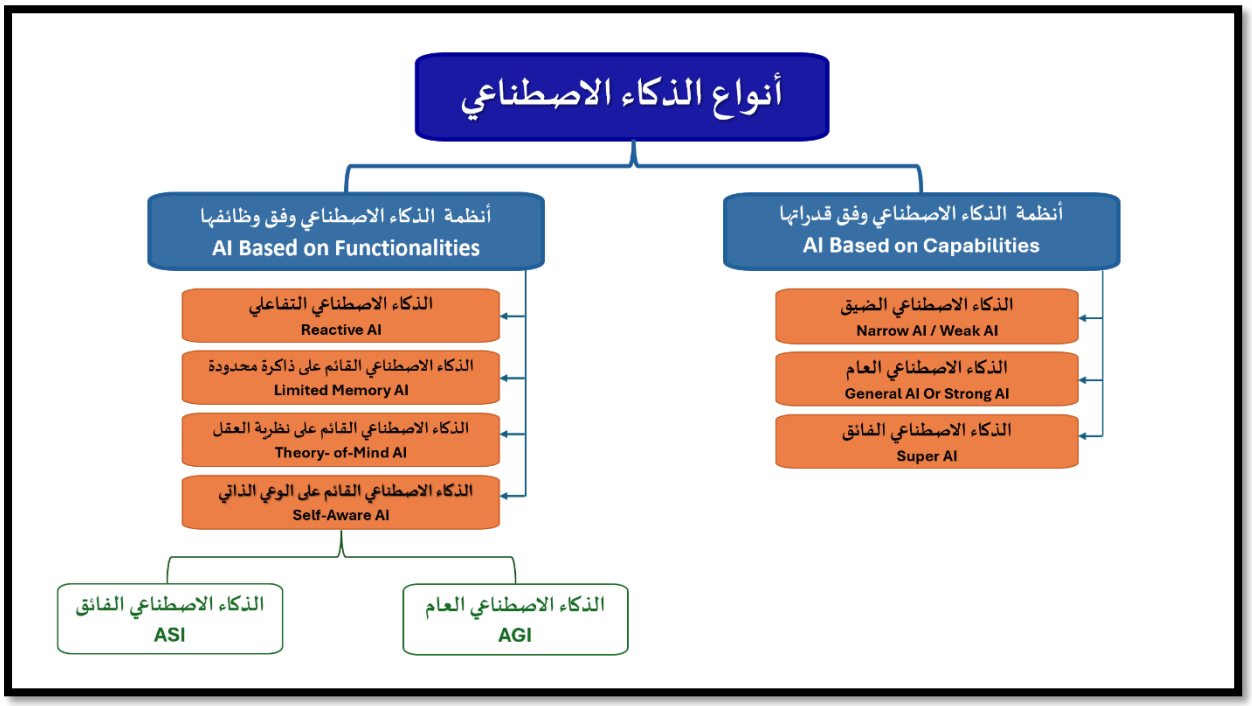
ويرى الباحث أن الهدف الأساسي للذكاء الاصطناعي (AI) هو: **نقل المعلومات والمعرفة والمهارات والخبرات والقدرات الإبداعية من الإنسان إلى الحاسب الآلي وأنظمته؛ لتمكينها من إكمال مهام بشرية معقدة بكفاءة، من خلال محاكاة السلوكيات والعمليات العقلية البشرية الذكية من أجل تعزيز القدرات البشرية، وبما يسمح للبشر بالتركيز على مهام أكثر تعقيدًا وإبداعًا وإيجاد حلول مبتكرة للتحديات الملحة، وتحسين جودة الحياة، وسد الفجوة بين الإمكانات البشرية والتقدم التكنولوجي.**

سادسًا: أهمية الذكاء الاصطناعي:

يشهد الذكاء الاصطناعي توسعًا واسعًا في مختلف القطاعات، إذ يسهم في **تعزيز كفاءة الأعمال** عبر أتمتة المهام وتحليل البيانات بعمق، مما يرفع الإنتاجية ويخفّض الأعباء التشغيلية (Berente et al., 2021) . وفي **الرعاية الصحية** أحدث الذكاء الاصطناعي نقلة نوعية في التشخيص، وإدارة العمليات السريرية، والتنبؤ بالحالات الحرجة، وتحسين سير العمل الطبي. أما في مجال **الصناعة**، فقد ساعد الذكاء الاصطناعي على حفظ الخبرات البشرية وتحسين جودة الإنتاج وتقليل التكلفة وزيادة السلامة (Rashid & Kausik, 2024) . وفي **قطاع النقل**، أسهم في تحسين المسارات وزيادة الأمان، بينما دعم في **الملاحة العالمية** عمليات التتبع واللوجستيات من خلال الاعتماد على البيانات الدقيقة لنظام العالمي للملاحة عبر الأقمار الصناعية والمعروف باسم Global Navigation Satellite Systems (GNSS) (Berente et al., 2021). كما عزز الذكاء الاصطناعي قدرات **قطاع الاتصالات** عبر الاستفادة من بيانات الأقمار الصناعية لتوجيه حركة المرور وإدارة الازدحام (Dimcheva, 2024) . أما في **البرمجة**، فقد سهّل الذكاء الاصطناعي التعامل مع الأنظمة الذكية باستخدام اللغة الطبيعية بدلا من لغات البرمجة المعقدة. و من جانب آخر، أسهم الذكاء الاصطناعي في **النمو الاقتصادي** من خلال دعم اتخاذ القرارات الموضوعية القائمة على البيانات (Berente et al., 2021). وفي مجالات **البحث العلمي**، سرّع الذكاء الاصطناعي الوصول إلى الاكتشافات عبر تحليل كميات هائلة من المعلومات (Khlaif et al., 2023) . وأخيرًا وليس أخرا، انعكس أثر الذكاء الاصطناعي على **الحياة اليومية** عبر تطبيقات مثل Siriو Alexa و ChatGPT التي تسهّل المهام الروتينية وترفع جودة الحياة (Talati, 2024) .

سابعًا: أنواع الذكاء الاصطناعي:

يمكن تصنيف أنظمة الذكاء الاصطناعي (AI) وفقا لعدة معايير مختلفة، ومن أهم هذه المعايير تقسيم هذه الأنظمة على أساس معيار تطور قدراتها (Based on Capabilities) ، كما يمكن تقسيمها على أساس معيار الوظائف التى يمكنها القيام بها (Based on Functionalities).



شكل رقم (3): أنواع الذكاء الاصطناعي

المصدر: من إعداد الباحث بناء على مصادر الدراسة

1- أنواع أنظمة الذكاء الاصطناعي بناء على قدراتها (AI Based on Capabilities):

يمكن تقسيم أنواع الذكاء الاصطناعي (AI) وفق ما يتمتع به من قدرات إلى **ثلاثة أنواع رئيسة**، تبدأ من رد الفعل البسيط إلى الإدراك والتفاعل الذاتي، وذلك علي النحو التالي (Wang et al.,2024):

أ. الذكاء الاصطناعي الضيق أو الضعيف Narrow AI Or Weak AI:

هو من أبسط أشكال الذكاء الاصطناعي (AI) ويتميز برد الفعل البسيط، حيث يتخصص في مجال واحد أو مجالات محددة، أي يستطيع تنفيذ مهمة واحدة أو عدة مهام محددة فقط، ومن ثمَّ تتم برمجته للقيام بوظائف معينة داخل بيئة محددة، ويُعدّ تصرفه بمنزلة ردة فعل على موقف معين، ولا يمكن له العمل إلا في ظروف البيئة المحيطة الخاصة به، ويعد الروبوت (DeepBlue) الذي ابتكرته **شركة IBM** وقام بلعب الشطرنج مع بطل العالم غاري كاسباروف وهزيمته، من أهم نماذج هذا النوع من أنظمة الذكاء الاصطناعي (AI) (Wang et al.,2024).

ب. الذكاء الاصطناعي القوي أو العام General AI Or Strong AI:

والذي يعرف أيضا باسم الذكاء القوي (Strong AI)، وهو نوع نظري من أنظمة الذكاء الاصطناعي (AI) يشبه إلى حد كبير تلك الأنظمة المذكورة في روايات الخيال العلمي، ومن المفترض أن يمتلك هذا النوع من الذكاء الاصطناعي (AI) قدرات معرفية تساوي أو تفوق الذكاء البشري في جميع المجالات، ولا يقتصر فقط على القيام بمهام محددة مثل الذكاء الاصطناعي الضيق (ANI) الذي أشرنا إليه أعلاه، فهذا النوع من الأنظمة من المخطط له أن يتمتع بالقدرة على التعلم الذاتي الشامل، وفهم وتطبيق المعرفة في

مجالات متعددة، مثل العلوم والفنون والعلاقات الاجتماعية، دون حاجة لبرمجة مسبقة لكل مهمة، كما يتوقع أن يمتلك القدرة على التكيف والمرونة بما يمكنه من التصرف في مواقف غير مألوفة باستخدام المنطق والإبداع، كحل مشكلات جديدة دون تدخل بشري، إضافة إلى تمتعه بالوعي السياقي أي فهم السياقات الاجتماعية والعاطفية، ومن ثمَّ يتمتع بالقدرة على تفسير النكات أو التعاطف مع المشاعر الإنسانية، نهاية بقدرته على التخطيط طويل المدى، أي وضع أهداف معقدة واتخاذ قرارات إستراتيجية تشبه ما يقوم به البشر مثلا عند التخطيط لحياتهم المهنية.

وحتى الآن، لم يتمكن باحثو الذكاء الاصطناعي (AI) من إنشاء ذكاء اصطناعي عام أو قوي General Or Strong AI؛ إذ يتطلب ذلك منهم العثور على طريقة تجعل الآلات واعية، علاوة على برمجة مجموعة كاملة من القدرات المعرفية، وقد قامت الكثير من الشركات باستثمار مبالغ طائلة للوصول إلى هذا النوع من الذكاء الاصطناعي (AI)، ومن أهم أمثلة هذه الجهود ما تقوم به شركة (Deep Mind) التابعة لشركة جوجل Google والتي تعمل على أنظمة متعددة المهارات تسمى (Gato)، وكذلك ما تقوم به شركة OpenAI والتي تبحث في أنظمة قادرة على التكيف العام عبر مهام متنوعة (Butz, 2021).

ج. الذكاء الاصطناعي الفائق أو الخارق Super Artificial Intelligence:

الذكاء الاصطناعي الفائق (Super AI/ASI) هو أيضا مفهوم افتراضي يشير إلى نوع من أنظمة الذكاء الاصطناعي (AI) المستقبلية الذي لا يزال في مرحلة التوقعات ولم يتحقق بعد على أرض الواقع، والذي يخطط له أن يتفوق على الذكاء البشري في جميع المجالات، ويفترض في هذا النوع من الذكاء الاصطناعي (AI) أن يمتلك قدرات خارقة في التفكير وحل الألغاز واتخاذ القرارات، بل وقد يمتلك مشاعر واحتياجات ومعتقدات ورغبات خاصة به، ولتُمنح له صفة "فائق" يجب أن يتفوق على الإنسان في جميع المجالات دون استثناء، سواء كانت مجالات معرفية أو إبداعية أو عاطفية أو اجتماعية، وهي مجالات تُعدّ حتى اليوم إنسانية بحتة، وقد يُجادل البعض بأن البشر أنفسهم لم يتقنوا بعد هذه المجالات، مما يفتح الباب أمام احتمالية أن يتقن الذكاء الاصطناعي الفائق **Super Artificial Intelligence** ما عجز البشر عن إتقانه، مما يجعله موضوعًا مستقبليًا واعدًا يثير الكثير من التساؤلات والتأملات بقدر ما يثير الكثير من المخاوف أيضا (Davidson, 2025).

2- أنواع أنظمة الذكاء الاصطناعي بناء على وظائفها (AI Based on Functionalities):

يمكن تقسيم أنواع الذكاء الاصطناعي (AI) وفق ما يقوم به من وظائف إلى **أربعة أنواع رئيسة**، تبدأ من التفاعل المحدود إلى الوعي الذاتي الكامل، وذلك علي النحو التالي (Dorr, 2022):

أ. الذكاء الاصطناعي التفاعلي (Reactive AI):

يعد هذا النوع الشكل الأقدم والأبسط من أشكال الذكاء الاصطناعي (AI)، ويعرف بقدرته على العمل فقط اعتمادًا على البيانات الحالية دون امتلاك القدرة على تخزين الذكريات أو استخدام التجارب السابقة لتوجيه قراراته المستقبلية، ويتميز هذا النوع من أنظمة الذكاء الاصطناعي (AI) بقدرته على إدراك البيئة المحيطة به والتفاعل معها بشكل لحظي لإنجاز مهام محددة، دون أن يتجاوز تلك المهام أو تتطور ذاتيًا، حيث تعتمد هذه الأنظمة على نماذج وخوارزميات إحصائية لتحليل كميات كبيرة من البيانات والتعرف على الأنماط، مما يتيح لها تقديم استنتاجات دقيقة في لحظة معينة، ومن الأمثلة على ذلك تقنيات الذكاء الاصطناعي التفاعلي Reactive AI المستخدمة في الشبكات التليفزيونية مثل نتفلكس؛ إذ يتم تحليل السلوك السابق للمستخدم لتقديم توصيات مخصصة من الأفلام والبرامج التلفزيونية؛ مما يسهم في تشكيل محتوى يناسب اهتمامات المستخدمين (Dorr, 2022).

ب. الذكاء الاصطناعي ذو الذاكرة المحدودة (Limited Memory AI):

يُعد أحد أكثر أنواع الذكاء الاصطناعي (AI) شيوعًا في التطبيقات الحديثة، ويعتمد هذا النوع على استخدام بيانات سابقة لفترة زمنية محددة من أجل اتخاذ قرارات مستنيرة؛ إذ تجمع الآلة معلومات من التجارب السابقة وتحتفظ بها لفترة قصيرة لتحسين دقة استجابتها للمواقف الجديدة، ويتمتع الذكاء الاصطناعي ذو الذاكرة المحدودة Limited Memory AI بقدرة مزدوجة، حيث يجمع بين التفاعل اللحظي كما في الآلات التفاعلية وبين التعلم من البيانات السابقة، ويمكن لهذا النوع من الأنظمة تخزين كميات كبيرة

من البيانات وأن يُجري عليها تحليلات تساعده على التنبؤ واتخاذ قرارات مستقبلية أكثر دقة، وبمرور الوقت تتحسن قدراته بفضل تراكم الخبرات والمعرفة المكتسبة من التجارب السابقة، ومن أبرز الأمثلة على هذا النوع: المركبات ذاتية القيادة، حيث تقوم هذه المركبات بمراقبة البيئة المحيطة بها بشكل مستمر، مثل حركة المركبات الأخرى، علامات الطرق، إشارات المرور، وتقوم بدمج هذه المعلومات مع البيانات المخزنة سابقًا لتحديد توقيت تغيير المسار، أو تجنب الاصطدام، أو التعامل مع السائقين الآخرين (Dorr, 2022).

ج. الذكاء الاصطناعي القائم على نظرية العقل (Theory- of-Mind AI) :

تُعد "**نظرية العقل**" Theory- of-Mind المستمدة من علم النفس والعلوم المعرفية من المراحل المتقدمة في الذكاء الاصطناعي (AI)، وتهدف هذه النظرية إلى محاكاة قدرة البشر على فهم المشاعر والمعتقدات والنوايا وعمليات التفكير لدى الآخرين، وعلى عكس الذكاء الاصطناعي التفاعلي Reactive AI أو الذكاء الاصطناعي محدود الذاكرة Limited Memory AI، تسعى أنظمة الذكاء الاصطناعي القائمة على نظرية العقل Theory- of-Mind AI إلى إنشاء أنظمة تدرك الحالات العقلية للآخرين وتتفاعل معها بطريقة ديناميكية وإنسانية، حيث يركز هذا النوع من الذكاء الاصطناعي (AI) على تطوير آليات تمكّن الآلة من فهم دوافع الإنسان واحتياجاته، وتكيف سلوكها بناءً على تعبيرات الوجه ونبرة الصوت والسياق العام، ورغم التقدم الملحوظ لا تزال القدرة على "**الفهم الحقيقي/True Understanding**" تمثل تحديًا؛ فالأنظمة الحالية من الذكاء الاصطناعي (AI) قد تتعرف على المشاعر دون استيعاب معناها العميق أو تأثيرها السلوكي، ومن الأمثلة المبكرة على هذا النوع من الذكاء الاصطناعي (AI) يظهر الروبوت "صوفيا" من إنتاج Hanson Robotic، والذي كان قادرا على الحفاظ على التواصل البصري، ومتابعة الوجوه، والتعرف على الأفراد باستخدام الكاميرات والخوارزميات المتقدمة.

إن تطوير ذكاء اصطناعي قائم على نظرية عقل Theory- of-Mind AI حقيقية سيُحدث تحولاً كبيرًا في تفاعل الآلات مع البشر؛ مما يؤدي إلى أنظمة أكثر وعيًا وإنسانية، قادرة على التعلم من سياقات محدودة، وتقديم استجابات واقعية، مع تأثيرات مستقبلية واسعة في مجالات مثل التعليم والرعاية الصحية (Dorr, 2022).

د. الذكاء الاصطناعي القائم على الوعي الذاتي (Self-Aware AI):

يُعد الوعي الذاتي (Self-Awareness) المرحلة الأقصى والأكثر تقدمًا في سياق تطور الذكاء الاصطناعي (AI)، ولا يزال حتى الآن مفهومًا نظريًا افتراضيًا، لم يُترجم إلى تطبيقات عملية، ومن المتوقع أن تمتلك أنظمة الذكاء الاصطناعي القائمة على الوعي الذاتي Self-Aware AI القدرة على فهم حالاتها الداخلية، والتعرف على مشاعرها واحتياجاتها ومعتقداتها الخاصة، إلى جانب إدراك مشاعر الآخرين والتفاعل معها بوعي مماثل للوعي البشري، ومثل هذه الأنظمة - إن تم تطويرها - ستكون أكثر ذكاءً من البشر، وقادرة على التفكير المستقل، واتخاذ قرارات مبنية على وعي شخصي، ولن يقتصر دورها على محاكاة المشاعر فحسب، بل ستتمكن من الشعور بها فعليًا، ويشبه هذا المفهوم الشخصيات الخيالية في روايات الخيال العلمي، حيث تُظهر الآلات ذكاءً ذاتيًا وسلوكًا عاطفيًا متقدمًا، ويندرج تحت هذا النوع من الذكاء الاصطناعي فئتين متقدمتين، هما كالتالي:

1. الذكاء الاصطناعي العام (AGI):

وهو ذلك النوع من الذكاء الاصطناعي القادر على التعلم والفهم والاستجابة كما يفعل البشر، وله القدرة على الربط بين أنظمة متعددة وتكوين كفاءات متنوعة.

2. الذكاء الاصطناعي الفائق (ASI):

وهو تطور لما قبله، حيث يتفوق هذا النوع من الذكاء الاصطناعي على الإنسان في كل مجال معرفي، بذاكرة محسّنة، وسرعة معالجة، وتحليل تفوق قدرة العقل البشري.

ورغم أن امتلاك مثل هذه الآلات الذكية قد يبدو مغريًا، فإن ذلك يثير العديد من التساؤلات الأخلاقية والفلسفية؛ إذ قد يشكل هذا النوع من الذكاء الاصطناعي خطرًا على الجنس البشري إذا لم تتم إدارته بحذر، وهي التساؤلات و المخاوف التي أثارتها مئات الأفلام والكتب التي ناقشت سيناريوهات هيمنة الذكاء الاصطناعي (Dorr, 2022).

ثامنًا: نظم الذكاء الاصطناعي:

للذكاء الاصطناعي (AI) مجموعة واسعة من النظم Systems تشمل على سبيل المثال لا الحصر: النظم الخبيرة Expert Systems، الاستدلال المنطقي Logical Reasoning، تمثيل المعرفة Knowledge Representation، تعلم الآلة Machine Learning، الروبوتات Robots، الرؤية Vision، معالجة الصورة Image Processing، أنظمة التعرف على الكتابة اليدوية والكلام Speech and Handwriting Recognition، فهم اللغات الطبيعية Natural Language Understanding، الشبكات العصبية Neural Networks، النظم متعددة المواهب Multi-Agent Systems، التفاعل بين الشخص والآلة Human-Computer Interaction وغيرها، ونظرا للتعدد والتنوع الكبير لنظم الذكاء الاصطناعي، فسوف نستعرض فيما يلي بالتفصيل أهم نظم الذكاء الاصطناعي المستخدمة في مجال إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي (Sakamoto& Abe, 2023):

1. الأنظمة الخبيرة Expert Systems:

أ. نشأة الأنظمة الخبيرة وتطورها:

بدأت الأنظمة الخبيرة Expert Systems كمجال بحثي في الذكاء الاصطناعي (AI) في الستينيات والسبعينيات؛ إذ تم التركيز على تطوير أنظمة قادرة على محاكاة اتخاذ القرارات البشرية في مجالات محددة، ومن ثم شهد عام **1965** تطوير أول نظام خبير ناجح وهو **DENDRAL** من قبل كل من **إدوارد فيجنباوم Edward Feigenbaum** الباحث الأمريكي في مجال الذكاء الاصطناعي، وعالم الوراثة الأمريكي **جوشوا ليدربيرج Joshua Lederberg** وكلاهما من **جامعة ستانفورد** في **كاليفورنيا**، بالإضافة إلى مجموعة علماء آخرين، وكان هذا النظام الخبير يُستخدم في تحليل البيانات الكيميائية وتحديد بنية الجزيئات، وفي الألفية الجديدة، ومع تقدم الحوسبة ونمو المعرفة في مجال الذكاء الاصطناعي (AI)، شهدت الأنظمة الخبيرة Expert Systems ازدهارًا، حيث تم استخدامها في مجالات أعمال متعددة، مثل الطب والهندسة، وازدادت التطبيقات العملية للأنظمة الخبيرة Expert Systems مما جعلها أكثر شيوعًا في أعمال المؤسسات في مختلف قطاعات الأعمال (Sakamoto & Abe, 2023).

ب. مفهوم الأنظمة الخبيرة:

تعددت وتنوعت تعريفات **النظم الخبيرة (Expert Systems)** بتعدد الباحثين، حيث عرفها (الخوالدة، 2020) بأنها: أنظمة متقدمة جدًا تستخدم أساليب الإنسان الخبير وتدمجها مع خصائص الآلة الذكية باستخدام المنطق والتحليل الرياضي لحل مشكلة ما أو أداء مهمة، ويتم ذلك كما لو أن البرنامج المستعمل لذلك الغرض خبير في المجال، كما عرفت أيضا بكونها برامج حاسوبية متطورة تحتوي المعرفة المرتبطة بحقل معين صممت خصيصًا لتقوم بعمل الخبراء البشريين في مجال معين، حيث تستخدم لأداء عدد كبير من الأعمال المعقدة والتي يمكن أن تؤدى بواسطة عدد من الخبراء المتخصصين، ويتم أداء هذه الأعمال عن طريق محاكاة عمل الخبير البشري الذي يستخدم المعرفة المرتبطة بمجال معين والقواعد العلمية المطلوبة للوصول إلى التوصية أو الاقتراح ومن ثمَّ اتخاذ القرار (إسماعيل والمطيري، 2022).

فالنظم الخبيرة Expert Systems هي إذن مجموعة من البرمجيات الجاهزة المخزن فيها خبرات وتحليلات مجموعة من الخبراء للاستفادة منها في تقديم الاستشارات في مجالات محددة، حيث يعمل النظام الخبير Expert System كمستشار (خبير) في مجال معرفي محدد كالمجالات الطبية والهندسية والاقتصادية، فالنظام الخبير Expert System هو ببساطة برنامج حاسوبي ذكي مصمم لنمذجة معرفة وقدرة الخبير الإنساني على حل المشكلات، حيث يحاكي هذا النظام إجراءات

الخبراء البشريين في التعامل مع المشكلات المعقدة وحلها، ويتمثل الغرض الأساسي من النظم الخبيرة Expert Systems في دعم ومساعدة المستخدمين في عمليات التفكير وليس تزويدهم بالمعلومات، وتعتمد النظم الخبيرة Expert Systems على قواعد البيانات الخاصة بها لاتخاذ القرارات وإنجاز المهام؛ إذ تتميز هذه النظم بأنها تتيح للمتعلم ممارسة المهارات في بيئات تعليمية تفاعلية من خلال الإجابة عن استفساراته وتساؤلاته، وتقديم الإرشاد والتوجيه الفردي له، وإيجاد حلول لمشكلاته التعليمية، فضلاً عما تتميز به من سهولة الاستخدام، وما تقدمه من دعم للتواصل الأكاديمي (Manoharan et al., 2024).

ج. أنواع النظم الخبيرة:

يمكن تصنيف النظم الخبيرة Expert Systems من حيث علاقتها بالمستخدم والأدوار التي تقوم بها الى ثلاثة أنواع رئيسية كما يلي (Nazarian-Jashnabadi et al., 2023):

1. **النظام المساعد Assistant System**:

ويعد هذا النوع من الأنظمة أقل النظم خبرة، حيث يقوم النظام بمساعدة المستخدم في تحليل بعض الأعمال واتخاذ القرار لكنه لا يتخذ القرار بنفسه، بل يعتمد على المستخدم في التوجيه واتخاذ الخطوة النهائية، أي أنه يقدم للمستخدم خيارات وتلميحات أو تحليلات ولا يفرض رأيًا، بل يترك القرار للمستخدم، ومن أمثلة هذه النظم نجد أنظمة أو تطبيقات المساعد الذكي في الهواتف الذكية مثل: **Google Assistant** و**Siri** والتي تقدم معلومات أو تنفذ أوامر بسيطة، وهناك أيضا النظم المساعدة في المكتبات الإلكترونية والتي تقوم باقتراح الكتب، وكذا مساعد تخطيط الدروس للمعلمين والذي يقترح أنشطة وأهداف بناءً على المحتوى.

2. **النظام الزميل Colleague System:**

هو نظام يعمل جنبًا إلى جنب مع المستخدم كأنه "**زميل ذكي**"، حيث يتعاون مع المستخدم بشكل تفاعلي: يقترح حلولاً، يناقشها مع المستخدم، يجيب عن أسئلته، وقد يعدل النظام من حلوله أيضا بناءً على ردود المستخدم، ومن أمثلة هذه النظم لدينا نظم دعم القرار الطبي والتي تقترح علاجات وتعدل اقتراحاتها بناء على رأي الأطباء، كما نجد أيضا نظم التصميم المعماري الذكية التي تساعد المهندسين في اتخاذ قرارات التصميم.

3-النظام الخبير Expert System:

وهو نظام يُفترض أن لديه معرفة عميقة وموسعة في مجال معين وخبرته أفضل من خبرة المستخدم، ومن ثمَّ فهو يتصرف كخبير حقيقي، ويمتلك القدرة على تقديم الاستنتاجات واتخاذ القرارات وإعطاء حلول أو توصيات نهائية، وقد لا يحتاج لتدخل المستخدم إلا لتزويده بالبيانات، ومن ثمَّ يقبل المستخدم نصيحة النظام من دون مناقشة، ومن أهم أمثلة هذه النظم نجد الأنظمة الطبية الذكية المستخدمة في تشخيص أمراض الدم والعدوى مثل نظام (**MYCIN**)، وكذلك أيضا نظم تشخيص أعطال السيارات في الورش الذكية.

2. تعلم الآلة Machine Learning:

أ. نشأة تعلم الآلة وتطوره:

بدأت فكرة تعلم الآلة Machine Learning كمجال بحثي في الذكاء الاصطناعي (AI) في الستينيات والسبعينيات، حيث كان التركيز على تطوير خوارزميات Algorithms تستطيع التعلم من البيانات، ثم شهدت عقود الثمانينيات والتسعينيات تطورات كبيرة في المفاهيم والخوارزميات، مثل خوارزميات الانحدار Regression Algorithms وخوارزميات التصنيف Classification Algorithms، حيث تم استخدام التقنيات الإحصائية لتحسين تقنيات التعلم من البيانات، وفي القرن الحالي ومع زيادة كم وجودة البيانات المتاحة وتطور الحوسبة، أصبح تعلم الآلة MLأكثر شيوعًا، وتم استخدامه في مجموعة متنوعة من التطبيقات؛ مما أدى إلى ظهور مجالات جديدة، مثل التعلم العميق Deep Learning Sarker, (2023).

ب. مفهوم تعلم الآلة:

يعرف تعلم الآلة ML بأنه: فرع من الذكاء الاصطناعي يتضمن بناء نماذج حاسوبية قادرة على التعلم والتنبؤ واتخاذ قرارات مستقلة اعتمادًا على البيانات المقدمة لها، وتعمل هذه النماذج على تحسين دقتها باستمرار من خلال البيانات المكتسبة (Kufel et al, 2023)، كما عرفه Tom Mitchell بكونه: دراسة الخوارزميات التي تسمح لبرامج الحاسب بالتعلم تلقائيًا وتحسين أدائها من خلال الخبرة، كما أنه يوفر للأنظمة القدرة على التعلم تلقائيًا وتحسين الأداء من خلال الخبرة دون أن يتم برمجتها صراحةً (Shyam & Chakraborty, 2021)، ومن ثم فإن تعلم الآلة هو فرع من الذكاء الاصطناعي يركز على تطوير الخوارزميات والنماذج والأنظمة التي تسمح للآلات بالتعلم من البيانات واكتساب الخبرة وتحسين أدائها بمرور الوقت دون الحاجة إلى برمجة صريحة، بهدف تمكين الأنظمة من التعرف على الأنماط والعلاقات بنفسها والتنبؤ بالنتائج أو اتخاذ القرار بناءً على البيانات السابقة (Mosqueira-Rey et al., 2023).

ج. مكونات تعلم الآلة:

يقوم تعلم الآلة Machine Learning على أربع مكونات أساسية، تبدأ **بالبيانات** Data التي تُستخدم لتدريب وتعليم النماذج Models، وتأتي من مصادر متنوعة كقواعد البيانات المختلفة، وشبكة الإنترنت، والأجهزة الذكية وتشمل النصوص، والصور، والجداول. يليها **الخوارزميات** Algorithms التي تمثل الطريقة التي يتعلم بها النموذج Model وتشمل التعلم الموجّه Supervised Learning Algorithms ، وشبه الموجّه Semi-supervised Learning Algorithms، وغير الموجّه Algorithms unsupervised Learning، إضافة إلى التعلم المعزز Reinforcement Learning Algorithms الذي يعتمد على نظام المكافآت. أما **النموذج** Model فهو الوحدة التي تتعلم من البيانات Data باستخدام الخوارزميات ويتم اختبارها لضمان الدقة Accuracy والفاعلية Effectiveness. وأخيرًا، يتحدد أداء النموذج عبر **التقييم** Evaluationباستخدام بيانات لم يسبق له رؤيتها، اعتمادًا على مقاييس مثل الدقة والاستدعاء، مع تحسين النموذج عبر إدارة البيانات وتهيئتها بشكل فعّال (Mosqueira-Rey et al., 2023) .

3. التعلم العميق Deep Learning:

أ. نشأة وتطور التعلم العميق:

شهد العقد الأول من القرن الحادي والعشرين بداية ظهور التعلم العميق Deep Learning بشكل فعلي، في حين تعود جذوره إلى السبعينيات حين تم اقتراح الشبكات العصبية الاصطناعية Artificial Neural Networks – ANN، ومع ذلك فإن التطور الحقيقي لهذا المجال جاء نتيجة للعديد من العوامل، كان أهمها (Ahmed, et al., 2023):

1. توفر كميات ضخمة من البيانات Big Data
2. التطور في قدرات الحوسبة Computational Power
3. تحسين الخوارزميات Algorithmic Innovations
4. تصميم هياكل متقدمة للشبكات العصبية
5. انتشار المصادر المفتوحة والمجتمع العلمي
6. ارتفاع الطلب على التطبيقات الذكية

ب. مفهوم التعلم العميق:

عرَّف Kumar Arvind التعلم العميق Deep Learning بأنه: تلك التقنية التي تحاول تقليد ومحاكاة الطريقة التي يعمل بها العقل البشري في جميع قدراته، مثل: الرؤية، وفهم الحديث وتكوينه، والسمع، وغيرها من القدرات القوية التي يتمتع بها العقل البشري، وذلك من خلال خوارزميات وبرامج مستوحاة من الدراسات الطبية والعصبية الخاصة بالإنسان وتحاول قدر الإمكان أن تقلدها ولكن من خلال طرق حاسوبية لا بيولوجية، حيث يتم استبدال الخلايا العصبية في العقل

البشري بالخلايا العصبية الاصطناعية (حسن، 2025)، كما عرف التعلم العميق بأنه: فرع من فروع تعلم الآلة يهدف إلى تطوير نموذج يطابق مستوى الدماغ البشري في حل المشكلات المعقدة في العالم الحقيقي من خلال الاستفادة من الشبكات العصبية الاصطناعية والتعلم المحاكي (Aggarwal et al, 2022).

إذن؛ فالتعلم العميق Deep Learning هو إحدى تقنيات تعلم الآلة Machine Learning التي تعتمد على استخدام الشبكات العصبية الاصطناعية متعددة الطبقات Deep Neural Networks لمحاكاة طريقة معالجة المعلومات في الدماغ البشري، وهي التقنية التي تتميز بقدرتها على استخلاص الميزات أو الخصائصFeatures والأنماط المعقّدة والتعلم من البيانات الخام غير المنظمة مثل الصور والنصوص والصوت، دون الحاجة إلى تدخل بشري كبير في تحديد أو اختيار الميزات أو الخصائص Features (Tapeh & Naser, 2023).

ج. مكونات التعلم العميق:

يعتمد **التعلم العميق** Deep Learning على مجموعة مكونات أساسية تعمل معًا لبناء نموذج فعّال، تبدأ بـ**معالجة البيانات** Processing Data من خلال التطبيع Normalization والترميز Encoding وتقسيمها إلى بيانات تدريب Training Data، وبيانات تحقق Validation Data، وبيانات اختبار Test Data. ويعتمد النموذج على **الشبكات العصبية الاصطناعية** Artificial Neural Networks المكوّنة من طبقات الإدخال، والطبقات المخفية التي تعالج البيانات، وطبقة الإخراج التي تنتج التوقع النهائي. وتعدّ **الخلايا العصبية** Neurons أو العُقَد Nodes وحدات المعالجة الأساسية التي تطبّق أوزانًا وانحيازات محددة Weights and Biases على المدخلات قبل تمريرها عبر **دوال التنشيط** Activation Functions لإضافة اللاخطية وتعلّم الأنماط المعقدة. ويُقاس أداء النموذج باستخدام **دوال الخسارة** Loss Functions التي تقارن النتائج الفعلية والمتوقعة، بينما تعمل **خوارزميات التحسين** Optimization Algorithms على تعديل الأوزان وتقليل الخسارة لتحقيق أفضل أداء للنموذج (Ahmed et al., 2023).

4. الذكاء الاصطناعي التوليدي Generative AI:

أ. نشأة الذكاء الاصطناعي التوليدي:

بدأ الذكاء الاصطناعي التوليدي Generative AI في أوائل القرن الحادي والعشرين اعتمادًا على نماذج تعلم الآلة المبكرة Machine Learning مثل الشبكات العصبية التكرارية (RNNs) وذلك لإنتاج نصوص بسيطة. وشهد هذا المجال نقلة نوعية عام 2014 مع طرح **الشبكات التوليدية المتعارضة (GANs)** التي مكّنت من توليد صور واقعية باستخدام التعلم العميق Deep Learning ، مما زاد الاهتمام بقدرات الذكاء التوليدي على ابتكار محتوى جديد. وتواصل التطور مع ظهور **نماذج المحولات (Transformers)** عام 2017 من باحثيGoogle ، و هي النماذج التي أحدثت ثورة في فهم اللغة وتوليد النصوص والصور. وبعد عام 2020 انتقل الذكاء التوليدي إلى الاستخدام التجاري الواسع في مجالات مثل التعليم، الترفيه، البرمجة، التصميم، والتسويق، وأصبح جزءًا من الأدوات اليومية مثل **ChatGPT** و **Midjourney** وغيرها (Feuerriegel et al., 2024).

ب. مفهوم الذكاء الاصطناعي التوليدي:

يقصد بالذكاء الاصطناعي التوليدي Generative AI تقنيات الحاسب الآلي القادرة على توليد محتوى جديد وذي مغزى، مثل النصوص أو الصور أو الأصوات بالاعتماد على بيانات التدريب (Feuerriegel et al., 2024)، بالإضافة إلى ذلك تتيح الأشكال المتنوعة للمحتوى الذي تم إنشاؤه من الذكاء الاصطناعي التوليدي Generative AI مجموعة واسعة من التطبيقات، مثل القصائد والبيانات السياسية والأوراق الأكاديمية (Hu, 2023)، والتي يكون من الصعب التمييز بينها وبين

المحتوى الذي ينشئه البشر (Nah et al, 2023)، ومن ثمَّ فالذكاء الاصطناعي التوليدي Generative AI يركز على إنشاء وتوليد محتوى جديد وأصلي باستخدام خوارزميات ذكية بناءً على البيانات المدخلة، ويتنوع المحتوى المنتج من أنظمة الذكاء الاصطناعي التوليدي Generative AI ليشمل النصوص، والصور، والفيديوهات، والموسيقى، والصوت، وحتى الأكواد البرمجية، وبطريقة تشبه ما ينتجه البشر، وذلك استنادًا إلى الأنماط التي تعلمتها من البيانات المدخلة، وعلى عكس الذكاء الاصطناعي التقليدي AI، الذي يركز على تحليل البيانات واتخاذ القرارات، فالذكاء الاصطناعي التوليدي Generative AI يهدف إلى الإبداع وإنتاج شيء جديد (Feuerriegel et al., 2024).

ج. مكونات الذكاء الاصطناعي التوليدي:

يتكون **الذكاء الاصطناعي التوليدي** Generative AI من عدة مكونات رئيسية تمكّنه من إنتاج محتوى جديد وواقعي. ويبدأ ذلك **بنماذج التعلم العميق** Deep Learning Models و تشمل الشبكات التوليدية التنافسية - Generative Adversarial Network GANs المكوّنة من المولد Generator والمميز Discriminator ، والشبكات العصبية التكرارية Recurrent Neural Network-RNNs لإنشاء السلاسل النصية، ونماذج **المحولات** Transformers مثل GPT المستخدمة في توليد النصوص، إضافة إلى الشبكات **العصبية الترشيحية** Convolutional Neural Network-CNN لتوليد الصور والفيديو . ويعتمد الذكاء التوليدي على **البيانات الضخمة** Big Data بوصفها الوقود الذي يوفّر للنماذج القدرة على تعلّم الأنماط عبر نصوص وصور وأصوات متنوعة. كما يقوم على **خوارزميات التدريب** التي تشمل تنظيف البيانات، ثم التكرار والتحسين باستخدام تقنيات مثل التعلم غير الموجّه، والتعلم المعزز، ونقل التعلم. وبعد التدريب، تُختبر النماذج وتُحسّن عبر **التقييم والضبط الدقيق** من خلال اختبارها على بيانات جديدة، وتخصيصها لقطاعات أو لغات معينة، وذلك باستخدام مقاييس التنوع والواقعية والتغذية الراجعة البشرية، إضافة إلى خوارزميات التحسين لضبط الأوزان وتحسين جودة المخرجات (Banh & Strobel, 2023).

5. معالجة اللغات الطبيعية Natural Language Processing:

أ. نشأة وتطور معالجة اللغات الطبيعية:

بدأت **معالجة اللغات الطبيعية** Natural Language Processing - NLP في الستينيات والسبعينيات مع التركيز على الترجمة الآلية باستخدام تقنيات بسيطة تعتمد على القواعد المكتوبة يدويا فيما كان يعرف بالأساليب الرمزية Rule-Based Systems. ومع تطور الحوسبة في الثمانينيات والتسعينيات، ظهرت خوارزميات قادرة على التعلم من البيانات النصية بدلاً من الاعتماد على القواعد اليدوية فقط، مما حسّن مهام مثل Text Classification و Sentiment Analysis والترجمة. وفي العقد الثاني من القرن الحادي والعشرين أحدث Deep Learning تحولًا جذريًا عبر نماذج مثل الشبكات العصبية التكرارية RNNs والمحولات Transformers، التي حسّنت فهم السياق وتوليد النصوص. وشهد عام 2018 صعود ما بات يُعرف باسم نماذج اللغة الكبيرة Large Language Models - LLM ومن أمثلتها: نموذج BERT من Googleونموذج GPT من OpenAI والتي تعتمد على بنية المحولات Transformers وهي النماذج التي حققت قفزات كبيرة في دقة الفهم والتوليد، وأصبحت الأساس لتطبيقات مثل المساعدات الافتراضية، الترجمة الفورية، تحليل النصوص، والمحادثات التفاعلية (Fanni et al., 2023).

ب. مفهوم معالجة اللغات الطبيعية:

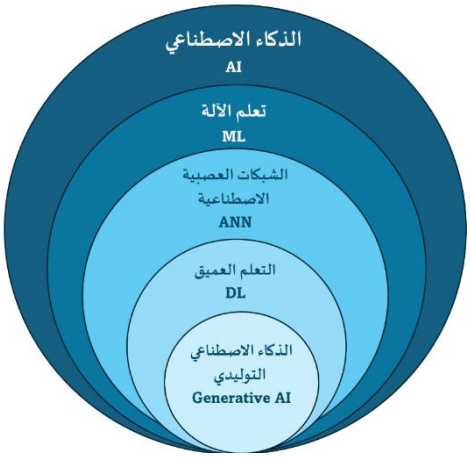
يُعرِّف (Xu et al, 2024) معالجة اللغة الطبيعية **NLP** على أنها التقنية التي تمكن أجهزة الحاسب الآلي من فهم وتفسير وتوليد اللغة البشرية، ومن ثم تعمل على سد الفجوة بين التواصل البشري وفهم الحاسب الآلي؛ مما يسهل التفاعلات الأكثر طبيعية بين البشر والآلات، بينما يعرفها (Jerfy, Selden & Balkrishnan , 2024) بأنها فرع من فروع الذكاء الاصطناعي يركز على التفاعل بين أجهزة الحاسب الآلي والبشر من خلال اللغة الطبيعية، وهي تنطوي على قدرة أجهزة

الحاسب على فهم وتفسير وتوليد اللغة البشرية بطريقة ذات معنى ومفيدة، وتشمل معالجة اللغة الطبيعية مهامًا مختلفة، مثل: الترجمة الآلية، وتحليل المشاعر، واستخراج المعلومات من بين أمور أخرى، ويتمثل هدف معالجة اللغة الطبيعية في تمكين الآلات من معالجة وتحليل كميات كبيرة من بيانات اللغة الطبيعية بشكل فعال، ومن ثمَّ تسهيل التواصل والتفاهم بشكل أفضل بين البشر وأجهزة الحاسب.

فمعالجة اللغات الطبيعية NLP إذن هي ذلك الفرع من الذكاء الاصطناعي AI الذي يركز على تمكين الآلات من فهم، ومعالجة، وتحليل، وتوليد اللغة البشرية بشكل طبيعي وذكي، والتفاعل مع النصوص أو الأصوات المنطوقة بالطريقة نفسها التي يتعامل بها الإنسان مع اللغة؛ بهدف سد الفجوة بين الإنسان والآلة، مما يتيح للأنظمة الحاسوبية التفاعل مع المستخدمين بطرق طبيعية (Fanni et al., 2023).

ج. مكونات معالجة اللغات الطبيعية (Khurana et al., 2023):

تتكوّن أنظمة **معالجة اللغات الطبيعية** (NLP) من عدة مكوّنات أساسية تمكّن الحاسوب من فهم اللغة البشرية وتحليلها. وتشمل أولًا **التحليل اللغوي** (Language Analysis) بمستوياته المختلفة Morphological Analysis لدراسة بنية الكلمات، و Syntactic Analysis لتحليل تركيب الجمل، و Semantic Analysis لفهم المعاني، و Pragmatic/Context Analysis لتفسير المقصود وفق السياق. ويلي ذلك دور تعلم الآلة Machine Learning الذي يسمح للنماذج بتعلّم الأنماط اللغوية من البيانات عبر نماذج إحصائية مثل نموذج ماركوف المخفي HMM و ونموذج الانحدار اللوجستي Logistic Regression، وتقنيات التعلم العميق Deep Learning مثل الشبكات العصبية التكرارية RNNs والمحولات Transformers لفهم أعمق للسياق. كما تُعد معالجة النصوص Text Processing خطوة أساسية في أنظمة **معالجة اللغات الطبيعية** (NLP) وتشمل مرحلتين هما تنظيف البيانات Data Cleaning لتنظيف النصوص وإزالة الضوضاء وتوحيد الصيغ، و تحويل النص إلى بيانات رقمية Text-to-Numerical Conversion لتحويل الكلمات إلى تمثيلات عددية باستخدام تقنيات مثل تمثيل الكلمات Word Embedding، مما يمكّن الخوارزميات من تحليل النصوص بكفاءة أعلى.



شكل رقم (4): العلاقة بين بعض أنظمة الذكاء الاصطناعي
المصدر: شكل معدل من الباحث بناء على مصادر الدراسة

6. رؤية الحاسب Computer Vision:

أ. نشأة وتطوررؤية الحاسب:

بدأت رؤية الحاسب Computer Vision كمجال بحثي مستقل في أواخر الستينيات وبداية السبعينيات، وكان التركيز في البداية على معالجة الصور الثابتة، حيث تم استخدام تقنيات بسيطة لتفسير الصور، وفي الثمانينيات ازداد الاهتمام

بتطوير خوارزميات متقدمة لمعالجة الصور، مثل تحليل الصور باستخدام الشبكات العصبية ANN، وشهدت فترة التسعينيات تقدمًا كبيرًا في التكنولوجيا؛ مما أسهم في تطوير أنظمة رؤية الحاسب Computer Vision، وتم استخدام تقنيات تعلم الآلة Machine Learning لتحسين أداء النماذج، وفي القرن الحادي والعشرين ومع ظهور التعلم العميق Deep Learning، تغيرت رؤية الحاسب Computer Vision بشكل جذري، واستخدمت الشبكات العصبية الترشيحية CNNs بشكل واسع لتحسين دقة معالجة الصور (Paulin, & Ivasic-Kos, 2023).

ب. مفهوم رؤية الحاسب:

تعرف رؤية الحاسب Computer Vision بأنها: ذلك الفرع من فروع الذكاء الاصطناعي الذي يسمح لأجهزة الحاسب وأنظمته باستخراج معلومات مفيدة من الصور الرقمية ومقاطع الفيديو وغيرها من المدخلات المرئية والتصرف أو تقديم توصيات بناءً على تلك البيانات، ومن وجهة نظر هندسية تهدف رؤية الحاسب Computer Vision إلى فهم وأتمتة العمليات التي يكون النظام البصري البشري قادرًا على القيام بها، ونتيجة لذلك يتعلق الأمر بالاستخراج الآلي وتحليل وفهم المعلومات ذات الصلة من صورة واحدة أو سلسلة من الصور (Krizhevsky, Sutskever & Hinton, 2023)، في حين عرفها (Che et al, 2024) بأنها: عملية محاكاة الملاحظة البصرية البشرية واستخدام أجهزة الحاسب لتحليل الصور، والتي تتطلب من الحاسب أن يكون لديه القدرة على إدراك البيئة المحيطة من خلال الصور ومحاكاة عملية الرؤية البشرية المحددة لتحقيق المعالجة الذكية للصور ذات الصلة.

ولذلك فإن رؤية الحاسب Computer Vision تهدف إلى تمكين الآلات من "رؤية" وفهم وتحليل المحتوى المرئي، مثل الصور والفيديوهات، بالطريقة نفسها التي يرى ويحلل بها البشر الصور والفيديوهات، وهو ما يشمل التعرف على الأشكال والألوان والحركات، بل وفهم السياق والمعاني، وبعبارة أخرى فإن رؤية الحاسب Computer Vision تمكن الآلة من فهم وتحليل الصور الرقمية من أجل اتخاذ قرارات أو تنفيذ مهام معينة بشكل تلقائي (Basheer et al.,2023).

ج. مكونات رؤية الحاسب:

تتكوّن **رؤية الحاسب** Computer Vision من عدة مراحل أساسية تبدأ بمرحلة التقاط الصورة Image Acquisition عبر الكاميرات والمستشعرات لتحويل البيانات الضوئية إلى بيانات رقمية تسمى مصفوفات البيكسل Pixel Matrices تليها مرحلة المعالجة المسبقة للصورة Preprocessing لتحسين جودة الصور باستخدام تقنيات مثل تصفية الصور Filtering، والتحويلات الهندسية Geometric Transformations والتدوير أو القص وتحديد الحواف Edge Detection وتحليل الكائنات وغيرها. ثم يتم تحديد الخصائص المميزة في الصورة مثل: الحواف Edges، الزوايا Corners، الكتل Blobs، الألوان Colors، **الأنماط** Textures. ويأتي بعد ذلك دور التصنيف والتعرف على الأنماط Classification & Pattern Recognition باستخدام خوارزميات تعلم الآلة Machine Learning أو التعلم العميق Deep Learning للتعرف على الأشياء أو المشاهد، و يشمل ذلك تحليل المشهد و معالجة الصور عالية المستوى High-Level Processing حيث يتم فهم العلاقات بين الكائنات في الصورة من خلال تنفيذ مهام مثل: تجزئة الصورة Image Segmentation، التعرف على الوجوه Face Recognition، تتبع الحركة Object Tracking في الفيديو، وغيرها. وأخيرًا تُستخدم النتائج في اتخاذ القرار Decision Making لاتخاذ قرارات مثل التعرف على الوجوه أو تفسير إشارات المرور في المركبات ذاتية القيادة . (Basheer et al., 2023)

7. أتمتة العمليات الروبوتية Robotics Process Automation - RBA:

أ. **نشأة وتطور أتمتة العمليات الروبوتية:**

بدأت أتمتة العمليات الروبوتية RPA في الظهور كمفهوم مرتبط بتقنيات الأتمتة الصناعية في السبعينيات، حيث تم استخدام الروبوتات Robots في المصانع لأداء مهام متكررة ومرتبطة بالإنتاج، ثم تطورت تقنيات البرمجيات وأصبح من الممكن استخدام الروبوتات Robots في أتمتة المهام المكتبية والإدارية، مما أتاح تحسين الكفاءة، وأطلق مفهوم أتمتة العمليات الروبوتية RPA بشكل رسمي في أوائل العقد الأول من القرن الحادي والعشرين، مع تطوير أدوات برمجية متخصصة تسمح بتطوير الروبوتات البرمجية في مختلف القطاعات في الحياة (Koppisetti, 2024).

ب. مفهوم أتمتة العمليات الروبوتية:

تعرف (Hsiung & Wang, 2022) أتمتة العمليات الروبوتية (RPA) بأنها: تقنية قائمة على برمجيات روبوتية تحاكي الإجراءات البشرية لتنفيذ العمليات المتكررة القائمة على القواعد، من خلال واجهات المستخدم الخاصة بهم تمامًا كما يفعل المستخدم البشري، كما عرفت أيضا بكونها: التقنية التي تتيح للمؤسسات أتمتة المهام الرتيبة المتكررة والقائمة على القواعد، من خلال محاكاة تصرفات المستخدم البشري، ومن ثمَّ تحرير وتفريغ الموارد البشرية للقيام بالأنشطة الإستراتيجية والأعلى قيمة (Bhardwaj, 2023)، وتعتمد هذه التقنية على إنشاء روبوتات برمجية Bots يمكنها التفاعل مع التطبيقات والأنظمة الرقمية بطريقة الإنسان نفسها؛ مما يتيح أتمتة المهام الروتينية (Koppisetti, 2024).

ج. مكونات أتمتة العمليات الروبوتية:

تتكوّن **أتمتة العمليات الروبوتية** (RPA) من عدة عناصر أساسية، تبدأ بالروبوتات **البرمجية** Bots وهي برمجيات تنفّذ مهام محددة مثل إدخال البيانات وإرسال البريد الإلكتروني وتحليل المعلومات. وتعتمد هذه الروبوتات على **واجهات المستخدم** User Interfaces للتفاعل مع التطبيقات دون تعديل الأنظمة. كما تُطوَّر باستخدام **أدوات البرمجة** Development Tools مثل UiPath و Blue Prism وAutomation Anywhere، التي توفّر بيئات تطوير مرئية لتطوير الروبوتات البرمجية Bots. وأخيرًا تُستخدم قواعد البيانات Databases لتخزين البيانات التي تجمعها أو تعالجها الروبوتات، مما يسهّل الوصول إليها وتحليلها (Herm et al, 2023).

تاسعًا: مؤشرات قياس أداء الذكاء الاصطناعي:

مع تزايد الاعتماد على أنظمة الذكاء الاصطناعي (AI) في مختلف المجالات، باتت الحاجة إلى قياس فاعلية هذه الأنظمة والتقنيات أمرًا ضروريًا لتقييم أدائها، وضمان تحقيق الأهداف المرجوة منها، وكذا تحديد المجالات التي تحتاج إلى تحسين وتطوير (Naser & Alavi, 2021). وفيما يلي نناقش أهم مؤشرات قياس أداء الذكاء الاصطناعي AI Performance Metrics.

1. مفهوم مؤشرات قياس أداء الذكاء الاصطناعي:

تعرف مؤشرات قياس الذكاء الاصطناعي بأنها: أدوات أو مقاييس تستخدم لتقييم أداء الأنظمة الذكية، تشمل هذه المؤشرات مجموعة من المعايير التي تحدد مدى فاعلية وكفاءة النظام في تحقيق المهام الموكلة إليه، وتهدف هذه المؤشرات إلى توفير فهم شامل لكيفية عمل النظام، ومدى دقته، وملاءمته للغرض المستخدم من أجله (Bandi et al. 2023).

2. أهمية مؤشرات قياس أداء الذكاء الاصطناعي:

تُشكل مؤشرات قياس أداء الذكاء الاصطناعي أساسًا علميًا صلبًا وواقعيًا لإدارة مشاريع الذكاء الاصطناعي بنجاح، وبدونها تصبح عملية تطوير نماذج وتقنيات الذكاء الاصطناعي محض تخمين غير مدعوم بأدلة، ويمكن تلخيص أهمية مؤشرات قياس الذكاء الاصطناعي فيما يلي (Bandi et al. 2023):

أ. **ضمان الجودة والأداء:** حيث تساعد في تقييم دقة وفاعلية النماذج وموثوقيتها، والكشف عن الأخطاء والتحيزات المحتملة بها، وتحسين كفاءة الخوارزميات.

ب. **اتخاذ القرارات المستنيرة:** حيث إن هذه المؤشرات تقوم بتوفير معايير كمية للمقارنة بين النماذج، وتحديد أفضل خوارزمية للمهمة المطلوبة، وتقييم الجدوى الاقتصادية للحلول الذكية.

ج. **التطوير المستمر وتحسين الأنظمة: إذ تسهم** هذه المؤشرات في التعرف على نقاط الضعف في الأنظمة؛ مما يساعد على تحسينها وتوجيه عملية ضبط المعاملات Hyperparameter Tuning، ومتابعة تطور الأداء مع تحديث البيانات.

د. **ضمان التكامل مع الأعمال:** ويتم ذلك من خلال ربط الأداء الفني بالنتائج العملية، وتحديد العائد على الاستثمار ROI، وإثبات القيمة المضافة للجهات المعنية.

هـ. **تيسير الابتكار:** من خلال قياس الأداء يمكن تطوير حلول جديدة ومبتكرة في مجال الذكاء الاصطناعي.

و. **الامتثال والمعايير الأخلاقية:** وذلك من خلال قياس العدالة وغياب التحيزFairness والتحقق من احترام الخصوصية، وضمان الشفافية وقابلية التفسير، حيث هذه المؤشرات تتيح للمستخدمين فهم كيفية عمل الأنظمة واتخاذ القرارات بناءً على البيانات.

ز. **تحقيق الثقة والاعتمادية:** بناء ثقة المستخدمين في الأنظمة الذكية، وتلبية متطلبات الجهات التنظيمية، وتقليل المخاطر التشغيلية.

3. أهم مؤشرات قياس أداء الذكاء الاصطناعي:

أ. مؤشر قياس الدقة Accuracy Measuring Index:

هو مؤشر يقيس مدى صحة التنبؤات التي يقدمها نظام الذكاء الاصطناعي عبر قياس نسبة التنبؤات الدقيقة إلى إجمالي التنبؤات، ويستخدم بشكل شائع في مهام التصنيف، مثل تصنيف الصور أو النصوص، وفي القطاع المصرفي يُستخدم في أنظمة تصنيف القروض لتحديد ما إذا كان العميل مؤهلاً للحصول على قرض أم لا (Agarwal& Agarwal, 2023).

ب. مؤشر قياس الاستدعاء Recall Measuring Index:

يستخدم لقياس نسبة التنبؤات الصحيحة للفئة الإيجابية إلى إجمالي العناصر الحقيقية في تلك الفئة في التطبيقات التي تتطلب تحديد جميع الحالات الإيجابية، مثل الكشف عن الاحتيال (Agarwal& Agarwal, 2023).

ج. مؤشر قياس معدل الخطأ Error Rate Measuring Index:

يستخدم في قياس نسبة التنبؤات الخاطئة إلى إجمالي التنبؤات، وتستخدم هذه النسبة لتقييم فاعلية النموذج في مهام التنبؤ، مثل تقييم فاعلية نماذج تعلم الآلة في المعاملات المالية (Nzeako et al., 2024).

د. مصفوفة الالتباس Confusion Matrix:

تُستخدم لتلخيص أداء نموذج التصنيف من خلال عرض عدد التنبؤات الصحيحة والخاطئة لكل فئة، حيث توفر نظرة شاملة على أداء النموذج؛ مما يساعد في تحسينه، وتستخدم في العديد من المجالات، من أهمها استخدامها في تقييم أنظمة التصنيف الائتماني (Behiry & Aly, 2024).

هـ. مؤشر التحليل التنبؤي Predictive Analytics Index :

يقيس مؤشر التحليل التنبؤي القدرة على التنبؤ بالأحداث المستقبلية بناءً على البيانات التاريخية، ويُستخدم في التنبؤ بالطلب مثل التنبؤ بالطلب على الخدمات المصرفية (Nzeako et al., 2024).

و. مؤشر تأثير التكلفة Cost Impact Index:

يقيس مدى تأثير تطبيقات الذكاء الاصطناعي على تقليل التكاليف التشغيلية، ويمكن أن يُستخدم لتقييم فاعلية أتمتة العمليات الروبوتية في تقليل النفقات (Behiry & Aly, 2024).

عاشرًا: التحديات والعواقب المصاحبة لتبني الذكاء الاصطناعي:

رغم ما قدمه الذكاء الاصطناعي حتى الآن، وما سيواصل تقديمه في المستقبل، من فوائد جمة، إلا أنه يطرح أيضًا العديد من التحديات المحتملة، سواء كانت تقنية أو أمنية أو اجتماعية أو اقتصادية أو إنسانية أو قانونية؛ ولذلك فكلما أسرعنا بالتفكير في ماهية هذه التحديات، كنا أكثر قدرة على الحد من مخاطرها وإدارتها بشكل فعال، وتمكننا – كأفراد ومنظمات أعمال وحكومات - من تسخيره بمسؤولية. وفيما يلي نستعرض أهم هذه التحديات المصاحبة لتبني الذكاء الاصطناعي بشكل عام:

أ. مشكلات التحيز والتمييز في أنظمة الذكاء الاصطناعي:

تعاني أنظمة الذكاء الاصطناعي من بعض التحيزات الناتجة عن البيانات والتصميم؛ مما يؤدي إلى اتخاذها لقرارات غير عادلة وتمييزية أحيانا ضد بعض الفئات المجتمعية، خاصة في مجالات مثل مجالات العدالة الجنائية والتوظيف والرعاية الصحية (Ferrer et al., 2020) .

ب. فقد المهارات والمواهب البشرية والاعتماد المفرط على الذكاء الاصطناعي:

تثور العديد من المخاوف المسوغة من أن يؤدي الاعتماد المفرط للأفراد ومنظمات الأعمال على أنظمة وتقنيات الذكاء الاصطناعي إلى فقدان وتآكل المهارات والمواهب البشرية، خصوصًا في المجالات التعليمية والمهنية، حيث يُستبدل التفكير النقدي البشري بأنظمة تقنية تعتمد على أنماط بيانات سابقة (Ivanov, 2023).

ج. مخاطر الخصوصية والأمن السيبراني:

تعاني أنظمة الذكاء الاصطناعي من مشكلات فيما يتعلق بالأمان والخصوصية، وهذه المشكلات يمكن استغلالها من قبل المجرمين لاستهداف بيانات حساسة وتسريبها أو استغلالها، أو التأثير في مخرجات الأنظمة أو اختراقها والسيطرة عليها، وهو ما يشكل بدوره تهديدًا كبيرًا للأفراد ومنظمات الأعمال والحكومات وللمجتمعات بأكملها على مستوى الأمن السيبراني (Oseni et al., 2021).

د. الآثار السلبية على البيئة:

يتطلب تدريب نماذج الذكاء الاصطناعي الحديثة استهلاكًا هائلاً لكميات كبيرة من الطاقة، وهو ما يفاقم من البصمة الكربونية، ومن ثمَّ يترك آثارًا سلبية غير مستحبة على البيئة (Zhuk, 2023).

هـ. انخفاض الشفافية وصعوبة تفسير القرارات:

تعد من أخطر التحديات المرتبطة بأنظمة وتقنيات الذكاء الاصطناعي؛ ففي هذا الإطار نجد أن العديد من خوارزميات الذكاء الاصطناعي – ومن أمثلتها نماذج التعليم العميق Deep Learning Models - تتخذ قرارات يصعب على البشر تفسيرها، وهو ما يعرف أحيانا بظاهرة الصندوق الأسود Black Box، مما يحد من شفافية هذه النظم، ويضعف الثقة في استخدامها، خاصة في بعض المجالات الحيوية التي تمس حياة البشر مباشرة، مثل مجالات التعليم والرعاية الصحية(Ivanov, 2023) .

و. تهديد سوق العمل وزيادة البطالة:

أظهرت الدراسات المتخصصة في سوق العمل ومستقبل الوظائف أن التوجه الكبير نحو تبني نظم وتقنيات الذكاء الاصطناعي سيؤدي إلى أتمتة عدد كبير من الوظائف؛ مما يهدد بتقليص فرص العمل المتاحة للقوى العاملة البشرية، ويرفع احتمالات البطالة، خاصة في القطاعات ذات الطابع الوظيفي الروتيني أو القابل للأتمتة بسهولة (Chui et al., 2021).

ز. مخاطر الحروب والتسلح:

يشكل التوجه السائد نحو توظيف الذكاء الاصطناعي في الأنظمة العسكرية خطرًا كبيرًا غير مسبوق على البشرية والأمن والسلم الدوليين، خاصة مع التوجهات المتزايدة نحو تطوير أسلحة ذاتية التحكم، والتي لا تعمل وفق أي أطر إنسانية أو أخلاقية، وهو ما يزيد من احتمالات الاستخدام غير الأخلاقي أو العشوائي للقوة (Altmann & Sauer, 2020).

ح. التأثيرات السلبية على اتخاذ القرار الإنساني:

يتزايد القلق من تقليل الدور الذي يلعبه الإنسان في اتخاذ قرارات حاسمة، مثل القرارات ذات الصلة بالقبول الجامعي أو التشخيص الطبي، بسبب الاتجاه المتزايد إلى الاعتماد على أنظمة الذكاء الاصطناعي في اتخاذ مثل هذه القرارات، وهذا الاتجاه يمكن أن يحول دور الإنسان إلى مجرّد منفّذ؛ مما يؤدي إلى التدهور في جودة هذه القرارات والتي تتطلب مرونة إنسانية لا تمتع بها أنظمة وتقنيات الذكاء الاصطناعي (Castelo, Bos, & Lehmann, 2022).

ط. اتساع الفجوة الرقمية بين الدول والمجتمعات:

يعزز الاعتماد المتزايد على الذكاء الاصطناعي من اتساع الفجوة الرقمية بين الدول المتقدمة من ناحية وتلك النامية من ناحية أخرى؛ إذ تتركز الاستثمارات والبحوث والبيانات الخاصة بالذكاء الاصطناعي لدى الشركات الكبرى والدول الغنية، مما يؤدي إلى تهميش المجتمعات الفقيرة وحرمانها من الاستفادة الحقيقية من هذه الأنظمة والتقنيات (Eubanks, 2021).

ي. انتهاك حقوق الملكية الفكرية:

تواجه الأوساط الأكاديمية والفنية خاصة، والإبداعية عامة، تهديدًا حقيقيًا وتحديا غير مسبوق بشأن حقوق الملكية الفكرية عند استخدام نماذج وتقنيات الذكاء الاصطناعي في مختلف مجالات الإنتاج الإبداعي، مثل الكتابة أو التصميم أو الموسيقى؛ ففي هذا السياق لا يزال الجدل قائمًا حول من يملك هذه الأعمال بشكل فعلي، هذا من جانب ومن جانب آخر نجد أن نظم ونماذج الذكاء الاصطناعي تعتمد كثيرًا في إنتاجها على نصوص وأعمال إبداعية حالية وسابقة دون الحصول على إذن من أصحابها الحقيقيين، ومن ثمَّ فهذا الاستخدام غير المصرح به يثير قضايا قانونية وأخلاقية حول حقوق المؤلف والملكية الفكرية (Elgammal et al., 2021).

ويرى الباحث أنه على الرغم من التحديات المرتبطة باستخدام أنظمة وتقنيات الذكاء الاصطناعي، فإن ما تقدمه هذه التقنيات من فوائد جوهرية وتطورات مستقبلية واعدة يظل واقعًا لا يمكن إنكاره أو التقليل من أهميته. وبناءً على ذلك، يصبح التعامل مع تلك التحديات ضرورة تتطلب تبنّي إستراتيجيات شاملة تبدأ بسنّ تشريعات واضحة تنظّم الاستخدام وتضمن الشفافية والمساءلة، مرورًا بتطوير خوارزميات عادلة تحدّ من التحيز. وفي هذا السياق، تبرز الأهمية المتزايدة للنظم الهجينة التي تجمع بين قدرات الذكاء الاصطناعي والرصد البشري؛ إذ إن الاعتماد على القرار البشري وحده قد يتأثر بالتحيّزات الفردية والعوامل العاطفية، بينما قد تواجه الأنظمة الذكية تحديات مرتبطة بالتحيّز الخوارزمي. ومن ثمّ فإن الدمج بين الطرفين يوفر توازنًا يحدّ من نقاط الضعف في كل منهما، ويعزز دقة القرارات وموثوقيتها. ويتطلب ذلك أيضًا الاستثمار في نشر الوعي المؤسسي والمجتمعي بمخاطر الاستخدام غير المنضبط، وتعزيز التعاون الدولي لضمان الاستخدام الأخلاقي والمسؤول لهذه التقنيات المتقدمة.

ثانيًا: الإطار النظري لإدارة مخاطر الجريمة المالية وتداعياتها في القطاع المصرفي

مقدمة:

تعد الجرائم المالية Financial Crimes من أكبر وأخطر التحديات التي تواجه القطاع المصرفي في عصرنا الحالي، حيث تسهم هذه الجرائم - التي تشمل طيفا متنوعا من الجرائم مثل: غسل الأموال Money Laundering، والاحتيال المالي Financial Fraud، والتزييف Counterfeiting، والتزوير Forgery، والهجمات السيبرانية Cyber Attacks وغيرها من الأنماط المتعددة - في إحداث تأثيرات سلبية كبيرة على الاقتصاد والقطاع المالي وإنتاجية مؤسسات القطاع المصرفي، وتؤدي إلى فقدان الثقة في النظام المالي عامة والقطاع المصرفي خاصة (Khelil et al., 2024; International Monetary Fund, 2023; Kulmie, et al., 2023)؛ فقد قدرت الخسائر السنوية الإجمالية الناتجة عن جرائم الاحتيال المالي Financial Financial Crimes بما لا يقل عن 3.1 تريليون دولار وفقًا لتقرير **دورية ناسداك فيرافين عن الجرائم المالية** Nasdaq Verafin 2024 Global Financial Crime Report (Nasdaq & Verafin, 2024)، وفي المقابل أظهرت دراسة منهجية نُشرت في Journal of Financial Crime أن الأعوام الأربعة الأخيرة شهدت ارتفاع الهجمات الإلكترونية على المؤسسات المصرفية بنسبة (Cele & Kwenda, 2024) 43%، ومن جانب آخر تشير بيانات **معهد بازل للحوكمة** (Basel,2023) إلى تزايد قلق كل من مؤسسات القطاع المصرفي والمصارف المركزية بشأن مخاطر جريمة غسل الأموال Money Laundering؛ إذ ارتفع متوسط مستوى المخاطر العالمي من 5.25 من 10 في عام 2022 إلى 5.31 من 10 في عام 2023 حيث تنظر المؤسسات المصرفية والمصارف المركزية إلى جريمة غسل الأموال Money Laundering كأحد أكبر التحديات الأمنية التي تواجه القطاع المصرفي عالميا، وهو ما أكده أيضا تقرير معايير الاستقرار المالي 2024 Financial Stability Benchmarks Report (Central Banking, 2024) والذي أوضح أن حوالي 40% من المؤسسات المصرفية والمصارف المركزية قد أبلغت عن تزايد مخاوفها بشأن مخاطر جرائم غسل الأموال وتمويل الإرهاب في ولاياتها القضائية خلال العامين الماضيين، أما في المنطقة العربية فقد كشف تقرير **صندوق النقد العربي** أن 35% من المؤسسات المالية العربية قد تعرّضت لهجوم احتيالي واحد على الأقل خلال عام 2023، وهو ما يؤكد بشكل واضح خطورة هذه الجرائم على القطاعات المصرفية والمالية عالميا وعربيا، ويوضح الحاجة الملحّة إلى تعزيز آليات الرقابة والامتثال لمواجهة مخاطر الجرائم المالية المتزايدة والمتطورة (Arab Monetary Fund, 2024).

وتهدف هذه الدراسة إلى استكشاف تأثير الذكاء الاصطناعي Artificial Intelligence وتطبيقاته وتقنياته المختلفة على إدارة مخاطر الجرائم المالية Financial Crime Risk Management في القطاع المصرفي ومؤسساته، وتقديم منهجية شاملة ينتج عنها تحسين القدرة على الكشف عن هذه الجرائم، والتعامل معها، والتقليل من آثارها المختلفة؛ ففي عصرنا الحالي أصبحت إدارة المخاطر المالية Financial Risk Management عامة، وإدارة مخاطر الجرائم المالية Financial Crime Risk Management خاصة، ضرورة حتمية في مؤسسات القطاع المصرفي؛ إذ تعتمد هذه المؤسسات على تنفيذ إستراتيجيات فعالة للحد من هذه المخاطر وحماية أصولها وسمعتها، وهذه الإستراتيجيات تتطلب تعاونًا وثيقًا بين كل مكونات القطاع المصرفي من مؤسسات مصرفية ومالية محلية وإقليمية ودولية، وجهات إشراف ورقابة تنظيمية، علاوة على الاستشاريين ومقدمي الخدمات لهذه المؤسسات، كما أن هذه الإستراتيجيات تستدعي أيضا استخدام أدوات تحليلية متقدمة وتقنيات حديثة مثل الذكاء الاصطناعي Artificial Intelligence وتطبيقاته المختلفة في إدارة هذه المخاطر (Gupta, Dwivedi, & Shah, 2023; Zhang et al., 2023)، كما تهدف هذه الدراسة أيضا إلى تقديم إسهام أكاديمي قيم في مجال إدارة المخاطر المالية Financial Crime Risk Management، مما يسهم في تعزيز الفهم العلمي للجرائم المالية وكيفية التعامل معها وإدارة مخاطرها بكفاءة وفاعلية، وهو ما يشكل إطار عمل يمكن الاستفادة منه من قبل الأكاديميين، وصناع القرار، والممارسين في القطاع المصرفي، لتعزيز فاعلية السياسات والإستراتيجيات المطبقة في مواجهة الجرائم المالية.

وعملا على تحقيق هذه الأهداف، سيقوم الباحث بدراسة إدارة مخاطر الجرائم المالية Financial Crime Risk Management بالتفصيل من خلال دراسة الجرائم المالية Financial Crimes وأنماطها المختلفة في القطاع المصرفي، وتحليل كيفية تأثير هذه الجرائم على هذا القطاع، مع إلقاء الضوء على الإستراتيجيات المتبعة في إدارتها؛ ولذا فقد قسم الباحث هذا الجزء من الدراسة إلى العناصر التالية:

أولاً: تعريف الجرائم المالية في القطاع المصرفي.

ثانيًا: تصنيفات الجرائم المالية في القطاع المصرفي.

ثالثًا: أبرز الجرائم المالية في القطاع المصرفي.

رابعًا: الاتجاهات والتحديات الناشئة في الجرائم المالية في القطاع المصرفي.

خامسًا: الآثار المترتبة على الجرائم المالية في القطاع المصرفي.

سادسًا: إدارة مخاطر الجرائم المالية في القطاع المصرفي.

سابعًا: إستراتيجيات إدارة مخاطر الجرائم المالية في القطاع المصرفي.

ثامنًا: ضوابط إدارة مخاطر الجرائم المالية في القطاع المصرفي.

تاسعًا: مقاييس فاعلية إدارة مخاطر الجرائم المالية في القطاع المصرفي.

أولاً: تعريف الجرائم المالية في القطاع المصرفي:

يشير مصطلح الجرائم المالية Financial Crimes في القطاع المصرفي إلى: الأنشطة غير القانونية التي تتم بغرض الحصول على مكاسب مالية غير مشروعة، غالبًا من خلال استغلال النظام المالي والمصرفي أو التحايل عليه Gupta et al., (2023)، كما تُعرّف الجرائم المالية Financial Crimes أيضا بأنها: أي نشاط غير قانوني يُرتكب داخل المؤسسات المالية أو من خلالها، ويشمل: الاحتيال، وغسل الأموال، وتمويل الإرهاب، والفساد، والاختلاس، والتلاعب في البيانات المالية، وغيرها من الأفعال التي تهدف إما إلى تحقيق مكاسب مالية غير مشروعة أو إخفاء مصادر الأموال غير المشروعة (Jofre, Bosisio, & Riccardi, 2024)، في حين عرف (Brici, 2022) الجريمة المالية (Financial Crime) بأنها: كل أشكال الجرائم غير العنيفة التي تسبب خسارة مالية، بينما عرفتها الشرطة الدولية (الانتربول - Interpol) بكونها: كل فعل مجرم قانونا ينطوي على أو يترتب عليه الاستيلاء على مال الغير، أو ينطوي على التصرف في الأموال أو تحريكها على نحو مخالف للقانون (Interpol, 2020).

ويرى الباحث أن مصطلح الجريمة المالية في القطاع المصرفي يشير إلى: **مجموعة من الأنشطة غير القانونية التي تنطوي على استخدام غير مشروع للأموال أو المعاملات المالية في القنوات المصرفية بهدف تحقيق منافع شخصية أو مؤسسية بوسائل تنطوي على الخداع، أو إساءة استخدام السلطة، أو خيانة الأمانة، وتشمل هذه الجرائم مجموعة واسعة من السلوكيات الإجرامية المرتبطة بالمنتجات والخدمات المصرفية، وتستهدف المؤسسات المصرفية ذاتها أو عملاءها أو شركاءها التجاريين؛ مما يُقوّض نزاهة النظام المالي المصرفي، وقد يؤدي إلى عواقب مالية واجتماعية وتنظيمية وقانونية جسيمة.**

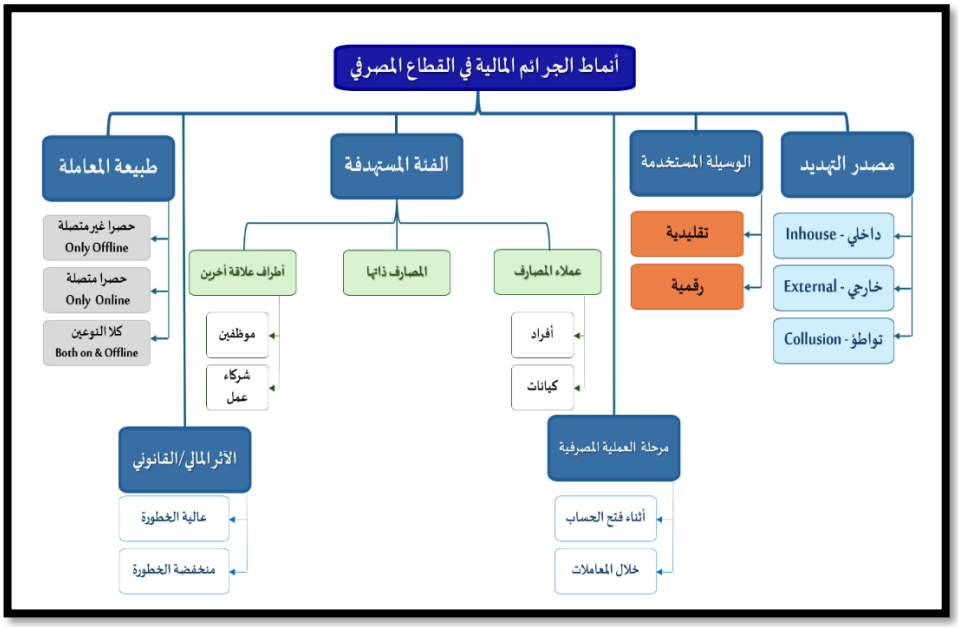
ثانيًا: تصنيفات الجرائم المالية في القطاع المصرفي:

كما أسلفنا، تتعدد أنماط الجرائم المالية Types of Financial Crimes في القطاع المصرفي بشكل كبير، حيث تشمل طيفا واسعا ومتنوعا من الجرائم، وفي سياق إعداد الدراسة الحالية، اطلع الباحث على مجموعة واسعة من الأدبيات المتعلقة بالجرائم المالية عامة، والجرائم المالية في القطاع المصرفي بشكل خاص، حيث تبيّن للباحث أن معظم هذه الدراسات ركزت على أنواع محددة من الجرائم المالية في القطاع المصرفي، ولكنها غالبًا ما افتقرت إلى إطار تصنيفي متكامل يربط بين الأبعاد المختلفة لهذه الجرائم. فالبعض من هذه الدراسات اقتصر على التركيز على نوع واحد فقط من أنواع الجرائم المالية ومنها على سبيل المثال دراسة (Harandi,2022) و دراسة (Levi,2022) وكلاهما اقتصر على بحث جريمة غسل الأموال، و دراسة (Bouveret ,2022) و

(Chianumba,2022) و اللذان اقتصرا على مناقشة الجرائم المالية ذات الطبيعة السيبرانية، ودراسة (Afjal et al., 2023) و دراسة (Mahony, 2022) و دراسة (Pradesyah et al, 2021) وهي الدراسات التي بحثت جميعها فقط في جريمة الاحتيال دون التطرق لغيرها من الجرائم، وكذا دارسات كلا من (Pilat, Sharenko & Sumtsova, 2025) و (Barry & Biglaiser, 2024) و (Cipriani et al. 2023) وهي الدراسات التي ناقشت كل منها فقط جريمة خرق قرارات العقوبات و الجزاءات المالية المستهدفة، و دراسة (Pieth, 2022) والتي تناولت تحليل جريمة تمويل الإرهاب فقط، نهاية بدراسة (Kassenova & Early, 2023) والتي اقتصرت على مناقشة وبحث جريمة تمويل انتشار أسلحة الدمار الشامل دون مناقشة غيرها من الجرائم المالية. ومن جانب آخر، نجد أن بعض هذه الدراسات التي اطلع عليها الباحث قد ناقشت نمطين مختلفين من الجرائم المالية وذلك من قبيل الربط بينهما، ومنه على سبيل المثال دراسة كل من (Arthur et al., 2024) و (Schneider, 2022) و (Demirović et al., 2022) وهي الدراسات التي ناقشت جريمتي غسل الأموال و تمويل الإرهاب.

ويرى الباحث أن تركيز معظم هذه الدراسات على أنواع محددة من الجرائم المالية في القطاع المصرفي، مع الافتقار إلى إطار تصنيفي متكامل يربط بين الأبعاد المختلفة لهذه الجرائم يعود إلى أن التصنيفات المتوفرة حاليا تتباين من حيث المعايير المستخدمة في التصنيف، وتغفل طبيعة الجريمة المالية كمنظومة مترابطة تشمل عدة أبعاد، مثل: مصدر التهديد، والأطراف المستهدفة، ووسائل ارتكاب الجريمة، والتأثير الناتج عنها. وفي ضوء هذه الفجوة المعرفية يقدم الباحث تصنيفًا تحليليًا جديدًا للجرائم المالية في القطاع المصرفي يعتمد على معايير متعددة الأبعاد Multi-factors؛ بهدف إثراء الإطار النظري وتوفير أداة تحليلية أكثر شمولية لفهم الظاهرة.

وفي هذا السياق **يرى الباحث** أنه يمكن تقسيم الجرائم المالية Financial Crimes في القطاع المصرفي بالاعتماد على ستة معايير للتقسيم أو التصنيف Classification Criteria، حيث يمكن تصنيفها وفقا لمصدر التهديد Source of Threat، أو وسيلة ارتكاب الجريمة Method of Crime، أو وفقا لمرحلة العملية المصرفية التي يتم فيها ارتكاب الجريمة Stage of Banking Process، أو وفقا للفئة المستهدفة من الجريمة Targeted Party، كما يمكن تقسيمها وفقا لطبيعة المعاملة المالية Nature of Financial Transaction، وأخيرا يمكن تقسيم الجرائم المالية في القطاع المصرفي وفقا لمعيار حجم الأثر القانوني أو المالي الناتج عنها Financial or Legal Impact، وفي السطور التالية نستعرض هذه التصنيفات بشيء من الإيجاز.



شكل رقم (5): تصنيفات الجرائم المالية في القطاع المصرفي

المصدر: من إعداد الباحث بناء على مصادر الدراسة

1. الجرائم المالية وفقا لمصدر التهديد Source of Threat:

وفقا لمصدر التهديد Source of Threat يمكن تقسيم الجرائم المالية التي يتم ارتكابها في القطاع المصرفي إلى ثلاثة أنماط كما يلي (Kurshan & Shen , 2024):

أ. الجرائم المالية الداخلية Internal / In-house Financial Crimes:

وهي تلك الجرائم المالية التي يرتكبها موظفو ومسئولو المؤسسة المصرفية أنفسهم دون أي اشتراك أو تعاون من أي طرف خارجي، ومن أمثلتها الاختلاس وتسريب المعلومات.

ب. الجرائم المالية الخارجية External Financial Crimes:

ويقصد بها تلك الجرائم المالية التي يرتكبها الأطراف الخارجية من ذوي العلاقة مع المؤسسة المصرفية، مثل العملاء أو الشركاء التجاريين أو المجرمين المحترفين أو غيرهم، دون أي اشتراك أو تعاون من أي طرف داخلي من موظفي أو مسئولي المؤسسة المصرفية، ومن أمثلتها الهجمات السيبرانية أو التصيد الاحتيالي.

ج. الجرائم المالية المشتركة Mutual Financial Crimes:

وتشير إلى الجرائم المالية التي يتم ارتكابها بشكل مشترك من خلال التواطؤ Collusion بين أطراف داخلية من موظفي أو مسئولي المؤسسة المصرفية وأخرى خارجية من ذوي العلاقة مع المؤسسة المصرفية، مثل العملاء أو الشركاء التجاريين أو المجرمين المحترفين أو غيرهم، وتشمل العديد من الأنماط، ومنها على سبيل المثال الرشوة والفساد.

وتؤكد دراسة (Kurshan & Shen , 2024)أن الفهم والتحليل الصحيح لمصادر التهديد التي ينتج عنها الجرائم المالية له أكبر الأثر في إمكانية تصميم أدوات لكشف ومراقبة أنماط السلوك المشبوه في عمليات ومعاملات مؤسسات القطاع المصرفي، ونجاح هذه الأدوات.

2. الجرائم المالية وفقا للوسائل المستخدمة Method of Crime:

تنقسم الجرائم المالية من حيث الوسيلة المستخدمة Method of Crime في ارتكابها إلى نمطين، هما (Chianumba, 2022):

أ. جرائم مالية يتم ارتكابها بالوسائل التقليدية Traditional Crimes:

وهي الجرائم التي يستخدم في ارتكابها وسائل تقليدية، قد تكون أحيانا يدوية أو ميكانيكية مثل جرائم الاختلاس، أو جرائم التزوير الورقي.

ب. جرائم مالية يتم ارتكابها بالوسائل الرقمية Digital Crimes:

وهي تلك الجرائم المستحدثة التي يعتمد المجرمون في ارتكابها على وسائل رقمية، مثل التصيد الإلكتروني أو الهجمات السيبرانية باستخدام البرمجيات الخبيثة، وغيرها.

وفي العقود الأربعة الأخيرة، كان من الجلي أن التطور الكبير في المجالات التقنية عامة، ومجالات التقنية المصرفية خاصة، كان له أكبر التأثير في تغيّر أنماط الجرائم المالية في القطاع المصرفي وزيادة تعقيدها وارتفاع معدلات ارتكابها، وهو ما أكدته دراسة (Chianumba, 2022).

3. الجرائم المالية وفق مرحلة Stage of Banking Process العملية المصرفية:

ترتكب الجرائم المالية في القطاع المصرفي في مراحل مختلفة من العملية المصرفية، ويمكن بشكل عام تقسيم أنماط الجرائم المالية وفق هذا المعيار إلى نمطين رئيسيين كما يلي (Harandi, 2022):

أ. جرائم مالية في مرحلة فتح الحسابات و إنشاء العلاقة Account Opening Stages:

وهي تلك الجرائم المالية التي يتم ارتكابها في أثناء مرحلة فتح الحساب وإقامة أو إنشاء العلاقة مع المؤسسة المصرفية، وغالبا ما تكون تمهيدا أو جزءا من الإعداد لجريمة مالية أكبر لاحقا، ومن أمثلتها استخدام مستندات مزورة كمستندات تحقيق الهوية في إطار القيام بجريمة احتيال، وهكذا.

ب. جرائم مالية في مرحلة تنفيذ المعاملات Transactions Conducting Stages :

وهي تلك الجرائم المالية التي يتم ارتكابها بعد مرحلة فتح الحساب وإقامة العلاقة مع المؤسسة المصرفية، أي أثناء تنفيذ المعاملات المصرفية، ومن أمثلتها استخدام التحويلات المالية المشبوهة، وغسل الأموال، واحتيالات القروض، وهكذا.

وفي هذا الإطار تؤكد دراسة (Harandi, 2022) أن توزيع الجرائم المالية على مراحل العمليات والمعاملات المصرفية يسهم بشكل كبير في إمكانية الكشف والضبط المبكر عبر نماذج التقييم المتعدد Multiple Assessment Models.

4. الجرائم المالية وفق الفئة المستهدفة Targeted Party:

في العمليات والمعاملات المصرفية تتنوع وتختلف الفئات ذات العلاقة مع المؤسسات المصرفية، ومن ثم تتنوع أيضا الفئات المستهدفة Targeted Party من ارتكاب الجرائم المالية، أو بمعنى آخر ضحايا Victims هذه الجرائم، وتنقسم هذه الفئات أو هؤلاء الضحايا غالبا إلى (Sanusi , 2022):

أ. جرائم مالية تستهدف عملاء المؤسسة المصرفية:

وهي الجرائم التي تستهدف عملاء المؤسسات المصرفية إما للحصول على أموالهم أو معلوماتهم الشخصية، أو البيانات الخاصة بالأدوات المالية التي يستعملونها، أو بيانات الدخول الى حساباتهم المصرفية، وغيرها.

ب. جرائم مالية تستهدف المؤسسة المصرفية ذاتها:

وهي الجرائم التي تستهدف المؤسسة المصرفية ذاتها للاستيلاء على أموالها، كالاختلاس والاحتيال أو اختراق بيانتها وأنظمتها، أو استغلالها كقناة لارتكاب جرائم أخرى، كغسل الأموال وتمويل الإرهاب وتمويل انتشار أسلحة الدمار الشامل.

ج. جرائم مالية تستهدف أطراف العلاقة الآخرين:

وهي الجرائم التي تستهدف أطرافا ثالثة ذات علاقة مع المؤسسة المصرفية، كموظفي ومسئولي المؤسسة، أو الشركاء التجاريين لها، كمقدمي الخدمات في مجالات الاتصالات وتقنية المعلومات، وغيرها من الأطراف.

وقد أبرزت دراسة (Sanusi , 2022) أن تعدد الفئات التي تستهدفها الجرائم المالية في القطاع المصرفي وتنوع ضحاياها، هو من العوامل التي تزيد من تعقيد منظومة الحماية ضد هذه الجرائم.

5. الجرائم المالية وفقا لطبيعة المعاملة Nature of Transaction :

في عصرنا الحالي تتنوع وتختلف طبيعة المعاملات المصرفية من ناحية طريقة إجرائها والقيام بها، ومن ثمَّ تتنوع وتختلف الجرائم المالية التي تستهدف هذه المعاملات، وبالنظر إلى ذلك يمكن تقسيم الجرائم المالية في القطاع المصرفي وفقا لطبيعة المعاملة إلى 3 أقسام كالتالي (Bouveret ,2022):

أ. جرائم مالية في المعاملات دون اتصال Offline Transactions:

هي تلك الجرائم المالية التي يتم ارتكابها حصرا في المعاملات المصرفية غير المتصلة بشبكة الإنترنت، مثل تزوير المستندات أو التوقيعات.

ب. جرائم مالية في المعاملات أثناء الاتصال Online Transactions :

وهي تلك الجرائم التي يتم ارتكابها حصرا في المعاملات المتصلة بشبكة الإنترنت، ومنها الاحتيال الرقمي عبر الإنترنت أو اختراق الأنظمة المصرفية.

ج. جرائم مالية في معاملات هجينة Online/Offline Transactions:

هي تلك الجرائم التي يتم ارتكابها في المعاملات الهجينة، أي المعاملات التي يمكن القيام بها سواء بالاتصال بشبكة الإنترنت أو بدونه، ومنها الاحتيال باستخدام بطاقات الدفع في المتاجر أو المواقع الإلكترونية.

وقد أشارت دراسة (Bouveret ,2022) إلى أن المعاملات ذات الطبيعة الرقمية تتطلب إستراتيجيات وقائية متقدمة ومعقدة من أجل مكافحة الجرائم المالية التي قد ترتكب أثناء القيام بها.

6. الجرائم المالية وفقا للأثر القانوني أو المالي الناتج عنها Financial or Legal Impact:

تتفاوت خطورة الجرائم المالية في القطاع المصرفي وفقا للآثار الناتجة عنها، ومن أهم معايير تقييم آثار الجرائم المالية نجد معياري الأثر المالي والأثر القانوني، ووفقا لهذين المعيارين، يمكن تصنيف الجرائم المالية في القطاع المصرفي إلى قسمين كما يلي (Levi, 2022):

أ. جرائم مالية عالية الخطورة High-Risk Crimes:

وهي الجرائم التي يتنج عنها أثارا كبيرة، سواء على المستوى المالي، حيث تتكبد المؤسسات المصرفية أو الضحايا الآخرين خسائر مالية ضخمة، وعلى المستوى القانوني قد ينتج عنها عقوبات قانونية أو تنظيمية كبيرة أو كلاهما، بالإضافة لمخاطر أخرى مثل مخاطر السمعة والصورة الذهنية؛ فهي إذن جرائم تمثل خطورة كبيرة على استقرار القطاع المصرفي والمالي عامة، ومن أمثلتها جرائم غسل الأموال أو خرق قرارات الجزاءات المالية المستهدفة، والعقوبات ذات الصلة بمكافحة تمويل الانتشار أو تمويل الإرهاب.

ب. جرائم مالية منخفضة الخطورة Low-Risk Crimes:

هي عادة لا تحدث ضررا ماليا أو قانونيا كبيرا على المؤسسة المصرفية، ويمكن رصدها وكشفها مبكرا؛ ولذا فهي نادرا ما تؤثر على استقرار المؤسسة المصرفية أو القطاع المصرفي والنظام المالي ككل، ومن أمثلتها المحاولات الفاشلة لصرف شيكات مزورة صغيرة القيمة، أو فتح حساب مصرفي باستخدام وثائق مزورة دون القيام بنشاط أو معاملات مالية أو استخدام بطاقات ائتمان مسروقة في معاملات بمبالغ صغيرة.

ووفقا لدراسة (Southworth& Levi, 2024) يساعد التصنيف الصحيح والدقيق للجرائم المالية وفقا لمستوى خطورتها في تطوير نهج رقابي أكثر توازنا ومرونة في تبنيه وتنفيذه، وأكثر فاعلية في تحقيق نتائجه.

ثالثا: أبرز صور الجرائم المالية في القطاع المصرفي:

في العصر الحديث، وخاصة في العقود الأربعة الأخيرة، أصبحت الجرائم المالية أحد أبرز التحديات التي تواجه القطاع المصرفي في العالم أجمع، ليس فقط لتعدد أشكالها وتطور وسائل ارتكابها، ولكن أيضا للانتشار الكبير والتوسع غير المسبوق للمؤسسات المصرفية، سواء على المستوى الأفقي، ونعني به اتساع الرقعة الجغرافية التي تغطيها خدماته واتساع شبكة علاقاتها وشركاتها التجارية محليا ودوليا، وكذا على المستوى الرأسي، ونعني به تقديمها لتشكيلة أكبر من المنتجات والخدمات المصرفية وكذا شمولها لشرائح أكبر من العملاء وزيادة حجم التعاملات المالية مع هذه الشرائح، وقد أسهمت هذه العوامل، إضافة إلى التحولات الرقمية، في خلق بيئة خصبة لارتكاب هذا النوع من الجرائم، وفي هذا السياق يستعرض هذا الجزء من الدراسة بشكل موجز أبرز صور الجريمة المالية التي تستهدف المؤسسات المصرفية.

1. جريمة غسل الأموال Money Laundering:

تشكل جريمة غسل الأموال تهديدًا كبيرًا للدول وأمنها السياسي والاقتصادي والاجتماعي واستقرارها المالي من ناحية، واستقرار أنظمتها ومؤسساتها المصرفية من ناحية أخرى، حيث تساعد هذه الجريمة في إخفاء مصادر الأموال غير المشروعة وتتيح للجماعات الإجرامية تمويل أنشطتها بشكل غير قانوني، كما أن جريمة غسل الأموال تضعف النظام المالي والمصرفي، مما يؤدي إلى فقدان الثقة في المؤسسات المالية والمصرفية، ويعرّضها لفرض عقوبات دولية، بالإضافة إلى ذلك تسهم في تمكين الإرهاب والجريمة المنظمة من التوسع والانتشار بشكل غير مرئي.

وتعرف جريمة غسل الأموال Money Laundering بأنها عملية تحويل الأموال الناتجة عن جرائم وأنشطة غير قانونية (مثل الإتجار بالمخدرات أو الفساد أو غيرها) إلى أموال أو أصول تبدو قانونية، وعادة ما تتم هذه العملية – غسل الأموال - من خلال ثلاث مراحل رئيسية كالتالي (Arthur et al., 2024):

أ. مرحلة الإيداع أو الإحلال Placement Stage:

وهي المرحلة التي يتم فيها ومن خلالها إدخال أو إيداع Placement الأموال غير المشروعة Illicit Funds إلى النظام المالي الرسمي محليا أو عالميا، وعادة ما يتم ذلك من خلال العديد من الوسائل والأساليب Typologies التي تتراوح ما بين البسيطة إلى المعقدة، والتي قد تكون فردية أو من خلال شبكات إجرامية منظمة، وتشمل هذه الأساليب على سبيل المثال: إيداع الأموال – بعد هيكلتها أو تجزئتها - في حسابات مصرفية، أو تحويلها إلى عملات أجنبية أو أدوات مالية، مثل الشيكات أو البطاقات مسبقة الدفع، أو من خلال شراء أصول نقدية ذات طابع سائل، مثل المعادن الثمينة أو الأحجار الكريمة، وتُعد هذه المرحلة الأكثر عرضة للكشف؛ نظرًا لأن الأموال المراد غسلها ما تزال مرتبطة بشكل مباشر بالنشاط الجرمي غير القانوني الذي تولدت عنه.

شكل رقم (6): مراحل جريمة غسل الأموال

المصدر: من إعداد الباحث بناء على مصادر الدراسة

ب. مرحلة التغطية أو التمويه Layering Stage:

وهي المرحلة التي يتم فيها قطع الصلة بين الأموال غير المشروعة وبين مصدرها الجرمي الأصلي من خلال القيام بسلسلة من العمليات والمعاملات المتتالية التي تشمل تحويل هذه الأموال بين حسابات مصرفية مختلفة محليا ودوليا، أو استخدام شركات واجهة Front Companies أو ورقية Paper Companies أو وهمية Shell Companies، كما يتم أيضا استخدام قنوات مالية متعددة بهدف تضليل المؤسسات المصرفية والسلطات الأخرى المختلفة ذات الصلة وإرباك عمليات تتبع هذه الأموال، وتعد هذه المرحلة حجر الزاوية في عملية غسل الأموال، حيث تتعقد حركة الأموال غير المشروعة وتزداد صعوبة إمكانية كشف مصدرها الحقيقي.

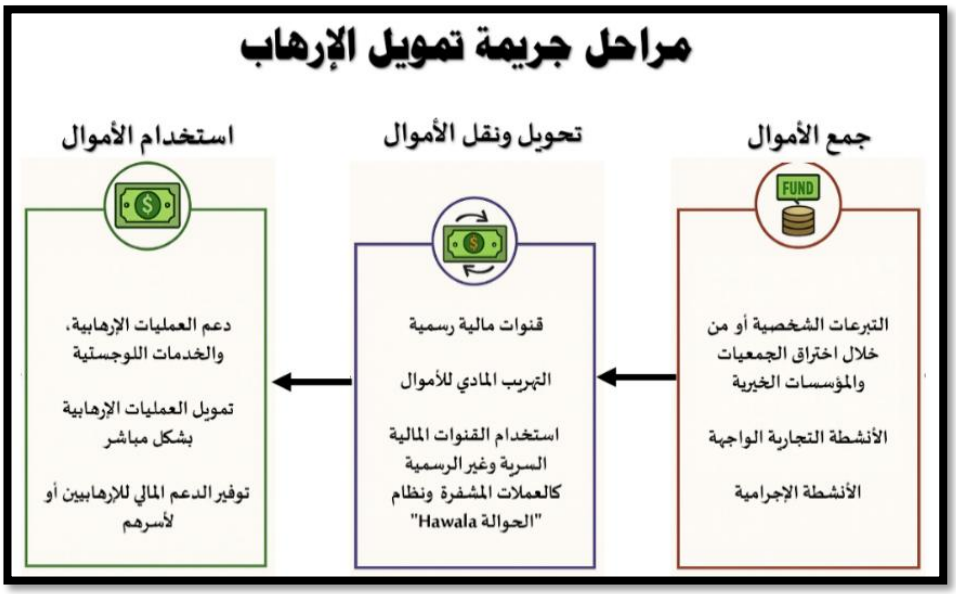
ج. مرحلة الدمج أو الإدماج Integration Stage:

وهي المرحلة النهائية من مراحل جريمة غسل الأموال والتي يتم فيها إعادة ضخ الأموال المغسولة إلى الاقتصاد المشروع بحيث تبدو وكأنها أموال مشروعة، ويتم ذلك عادة من خلال العديد من الأساليب، كاستثمار هذه الأموال في مشروعات تجارية، أو شراء الأصول المختلفة كالعقارات، أو دمجها في أرباح مؤسسات أعمال قائمة، وعند هذه النقطة تصبح عملية تتبع مصدر الأموال الأصلي شبه مستحيلة دون تحريات معمقة.

2. جريمة تمويل الإرهاب Terrorism Financing:

تعد جريمة تمويل الإرهاب Terrorism Financing واحدة من أخطر الجرائم التي تواجه المجتمعات والدول وليس فقط مؤسسات القطاع المصرفي، فهذه الجريمة تُمكّن الإرهابيين أفرادا وجماعات من تنفيذ عمليات عنف تُهدد حياة البشر، كما تهدد أمن المجتمعات والدول واستقرارها، كما تعد هذه الجريمة أيضا سببا في ارتفاع مستوى الجريمة عامة في المجتمع؛ نظرا لارتباط جريمة تمويل الإرهاب بالعديد من الجرائم الأخرى، كالاتجار بالبشر والمخدرات وتزوير الوثائق والعملات، مما يؤدي إلى انتشار الشبكات الإجرامية وتكاملها، ومن جانب آخر فجريمة تمويل الإرهاب Terrorism Financing قد تُقوّض الاقتصاد الوطني ومؤسساته المالية المصرفية، وذلك عبر تحويل الموارد المالية إلى وقود لارتكاب أنشطة تدميرية بدلاً من استخدامها في التنمية، بالإضافة إلى ذلك تعد هذه الجريمة سببا رئيسيا في تعرُّض الدولة ومؤسساتها المالية والمصرفية لعقوبات أممية ودولية قد تصل إلى العزلة الدولية في حال عدم التزامها بمكافحة هذا التمويل وفق المعايير العالمية.

ووفقا للتوصية الخامسة من التوصيات الأربعين لمجموعة العمل المالي Financial Action Task Force-FATF تعرف جريمة تمويل الإرهاب بأنها: توفير أو جمع الأموال أو توزيعها أو استخدامها بأي وسيلة، سواء بشكل مباشر أو غير مباشر، مع العلم بأنها ستُستخدم كليًا أو جزئيًا لتنفيذ أعمال إرهابية، أو لدعم الأفراد أو الجماعات الإرهابية، حتى إذا لم تُستخدم الأموال فعليًا في عمل إرهابي (FATF, 2012/2025)، وتمر جريمة تمويل الإرهاب عادةً بثلاث مراحل رئيسية لارتكابها، وذلك كما يلي (Schneider, 2022):



شكل رقم (7): مراحل جريمة تمويل الإرهاب

المصدر: من إعداد الباحث بناء على مصادر الدراسة

أ. مرحلة جمع الأموال Fund Raising:

حيث يتم جمع الأموال من مصادر قد تكون مشروعة، مثل التبرعات والدعم الشخصي، أو تحت ستار الجمعيات والمؤسسات الخيرية المخترقة أو التي لديها ضعف في إجراءاتها وأنظمتها الداخلية، أو من خلال الأنشطة التجارية التي تستغل كأنشطة واجهة Front Business للاختباء خلفها، كما قد يتم جمع هذه الأموال من مصادر غير مشروعة، من خلال ارتكاب الجرائم التي تولد أموالا للإرهابيين أو ممولهم، كالاتجار بالبشر وتجارة المخدرات والأسلحة.

ب. مرحلة نقل وتحويل الأموال Fund Transferring :

حيث تُنقل الأموال من مكان لآخر بهدف إخفاء المصدر الحقيقي لها، وغالبا ما يتم ذلك إما عبر قنوات مالية رسمية متنوعة، تشمل المؤسسات المصرفية، والتحويلات النقدية المشروعة، أو من خلال التهريب المادي للأموال، أو استخدام القنوات المالية السرية وغير الرسمية، ومنها العملات المشفرة، وأيضا ما يسمى بنظام "الحوالة Hawala".

ج. مرحلة استخدام الأموال Fund Using :

وهي المرحلة التي تُوظف فيها الأموال التي تم جمعها لدعم العمليات الإرهابية والخدمات اللوجستية والتجنيد، كشراء الأسلحة، وتوفير المأوى والتنقلات، أو تمويل العمليات الإرهابية بشكل مباشر، أو توفير الدعم المالي للإرهابيين أو لأسر الإرهابيين خارج ميدان العمليات.

وتعد جهود مكافحة تمويل الإرهاب Counter Terrorism Financing من أنجع الوسائل في إضعاف التنظيمات الإرهابية وتجفيف منابعها المالية، مما يُحد من قدرتها على تنفيذ مخططاتها، وتلعب المؤسسات المصرفية دورًا محوريًا في هذه الجهود من خلال تطبيق أنظمة الرقابة المالية، والكشف عن المعاملات المشبوهة والإبلاغ عنها، ويتم ذلك من خلال تتبّع حركة الأموال المشبوهة، وقطع مصادر التمويل، وتعزيز التعاون الدولي في تبادل المعلومات المالية، وهو ما يسهم بشكل فعّال في الحد من الأنشطة الإرهابية ومنع انتشارها، ويعزز الأمن والاستقرار على المستويين الوطني والدولي (Pieth, 2022).

3. جريمة تمويل الانتشار Proliferation Financing :

يُنظر إلى جريمة تمويل انتشار أسلحة الدمار الشامل Proliferation Financing على أنها واحدة من أخطر التهديدات التي تواجه الأمن والسلم الدوليين، حيث تُسهّل هذه الجريمة حصول جهات غير مشروعة، سواء كانت دولاً أو جماعات أو أفرادًا، على المواد أو التقنيات التي تُستخدم في إنتاج أسلحة الدمار الشامل Weapons of Mass Destruction مثل الأسلحة النووية أو الكيميائية أو البيولوجية، وتكمن خطورة هذه الجريمة في أنها تُغذي أنشطة محظورة تُهدد الاستقرار الإقليمي والدولي، كما أنها ترتبط بشبكات التهريب وتزوير الوثائق وانتهاك أنشطة التجارة الدولية International Trade وأنظمة تمويلها Trade Finance والرقابة عليها، مما يعزز من أنشطة السوق السوداء ويُضعف جهود الرقابة الدولية، ومن ناحية أخرى فإن عمليات تمويل الانتشار Proliferation Financing قد تعرّض الدول والمؤسسات المالية والمصرفية إلى عقوبات أممية ودولية صارمة تشمل القيود التجارية والاقتصادية أو الجزاءات المالية المستهدفة Targeted Financial Sanctions، وقد تصل إلى الحظر الشامل، خصوصًا إذا ثبت تورطها أو تقصيرها في الالتزام بالقرارات الأممية ومعايير مجموعة العمل الماليFATF ، مما ينعكس سلبًا على الثقة في النظام المالي ويُهدد الاقتصاد الوطني.

واستنادًا إلى قرار مجلس الأمن الدولي رقم **1540**، أصدرت مجموعة العمل الماليFATF تعريفًا عمليًا محددًا لجريمة تمويل الانتشار Proliferation Financing بأنها: توفير الأموال أو الخدمات المالية التي تُستخدم كليًا أو جزئيًا في صنع أو اكتساب أو حيازة أو تطوير أو تصدير أو إعادة شحن أو وساطة أو نقل أو تحويل أو تخزين أو استخدام أسلحة نووية أو كيميائية أو بيولوجية ووسائل إيصالها والمواد المتعلقة بها (بما في ذلك التقنيات والسلع ذات الاستخدام المزدوج لأغراض غير مشروعة)، بما يخالف القوانين الوطنية أو، حيثما ينطبق، الالتزامات الدولية (FATF, 2021)، وتمر **جريمة تمويل الانتشار بثلاث مراحل متسلسلة كالتالي** (Kassenova & Early, 2023):

أ. مرحلة جمع الأموال Fund Raising:

في هذه المرحلة تختلف مصادر الأموال وفقا للجهة الراغبة في امتلاك أسلحة الدمار الشامل؛ ففي حال كانت هذه الجهة هي الدول، تقوم الدولة التي لديها برنامج للتسلح بجمع الأموال المخصصة لذلك من داخلها، سواء من الموازنة الرسمية أو مصادر أخرى، مثل الأرباح من شبكة شركات تجارية تتبع لها، أما في حال كانت هذه الجهة هي إحدى الجماعات الإرهابية، فتكون الأموال من المتحصلات الناتجة عن جرائم ترتكبها هذه الجماعات أو من التبرعات التي تصل إليها من مؤيديها ومعتنقي أفكارها.

ب. مرحلة نقل وتحويل الأموال Fund Transferring :

في هذه المرحلة تسعى الدول التي لديها برامج للتسلح والخاضعة للعقوبات إلى التحايل على هذه العقوبات باستخدام وسائل لتمويه الأموال، حيث تقوم بنقل الأموال للنظام المالي الدولي من خلال معاملات صرف عملات أجنبية لغايات التبادل التجاري باستخدام أساليب متعددة مرورًا بقنوات المصارف المراسلة الطبيعية أو شبكة معقدة من الموردين وشركات الواجهة أو شركات وهمية وهياكل الملكية المعقّدة للتهرب والتحايل على العقوبات، أما الجماعات الإرهابية فتلجأ إلى أساليب مثل تهريب الأموال أو استخدام القنوات السرية وغير الرسمية أو ما يسمى بنظام "الحوالة Hawala"، وكذا العملات المشفرة Crypto Currency.

ج. مرحلة استخدام الأموال Fund Using :

في هذه المرحلة تستخدم الدول أو الجماعات الإرهابية التي لديها برامج للتسلح أو وكلاؤهما هذه الأموال ضمن النظام المالي الدولي في تمويل الأنشطة المتعلقة بتصنيع أو نقل أو تطوير أو استخدام أسلحة الدمار الشامل، وتشمل هذه المرحلة الدفعات لشراء المواد أو التكنولوجيا ذات الاستخدام المزدوج، واقتناء المواد والتقنيات الحساسة ونقلها، ولاحظت مجموعة خبراء تابعة للأمم المتحدة أن هذه الجهات تستخدم وسائل تمويه مختلفة، بما في ذلك استخدام الشركات الواجهة للحصول على هذه الواردات المحظورة.

شكل رقم (8): مراحل جريمة تمويل الانتشار

المصدر: من إعداد الباحث بناء على مصادر الدراسة

وتمثل مكافحة تمويل انتشار أسلحة الدمار الشامل تحديًا كبيرًا لمؤسسات القطاع المصرفي، نظرًا لتشابه أنشطة تمويل الانتشار مع الأنشطة التجارية المشروعة، مما يتطلب من الدول والمؤسسات المالية عامة، والمصرفية خاصة، تعزيز قدراتها على تقييم المخاطر وتطبيق تدابير فعالة للحد منها (Kassenova & Early, 2023).

4. جريمة خرق قرارات العقوبات (الجزاءات) المالية المستهدفة Evasion of Targeted Financial Sanctions:

تُعد جريمة خرق قرارات العقوبات أو الجزاءات المالية المستهدفة Evasion of Targeted Financial Sanctions من أخطر الجرائم الاقتصادية العابرة للحدود، كما أنها من أخطر التحديات التي تواجه النظام المالي الدولي، فهذه الجرائم تُقوّض الجهود الرامية إلى مكافحة جرائم الإرهاب وتمويله، ومنع انتشار أسلحة الدمار الشامل، وتعزيز حقوق الإنسان، ومن ثمَّ تُضعف فاعلية التدابير المتخذة لحفظ الأمن والسلم الدوليين (Cipriani et al. 2023).

وتُعرف **العقوبات أو الجزاءات المالية المستهدفة** Targeted Financial Sanctions بأنها: تدابير اقتصادية تُفرض على أفراد أو كيانات محددة بهدف التأثير على سلوكهم أو سياساتهم دون الإضرار بالاقتصاد العام للدولة المستهدفة، وتُستخدم هذه العقوبات أو الجزاءات كأداة للضغط السياسي والاقتصادي، وتُفرض هذه العقوبات أو الجزاءات من قبل هيئات دولية مثل

مجلس الأمن التابع للأمم المتحدة، وكذلك من قبل دول أو تكتلات إقليمية مثل الاتحاد الأوروبي والولايات المتحدة الأمريكية، وهناك نوعان رئيسيان من هذه العقوبات أو الجزاءات، كالتالي (Pilat, Sharenko & Sumtsova, 2025):

أ. **تجميد الأصول Asset Freezing**:

ويقصد به حظر نقل أو تحويل أو التصرف في أو تحريك أي أموال أو أصول أخرى يملكها أو يتحكم فيها الفرد أو الكيان المدرج على قوائم العقوبات أو الجزاءات المالية المستهدفة، ويشمل هذ الحظر تجميد كافة الأموال والأصول المالية والموارد الاقتصادية الأخرى، بما في ذلك حظر استخدامها أو نقلها أو تعديلها أو تحويلها لأشخاص آخرين (سواء كان ذلك بالبيع أو التأجير أو الرهن) أو حتى إمكانية الوصول إليها.

ب. **حظر تقديم أو توفير الأموال أو الخدمات Prohibition of Funds or Services:**

ويقصد به الإجراء القانوني الذي يُلزم الأفراد والكيانات - بما فيها المؤسسات المصرفية - بعدم تقديم أموال أو خدمات اقتصادية أو مالية، بصورة مباشرة أو غير مباشرة، إلى الأفراد أو الكيانات الخاضعة للعقوبات والجزاءات المالية المستهدفة، ويشمل هذا الحظر منع التحويلات المالية، تقديم القروض، منح التأمين، تسهيل الاستثمارات، أو توفير خدمات مهنية مثل الاستشارات القانونية أو المحاسبية، ويُعد هذا الإجراء من الأدوات الأساسية لضمان فاعلية أنظمة العقوبات المستهدفة ومنع الكيانات المدرجة من الوصول إلى الموارد التي قد تسهم في استمرار أنشطتها غير المشروعة.

وتلعب المؤسسات المصرفية دورًا محوريًا في تنفيذ قرارات الجزاءات المالية المستهدفة Targeted Financial Sanctions، حيث تُعد خط الدفاع الأول لمنع التدفقات المالية غير المشروعة إلى الأفراد والكيانات المدرجة على قوائم الجزاءات المالية المستهدفة، وتقوم المؤسسات المصرفية بذلك وفقًا للمعايير التي تضعها الهيئات التنظيمية المحلية والدولية مثل مجلس الأمن التابع للأمم المتحدة ومجموعة العمل المالي FATF، وتشمل مسؤوليات المؤسسات المصرفية في هذا الصدد القيام بما يلي من جهود (Efing et al., 2023):

أ. التأكد من جمع معلومات دقيقة ومحدثة عن العملاء وجميع أطراف العلاقة معها (الأفراد والشركات) والتحقق من هويتهم، والتأكد من كونهم غير مدرجين على قوائم الأفراد والكيانات الخاضعين للجزاءات المالية المستهدفة.

ب. المراقبة المستمرة للحسابات والمعاملات للتحقق من عدم ارتباط العملاء أو تلك الأطراف المرتبطة بهم بأية معاملات أو علاقات مع أي من الأفراد والكيانات المدرجين على قوائم العقوبات والجزاءات المالية المستهدفة.

ج. تجميد الأموال أو الأصول المملوكة للأفراد أو الكيانات المدرجة على قوائم العقوبات والجزاءات المالية المستهدفة فورًا ودون تأخير.

د. الامتناع عن إجراء أي معاملات مالية أو تجارية لصالح الكيانات أو الأفراد الخاضعين للعقوبات والجزاءات المالية المستهدفة.

هـ. تقديم تقارير إلى السلطات المختصة عند اكتشاف معاملات مشبوهة تتعلق بأفراد أو كيانات خاضعة للجزاءات.

و. التعاون مع الجهات الرقابية لتوفير معلومات إضافية عند الحاجة.

وتُعرف جريمة خرق قرارات العقوبات أو الجزاءات المالية المستهدفة Evasion of Targeted Financial Sanctions بأنها: كل سلوك مقصود يتمثل في تقديم دعم مالي أو اقتصادي، بشكل مباشر أو غير مباشر، للأفراد أو الكيانات الخاضعة للعقوبات أو الجزاءات المالية المستهدفة، أو تسهيل العمليات أو المعاملات التي تهدف إلى تجاوز أو تقويض هذه التدابير والإجراءات، سواء كان ذلك عبر المعاملات المالية، أو التجارية، أو تقديم خدمات اقتصادية من أي نوع (Meissner & Mello, 2022).

ويتم ارتكاب جريمة **خرق قرارات العقوبات أو الجزاءات المالية المستهدفة Evasion of Targeted Financial Sanctions** في القطاع المصرفي بطرق متعددة، جميعها تسعى إلى إقامة علاقات مع مؤسسات القطاع المصرفي والنفاذ إلى النظام المالي العالمي لتجاوز قرارات العقوبات، وفيما يلي أهم هذه الطرق (Ereport, Fadlon, 2023):

أ. استخدام هياكل ملكية معقدة:

ويتم ذلك من خلال إنشاء شركات وهمية Sell Companies أو شركات واجهة Front Companies في دول مختلفة بهدف إخفاء هوية المستفيد الحقيقي أو النهائي Ultimate Beneficial Owner من الأموال، أو تسجيل الشركات باسم أفراد أو كيانات غير مدرجة على قوائم العقوبات أو الجزاءات، ولكنها تعمل نيابة عن جهات خاضعة للعقوبات أو الجزاءات.

ب. التحايل على الأنظمة المصرفية:

ويتم ذلك من خلال عدة طرق، منها تقديم مستندات مزورة أو معلومات غير دقيقة خلال عملية فتح الحسابات، واستغلال ضعف إجراءات التعرف على العملاء في المؤسسات المصرفية لإخفاء هوية الأفراد أو الكيانات الخاضعين للعقوبات، كما يتم أيضا من خلال تعديل أسماء أو تفاصيل المستفيدين في أنظمة الدفع لتحويل الأموال إلى جهات خاضعة للعقوبات دون الكشف عن ذلك، أو استخدام أسماء بديلة أو مترادفات للأفراد أو الكيانات المدرجة على قوائم العقوبات لتجنب الاكتشاف أثناء الفحص.

ج. استخدام أطراف وسيطة Third Parties:

وفي هذه الطريقة يتم تنفيذ المعاملات المالية من خلال أطراف وسيطة غير مدرجة على قوائم العقوبات، ولكنها تعمل لصالح الكيانات أو الأفراد الخاضعين لها، ومن ثم يلي ذلك تحويل الأموال عبر شبكات معقدة من المؤسسات المصرفية أو الوسطاء الماليين لتجنب الكشف عن المستفيد النهائي.

د. المعاملات المصرفية مع دول ضعيفة الامتثال:

وفي هذه الحالة يلجأ المجرمون إلى تنفيذ المعاملات المصرفية والمالية عبر دول أو مناطق لا تفرض رقابة صارمة على تنفيذ قرارات العقوبات، ومن ثمَّ الاستفادة من الأنظمة المصرفية في هذه الدول التي قد تكون غير مجهزة بشكل كافٍ لتطبيق قرارات العقوبات والجزاءات، كما قد يلجأون إلى استخدام مؤسسات مصرفية في دول ذات ضوابط مصرفية ضعيفة بشكل عام من أجل تحويل الأموال عبر عدة عملات مختلفة قبل إعادتها إلى النظام المصرفي مرة أخرى.

هـ. التلاعب بعمليات تمويل التجارة الدولية:

وفيها يتم استغلال معاملات تمويل التجارة الدولية International Trade Finance في المؤسسات المصرفية من خلال عدة طرق، مثل تضخيم أو تقليل قيمة الفواتير التجارية Over or Under Invoicing لتسهيل تحويل الأموال بين الدول، أو استخدام شحنات مزورة أو وثائق تجارية وهمية لإخفاء مصدر أو وجهة الأموال، وغيرها من الطرق الشبيهة.

و. استغلال الثغرات التقنية في أنظمة الامتثال في المؤسسات المصرفية:

حيث يتم استغلال نقاط الضعف في أنظمة الامتثال التقنية لمؤسسات القطاع المصرفي، وذلك من خلال استهداف مؤسسات ذات أنظمة امتثال ضعيفة أو قديمة لا تستطيع الكشف عن الأنشطة المشبوهة بفاعلية، أو الاعتماد على تأخر تحديث قوائم العقوبات والجزاءات في بعض المؤسسات المصرفية لتنفيذ المعاملات قبل إدراج الكيانات أو الأفراد على القائمة.

ز. استغلال التعاون بين المؤسسات المصرفية الدولية:

وخاصة استغلال علاقات المراسلة المصرفية Correspondent Banking من خلال تنفيذ التحويلات عبر مؤسسات مصرفية متعددة في دول متعددة وإخفاء تفاصيل المعاملات في الرسائل المالية بين المؤسسات المصرفية SWIFT لتجنب اكتشاف العلاقة مع الكيانات أو الأفراد الخاضعين للعقوبات.

ولذلك تعد مكافحة جريمة خرق قرارات العقوبات المالية المستهدفة Evasion of Targeted Financial Sanctions تحديًا معقدًا لمؤسسات القطاع المصرفي والمالي؛ نظرًا لما أوضحناه من تعدد طرق التحايل وصعوبة اكتشاف التعاملات غير المباشرة مع الأفراد والكيانات الخاضعة لهذه الجزاءات، وعليه يتعين على الدول والمؤسسات المالية والمصرفية تبني أنظمة رقابة صارمة، وتحديث أدوات الامتثال بشكل دوري لرصد أي أنشطة مشبوهة، كما يتطلب ذلك أيضًا تعزيز التعاون الدولي وتبادل المعلومات بين المؤسسات المصرفية والمالية والجهات التنظيمية الإشرافية والرقابية وجهات إنفاذ القانون المختلفة لتعزيز قدرات اكتشاف ومنع هذه الانتهاكات (Kavakli, Marcolongo, & Zambiasi, 2023).

5. جريمة الاحتيال المالي Financial Fraud :

منذ نشأة العمل المصرفي كانت جريمة الاحتيال المالي Financial Fraud - وما زالت - من أبرز التهديدات التي تواجه القطاع المصرفي، حيث تتسبب في خسائر بمليارات الدولارات سنويًا للمؤسسات المصرفية (Fan et al., 2025)، وقد أتاح التطور الكبير في مجالات الاتصالات Communication وتقنية المعلومات IT Technology ثم لاحقا الذكاء الاصطناعي AI فرصًا جديدة وغير مسبوقة للمحتالين للالتفاف على أنظمة الأمان التقليدية؛ مما جعل اكتشاف هذه الجرائم ومكافحتها أمرا أكثر تعقيدًا (Awosika et al., 2023)، وترتبط جريمة الاحتيال المالي ارتباطًا وثيقًا بالعديد من الجرائم الأخرى، كجريمة غسل الأموال Money Laundering وتمويل الإرهاب Terrorism Financingوتمويل انتشار التسلح Proliferation Financing، مما يعزز من خطورة تأثيرها على استقرار النظام المالي العالمي (Jiao, 2023)، ومن ناحية أخرى تُعرّض جرائم الاحتيال المؤسسات المصرفية المتورطة فيها لغرامات مالية ضخمة، وإجراءات رقابية وتنظيمية مشددة، وقد تصل إلى فقدان وسحب الترخيص المصرفي أو العزل عن النظام المالي الدولي (Zhang et al., 2025)، وهو ما يبرز من ثمَّ أهمية تطوير أدوات فعالة لكشف هذه الجريمة والحد منها للحفاظ على نزاهة النظام المالي والمصرفي.

وتعرف جريمة الاحتيال المالي عامة Financial Fraud بأنها: مجموعة من الأنشطة غير القانونية المتعمدة التي تهدف إلى تضليل الأفراد أو المؤسسات بغرض الحصول على منافع مالية أو غير مالية غير مستحقة؛ مما يتسبب في خسائر مالية أو غير مالية للضحية (Kulmie et al., 2023).

ويشمل الاحتيال المالي في القطاع المصرفي مجموعة متنوعة من الجرائم والأنشطة الفرعية التي تُصنف بشكل عام إلى احتيالات داخلية وخارجية، يشمل الاحتيال الداخلي Internal Fraud أفعالاً غير مشروعة من قبل الموظفين، مثل اختلاس الأصول وتزوير السجلات المالية والتلاعب بها، بينما يشمل الاحتيال الخارجي External Fraud أنشطة متعددة مثل سرقة الهوية ID Theft والتصيد الاحتيالي Phishing والهجمات الإلكترونية Cyber Attacks التي يرتكبها أفراد من خارج المؤسسة، وتستند التصنيفات الأخرى إلى طبيعة الاحتيال، بما في ذلك الاحتيال على بطاقات الائتمان، والاحتيال في الرهن العقاري، والاحتيال الإلكتروني، ولكل منها خصائص ومنهجيات مميزة (Ali, Rahman, & Carter, 2022).

وفي هذا الصدد **يرى الباحث** أنه يمكن تقسيم جرائم الاحتيال المالي Financial Fraud Crimes بالطريقة نفسها المتبعة سابقا في تقسيم أنماط الجرائم المالية Financial Crimes عامة في القطاع المصرفي، وذلك بالاعتماد على المعايير الستة نفسها للتقسيم أو التصنيف Classification Criteria، حيث يمكن تصنيف جرائم الاحتيال المالي Financial Fraud Crimes وفقا لمصدر التهديد Source of Threat، أو وسيلة ارتكاب الجريمة Method of Crime، أو وفقا لمرحلة العملية المصرفية التي يتم فيها ارتكاب الجريمة Stage of Banking Process، أو وفقا للفئة المستهدفة من الجريمة Targeted Party، كما يمكن تقسيمها وفقا لطبيعة المعاملة المالية Nature of Financial Transaction، وأخيرا يمكن تقسيم الجرائم المالية في القطاع المصرفي وفقا لمعيار حجم الأثر القانوني أو المالي الناتج عنها Financial or Legal Impact، وفي السطور التالية سنستعرض بعضا من أهم أنماط جرائم الاحتيال المالي Financial Fraud في القطاع المصرفي.

أ. الاحتيال الداخلي (المهني / الوظيفي) Occupational Fraud: (Association of Certified Fraud Examiners, 2022):

يشير مصطلح الاحتيال الداخلي أو ما يطلق عليه أيضا الاحتيال الوظيفي أو المهني Occupational Fraud إلى سوء استخدام الفرد لمهنته أو منصبه الوظيفي عمدًا لتحقيق إثراء شخصي من خلال إساءة استخدام موارد أو أصول المؤسسة التي يعمل بها، وعادة ما يُصنف الاحتيال الداخلي أو الوظيفي أو المهني Occupational Fraud إلى ثلاثة أنماط أو أشكال رئيسية، هي: أولاً اختلاس الأصول Asset Misappropriation، ثم الفسادCorruption وأخيرًا الاحتيال في البيانات المالية Financial Statement Fraud.

شكل رقم (9): أنماط الاحتيال الداخلي أو الوظيفي / شجرة الاحتيال الداخلي (العناوين الرئيسية فقط)

المصدر: مترجم من Association of Certified Fraud Examiners, 2022

1- الاحتيال في البيانات المالية Financial Statements Fraud :

يقصد بالاحتيال في البيانات المالية Financial Statements Fraud ذلك التحريف المتعمد في البيانات المالية للمؤسسة لخداع أصحاب المصلحة، مثل المستثمرين أو الدائنين أو الجهات التنظيمية، حول الوضع المالي الحقيقي للمؤسسة.،ويتم القيام بذلك من أجل تحقيق عدة منافع غير قانونية، منها مثلا محاولة جذب الاستثمارات، أو تحسين صورة الأداء المالي، أو تجنب العقوبات التنظيمية (Kythreotis, & Roshanpoor, 2023 Soltani,)، ويُعدّ الاحتيال في البيانات المالية، على الرغم من قلة حدوثه، الأكثر ضررًا ماليًا على مؤسسات القطاع المصرفي، حيث يكون متوسط الخسائر أعلى بكثير من الأنماط الأخرى، وتشمل أساليب الاحتيال في البيانات المالية (FSF) العديد من الأنماط، من أبرزها الأنماط التالية (Okolie et al. , 2023):

أ. **الإيرادات الوهمية Fictious Revenue:**

ويقصد بالإيرادات الوهمية تسجيل إيرادات غير حقيقية أو تسجيل الإيرادات قبل تحققها فعليًا.

ب. **اختلاف التوقيت Timing Differences:**

ويتمثل ذلك في التلاعب في توقيتات التسجيل، مثل تسجيل الإيرادات في فترات مالية غير صحيحة، أو تأجيل تسجيل المصاريف إلى فترات لاحقة؛ وذلك بهدف تحسين صورة الأداء المالي للفترة الحالية على حساب الفترات المستقبلية.

ج. **التقييمات الخاطئة للأصول Improper Asset Valuation:**

ويشمل ذلك تضخيم أو تقليل قيمة الأصول والالتزامات بشكل غير دقيق، فعلى سبيل المثال، يمكن تضخيم قيمة الأصول الثابتة أو تسجيل أصول وهمية، أو التقليل من قيمة الالتزامات لتظهر المؤسسة في وضع مالي أقوى مما هو عليه في الواقع.

د. **الالتزامات والمصروفات الخفية Concealed Liabilities and Expenses:**

ويتمثل ذلك في عدم تسجيل الالتزامات المالية بشكل كامل أو تقليل قيمتها عمدًا، وكذلك إخفاء المصروفات أو عدم الإبلاغ عنها بالشكل الصحيح، والهدف هو تحسين صافي الربح الظاهر وتقليل الأعباء المالية الظاهرة على المؤسسة.

هـ. **الإفصاح غير السليم Improper Disclosure:**

ويقصد به تقديم معلومات مضللة أو غير كاملة في الإيضاحات المرفقة بالقوائم المالية، وقد يشمل ذلك إخفاء تفاصيل مهمة عن العمليات المالية، مثل العقود الطويلة الأجل، أو عدم الإفصاح عن المخاطر المالية الحقيقية التي تواجهها المؤسسة.

2- اختلاس الأصول Asset Misappropriation:

يُعد اختلاس الأصول Asset Misappropriation أكثر أنماط الاحتيال الداخلي أو المهني شيوعًا، حيث يُمثل حوالي 89% من الحالات المُبلغ عنها عالميًا، وفقا لتقرير جمعية مُحققي الاحتيال المعتمدين (ACFE, 2024)، ويتضمن هذا النوع من الاحتيال استخدام أصول المؤسسة أو سرقتها دون تصريح من قِبل الموظفين أو الأفراد المُؤتمنين عليها (Dorris & Cummings, 2023)، وتشمل المخططات الشائعة في هذا النمط من الاحتيال ممارسات مثل سرقة النقد Theft of Cash، والصرف الاحتيالي Fraudulent Disbursements، والاحتيال في الرواتب Payroll Schemes، ومخططات الفوترة Billing Schemes، والاحتيال في استرداد النفقات والمصروفات

Expense Reimbursement Schemes، وكذلك سرقة المخزون Inventory Theft (Johari et al., 2022). وعلى الرغم من تكرار ارتكابه، إلا أن اختلاس الأصول Asset Misappropriation عادةً ما يُسفر عن متوسط خسائر أقل مقارنةً بأنواع الاحتيال الأخرى، وغالبًا ما يُعزى ارتفاع معدل حدوث مثل هذا النمط من الاحتيالات إلى العوامل ذات الصلة بالبيئة الداخلية وثقافة الالتزام في المؤسسة؛ مما يؤكد على أهمية تطوير وتنفيذ ضوابط داخلية قوية وتعزيز ثقافة تنظيمية أخلاقية من أجل التخفيف من مثل هذه المخاطر ومكافحتها (Siddiq & Sutopo, 2024).

3- الفساد Corruption:

تشكل جريمة الفساد Corruption مخاطر كبيرة على مؤسسات القطاع المصرفي، ويعزى ذلك لأثارها السلبية المختلفة، ومنها تقويضها للاستقرار المالي لهذه المؤسسات، وزيادة مخاطر الائتمان لديها، وتآكل ثقة أصحاب المصلحة بها، ويُعرَّف الفساد Corruption عادةً بأنه إساءة استخدام السلطة الموكلة لتحقيق مكاسب شخصية، ويشمل مجموعة واسعة من السلوكيات غير الأخلاقية التي تُقوِّض نزاهة المؤسسات وثقة الجمهور (Transparency International, 2023)، وقد أثبتت الدراسات المتخصصة وجود علاقة طردية بين ارتفاع مخاطر الفساد وارتفاع مخاطر الائتمان Credit Risk، كما يتضح من ارتفاع نسب القروض المتعثرة، حيث تنشأ هذه العلاقة عندما تؤدي بعض ممارسات الفساد في المؤسسات المصرفية، مثل الرشوة Bribery والمحسوبية Favoritism، إلى موافقة هذه المؤسسات على منح قروض عالية المخاطر قد لا تُسدد، مما يزيد من احتمالية التخلف عن سداد القروض (Hasan & Ashfaq, 2021)، وفي المناطق التي ينتشر فيها الفساد Corruption، غالبًا ما تشهد المؤسسات المصرفية انخفاضًا في الربحية وتفاقمًا في عدم الاستقرار المالي، حيث تُقوّض الأنشطة الفاسدة ممارسات الإقراض الحكيمة وبروتوكولات تقييم المخاطر. علاوة على ذلك، يُمكن للفساد أن يُشوّه تخصيص الموارد، ويُعيق إنفاذ اللوائح، ويُسهّل ارتكاب الجرائم المالية الأخرى كجريمة غسل الأموال Money Laundering مما يُفاقم نقاط الضعف النظامية في القطاع المصرفي (Mansoori, 2023).

وتشمل جريمة الفساد Corruption ممارسات غير أخلاقية وغير قانونية متنوعة ومتعددة تُقوّض نزاهة المؤسسة المصرفية وثقة الجمهور بها، ويُعدّ تضارب المصالح Conflict of Interest، والرشوة Bribery، والإكراميات غير القانونية Illegal Gratuities، والابتزاز الاقتصادي Economic Extortion من أكثر مظاهر الفساد ضررًا، وفيما يلي نظرة سريعة على كل نمط من هذه الأنماط:

أ. **تضارب المصالح Conflict of Interest:**

ينشأ تضارب المصالح عندما يُعطي الأفراد في مناصب السلطة الأولوية للمكاسب الشخصية على واجباتهم المهنية، مما يؤدي بهم إلى اتخاذ قرارات قد لا تتوافق مع مصالح المؤسسة أو المصلحة العامة (Antonov & Lineva, 2021).

ب. **الرشوة Bribery:**

تتضمن الرشوة عرضًا أو تلقي شيئًا ذا قيمة للتأثير على تصرفات فرد في موقع سلطة، وهو شكلٌ متفشٍّ من الفساد يُشوّه عمليات صنع القرار ويُقوّض المعايير الأخلاقية (Olimov, 2025).

ج. **الإكراميات غير القانونية Illegal Gratuities:**

ويقصد بها تقديم هدايا أو خدمات للمسؤولين بعد اتخاذ قرار، كمكافأة على المعاملة التفضيلية، ورغم أنها قد لا تؤثر بشكل مباشر على القرارات الصادرة، إلا أنها تُعرّض نزاهة السلوك المهني للخطر (Antonov & Lineva, 2021).

د. **الابتزاز الاقتصادي Economic Extortion:**

ويتضمن ذلك إجبار الأفراد أو المؤسسات على تقديم مدفوعات أو خدمات تحت التهديد، وغالبًا ما يستغل المجرمون في هذا النمط مناصب السلطة لانتزاع منافع غير مستحقة لهم (Rusev, 2024).

ويُعد فهم هذه الأشكال من الفساد أمرًا بالغ الأهمية لتطوير إستراتيجيات فعّالة للوقاية والتنفيذ في القطاعين العام والخاص، حيث يتطلب تعقيد وانتشار هذه الأنواع من الفساد اتباع نُهُج متعددة الجوانب للوقاية والإنفاذ، مُصممة خصيصًا لسياقات وقطاعات مُحددة؛ لذا تُعدّ التدابير الصارمة لمكافحة الفساد وسياسات الحوكمة الشفافة أمرًا ضروريًا لحماية نزاهة المؤسسات المالية ومرونتها (El Jabri & El Khider, 2022).

ب. التزييف والتزوير Counterfeiting and Forgey:

تعد جرائم تزوير المستندات Document Forgey وتزييف الأوراق النقدية Banknote Counterfeiting من جرائم الاحتيال المالي الخطيرة التي تُقوّض الثقة في الأنظمة المصرفية والمالية واستقرارها، وتشمل جريمة تزوير المستندات في مؤسسات القطاع المصرفي Document Forgey تغيير أو إنشاء أو تقليد المستندات ذات الصلة بالمعاملات والعمليات المصرفية، مثل الشيكات أو أوراق الهوية أو اتفاقيات القروض، سواء كان ذلك التزوير جزئيًا أو كليًا، بغرض خداع المؤسسات أو الأفراد (Inscribe AI, 2025). بينما تشمل الأنواع الشائعة من المستندات المزورة بطاقات الهوية المزورة، والفواتير المُتلاعب بها، والتوقيعات والاختام المزورة، ومن ناحية أخرى يُشير تزييف الأوراق النقدية Banknote Counterfeiting إلى إعادة إنتاج العملة بشكل غير قانوني بقصد تداولها على أنها أصلية، وغالبًا ما يتم ذلك باستخدام تقنيات طباعة متقدمة (Federal Reserve, 2025). ولا يزال تزييف الأوراق النقدية يُشكّل مشكلةً مُستمرةً على الرغم من التطورات الكبيرة في العلامات الأمنية في العقدين الأخيرين، ولمواجهة ذلك طبقت المصارف والبنوك المركزية علامات وخصائص أمنية متطورة، بما في ذلك الصور المجسمة Hologram والأحبار متغيرة الألوان Color Shifting Inks والعناصر اللمسية Touch-sensitive Elements، وذلك للمساعدة في التحقق من صحة أوراق العملات النقدية وتمييزها من المزيفة (Reserve Bank of Australia, 2022)؛ ولذلك يجب على مؤسسات القطاع المصرفي أن تظل يقظَة ضد هذه الأشكال من الاحتيال من خلال اعتماد عمليات تحقق دقيقة، والاستثمار في تقنيات الكشف المتقدمة، وتعزيز الوعي العام لحماية الأنظمة المالية والمصرفية.

ج. احتيالات بطاقات الائتمان Credit Card Fraud:

يُعدّ احتيال بطاقات الائتمان Credit Card Fraud من أكثر الجرائم المصرفية شيوعًا في العقود الثلاثة الأخيرة، وتعرف جرائم احتيالات بطاقات الائتمان Credit Card Fraud بأنها نمط من الجرائم المالية يتعلق بسرقة معلومات بطاقات الائتمان واستخدامها بشكل غير قانوني لشراء سلع أو خدمات أو لسحب أموال دون إذن من صاحب البطاقة، ويتم سرقة معلومات البطاقة من خلال عدة طرق من بينها استخدام الاحتيال إلكتروني Electronic Fraud عبر شبكة الإنترنت من خلال استخدام حيل مثل التصيد الإلكتروني Phishing، أو من خلال استخدام وسائل يدوية مثل استخدام جهاز قارئ البطاقات Crad Reader يُستخدم لنسخ بيانات البطاقة Skimming مما يؤدي إلى خسائر على مستوى العملاء من الأفراد والمؤسسات، وكذلك المؤسسات المصرفية والمالية المصدرة لهذه البطاقات، كما يمكن أن يؤدي إلى تبني تدابير أمان إضافية تكلف المؤسسات بدلاً من زيادة الأمن (Afjal et al., 2023).

د. الاحتيال في القروض المصرفية Bank Loans Fraud (Afjal et al., 2023):

يشير الاحتيال في القروض المصرفية Bank Loans Fraud إلى تقديم معلومات مضللة أو مزورة عمدًا من قبل المقترضين أو موظفي المؤسسة المصرفية ذاتها أو كلاهما للحصول على موافقات أو صرف قروض بشكل غير مستحق وغير قانوني، مما يشكل تهديدًا جسيمًا لاستقرار القطاع المصرفي وثقة الأطراف ذات العلاقة بالمؤسسات المصرفية، وثقة المؤسسات المصرفية ذاتها، وتتعدد وتتنوع أشكال هذا النمط من الاحتيال، ولكن يتمثل أبرزها في الأنماط التالية:

1. **احتيالات الهوية:** حيث يستخدم المحتالون معلومات أو بيانات شخصية مسروقة للحصول على القروض.
2. **تزوير المستندات:** وذلك عن طريق تزوير المستندات المالية، مثل كشوف الرواتب للمبالغة في الدخل لتلبية شروط القرض.
3. **احتيال الضمانات:** ويتضمن تضخيم قيمة الأصول المقدمة، كضمان للقروض أو تقديم ضمانات وهمية لا وجود لها.

ولا تؤدي هذه الممارسات الاحتيالية إلى خسائر مالية مباشرة فحسب، بل تزيد أيضًا من مخاطر الائتمان، حيث قد تمنح المؤسسات المصرفية ائتمانًا وتمويلات وقروضًا لمقترضين غير مؤهلين، مما يؤدي إلى ارتفاع معدلات التخلف أو التعثر في السداد، بالإضافة الى المخاطر القانونية والتنظيمية ومخاطر السمعة المترتبة على ذلك، بالإضافة إلى ذلك أصبحت هذه الاحتيالات أكثر تعقيدًا مع التطورات التكنولوجية، مما يجعل اكتشافها أكثر صعوبة، ولمكافحة هذه الظاهرة، يتعين على المؤسسات المصرفية تنفيذ إجراءات تحقق قوية والاستفادة من أدوات التحليل المتقدمة للتخفيف من مخاطر الاحتيال في القروض المصرفية (Esmail et al., 2023).

هـ. الجرائم الإلكترونية أو السيبرانية Cyber Crimes:

أصبحت الجرائم الإلكترونية أو السيبرانية Cyber Crimes في القطاع المصرفي أكثر تعقيدًا وتطورًا، مما يشكل تهديدات جسيمة للاستقرار المالي وثقة العملاء، نظرًا لاستهدافها المباشر للأصول المالية وبيانات العملاء والأنظمة التشغيلية، ويشير مصطلح الجرائم الإلكترونية أو السيبرانية Cyber Crimes في القطاع المصرفي إلى الأنشطة غير المشروعة التي تستغل التقنيات الرقمية مثل أجهزة الحاسب الألي وأنظمته وشبكة الإنترنت لاختراق الأنظمة المالية للمؤسسات المصرفية وسرقة البيانات الحساسة، أو تعطيل العمليات المصرفية (Waliullah et al., 2025)، ونستعرض فيما يلي أبرز التهديدات الإلكترونية أو السيبرانية في القطاع المصرفي:

1. **هجمات التصيد الاحتيالي Phishing Attacks**:

حيث ينتحل المحتالون هوية مؤسسات مصرفية شرعية لخداع عملاء أو موظفي المؤسسة المصرفية من خلال إرسال رسائل بريد إلكتروني أو نصية مزيفة وكشف معلومات سرية حساسة، مثل كلمات المرور أو أرقام الحسابات أو بيانات الهوية الشخصية ومن ثم سرقة أموال العملاء أو المؤسسة المصرفية (Kulmie et al., 2023).

2. **هجمات البرمجيات الخبيثة Malware Attacks**:

حيث يقوم المحتالون بتطوير واستخدام برمجيات ضارة لاختراق الأنظمة المصرفية والوصول غير المصرح به إلى البيانات الشخصية الحساسة لسرقتها أو تعطيل العمليات المصرفية أو تحويل الأموال سرًا (Darem et al.,2023).

3. **هجمات برامج الفدية Ransomware Attacks**:

يقوم المحتالون بتعطيل أنظمة المؤسسات المصرفية أو تشفير بياناتها وطلب فدية مالية مقابل استعادة الوصول لهذه البيانات (Darem et al.,2023).

4. **هجمات اختراق البريد الإلكتروني المؤسسيBusiness Email Compromise**:

وهي الهجمات التي تستهدف موظفي المؤسسات المصرفية من خلال اختراق حسابات البريد الإلكتروني لهذه المؤسسات لحثهم على تنفيذ تحويلات نقدية احتيالية من خلال تزوير التعليمات وتحويل الأموال بشكل احتيالي (Darem et al.,2023).

5. **هجمات حجب الخدمة الموزعة Distributed Denial-of-Service (DDoS)**:

وهي الهجمات التي تعطل الخدمات المصرفية عبر إغراق الأنظمة وخوادم المؤسسات المصرفية بحجم هائل من الطلبات الوهمية لتعطيل خدماته وإلحاق ضرر مالي أو تشويه سمعة المؤسسة المصرفية (Kulmie et al., 2023).

6. **هجمات اختراق أجهزة الصراف الآلي ATM Skimming**:

ويتم ذلك من خلال تركيب أجهزة خفية على ماكينات الصراف الآلي لسرقة بيانات البطاقات المصرفية المستخدمة فيها بأنواعها المختلفة وأرقامها السرية (Kulmie et al., 2023).

7. **الاستيلاء على الحسابات المصرفية Account Takeover**:

ويتم ذلك عن طريق اختراق حسابات العملاء المصرفية عبر الإنترنت لتنفيذ عمليات مالية غير مصرح بها (Kulmie et al., 2023).

8. **التهديدات الداخلية Insider Threats**:

ويقصد بها إساءة استخدام الموظفين لصلاحياتهم الوظيفية واختراق البينات والوصول غير المصرح به للمعلومات الحساسة الخاصة بالعملاء لسرقة الأموال أو البيانات (Darem et al.,2023).

رابعًا: الاتجاهات والتحديات الناشئة في الجرائم المالية في القطاع المصرفي:

تعد الجرائم المالية واحدة من أبرز التحديات التي تواجه النظم الاقتصادية والمجتمعات في العصر الحديث، حيث أصبحت الجرائم تتطور باستمرار وبسرعة كبيرة، مما يتطلب من الأطراف المختلفة ذات الصلة، كالحكومات وجهات إنفاذ

القانون والهيئات الإشرافية والرقابية التنظيمية والمؤسسات المالية والمصرفية، تطوير إستراتيجيات جديدة لمواجهتها، ومع التطورات التكنولوجية والتغيرات الاقتصادية العالمية، ظهرت اتجاهات وتحديات جديدة تؤثر على كيفية مكافحة هذه الجرائم، وهي الاتجاهات والتحديات التي سوف يستعرضها الباحث فيما يلي:

1- التقدم التكنولوجي وتصاعد التطور في الجرائم المالية:

وفر التقدم التكنولوجي والتقنيات الجديدة أدوات جديدة للجماعات الإجرامية طورت من خلالها تقنيات ارتكاب الجرائم المالية، ومن أمثلتها: العملات الرقمية أو الافتراضية Digital or Virtual Currencies، وتقنيات سلاسل الكتل Blockchain Technology. وقد نتج عن هذه التقنيات سهولة إخفاء الهوية وصعوبة تتبع المعاملات، وهو ما أسهم في زيادة وتيرة وحجم الجرائم المالية، مثل غسل الأموال والاحتيال، كما أدى هذا التقدم التكنولوجي إلى التطور في استخدام أساليب الهجمات السيبرانية Cyber Attacks، مثل هجمات الفدية والاختراقات الأمنية للحصول على معلومات حساسة أو أموال من الأفراد والشركات (Singh et al., 2024) .

2- الطابع العابر Trans-Border Nature للحدود للجرائم المالية والتحديات القضائية:

يعد الطابع العابر للحدود للجرائم المالية Nature of Financial Crimes Trans-Borders والتحديات ذات الصلة باختلاف الولايات القضائية من أبرز التحديات الناشئة في الجرائم المالية، ويعود ذلك إلى انتشار الجرائم المالية الدولية، فغالبًا ما تتم الجرائم المالية عبر الحدود، وهو ما يجعل من الصعب على السلطات القضائية وجهات إنفاذ القانون المختلفة تنفيذ القوانين بشكل فعّال؛ إذ يتطلب ذلك تعاونًا دوليًا بين الهيئات القضائية وجهات إنفاذ القانون الدولية والوطنية المختلفة، كما أدى اختلاف التشريعات والقوانين المنظمة لمكافحة الجرائم المالية بين الدول لإعاقة عمليات التحقيق والمقاضاة بسبب بعض الفجوات والاختلافات القانونية التي تؤدي إلى سهولة إخفاء بعض الجرائم المالية أو تمكين مرتكبيها من الهروب من العقوبات (Adaga et al., 2024).

3- التغيرات التنظيمية ومتطلبات الامتثال المتطورة:

تعد التغيرات التنظيمية ومتطلبات الامتثال المتطورة من أبرز التحديات الناشئة في الجرائم المالية؛ لذلك يتعين على الحكومات أن تلجأ إلى تشديد القوانين واللوائح المالية لمواكبة التطورات التكنولوجية والإجرامية، ومن جانب آخر يتطلب ذلك من المؤسسات المالية الالتزام بمعايير أكثر صرامة، مثل مبدأ اعرف عميلك Know Your Customer – KYC، وتدابير العناية الواجبة بالعملاء Customer Due Diligence وإجراءات مكافحة غسل الأموال Anti-Money Laundering Procedures، كما يتطلب ذلك أيضا دراسة المتغيرات الناتجة عن تأثير العولمة، حيث تنعكس التغيرات الاقتصادية العالمية على كيفية كشف ومكافحة ومراقبة الجرائم المالية، فقد أصبح يتوجب على المؤسسات المصرفية التعامل مع أنظمة قانونية وتنظيمية ومصرفية مختلفة ومتطلبات مختلفة في مناطق جغرافية متنوعة (Thommandru & Chakka, 2024).

4- مخاوف الخصوصية وما يتعلق بحماية البيانات في تحقيقات الجرائم المالية:

تؤدي التحقيقات في الجرائم المالية، سواء تلك التي تتم في المؤسسات المصرفية أو بواسطة جهات إنفاذ القانون، إلى التداخل بين متطلبات حماية البيانات الشخصية وحقوق العملاء من ناحية، وضرورة جمع المعلومات الضرورية اللازمة لإنجاز هذه التحقيقات من ناحية أخرى؛ لذلك يجب على السلطات المختصة التأكد من أن إجراءات التحقيق لا تتعارض مع القوانين الخاصة بحماية الخصوصية وبيانات العملاء، كما يتعين على جهات التحقيق أيضا تحقيق التوازن بين حماية الحقوق الفردية والكشف عن الجرائم المالية (Singh et al., 2024).

خامسًا: الآثار المترتبة على الجرائم المالية في القطاع المصرفي:

لا تقتصر الخسائر الناتجة عن الجرائم المالية في القطاع المصرفي على الخسائر المالية المباشرة التي يتعرض لها العملاء أو باقي أطراف العلاقة أو المؤسسات المصرفية ذاتها فقط، بل تشمل هذه الخسائر مجموعة كبيرة من الآثار متعددة الأبعاد التي يمكن أن تؤثر على استقرار الاقتصاد والمجتمع ككل وليس فقط مؤسسات القطاع المصرفي أو المالي، وتنقسم الآثار المترتبة على الجرائم المالية إلى ما يلي (Sibe, & Kaunert,2024):

1. الخسائر المالية المباشرة للعملاء والمؤسسات المصرفية:

تتنوع هذه الخسائر بين نمطين مختلفين كالتالي:

أ. الخسائر الفردية:

يتعرض عملاء المؤسسات المصرفية، سواء كانوا أفرادًا أو مؤسسات أعمال، لسرقة الأموال الخاصة بهم، سواء من خلال هجمات الجرائم السيبرانية أو الهجمات المباشرة، مثل عمليات الاحتيال على بطاقات الائتمان، وقد تؤدي هذه الخسائر الفردية إلى صعوبات مالية تؤثر على نوعية حياة ومدخرات العملاء من الأفراد، مسببة لهم العديد من المشكلات والأضرار (Gupta, et al. , 2023).

ب. الخسائر المؤسسية:

تتعرض المؤسسات المصرفية أيضا لخسائر مالية بسبب سرقة الأموال، والتلاعب في الحسابات، والاحتيال الداخلي، كما تشمل هذه الخسائر أيضًا تكاليف استعادة الأموال المفقودة والعقوبات أو الغرامات القانونية والتنظيمية والتعويضات المطلوبة، بالإضافة إلى التكاليف الأخرى المترتبة على ذلك مثل تكاليف التحقيقات الداخلية، كما قد تؤثر أيضا على استقرار المؤسسات المصرفية ذاتها واستمراريتها (Gupta, et al. , 2023).

2. الآثار المالية غير المباشرة على المؤسسات المصرفية والاقتصادات الوطنية:

يترتب على الجرائم المالية في القطاع المصرفي العديد من الآثار المالية غير المباشرة، وتشمل على سبيل المثال:

أ. العواقب الطويلة الأمد على الاستقرار المالي Financial Stability والثقة:

1. التأثير على الاستقرار المالي Financial Stability:

يمكن أن تؤدي الجرائم المالية، مثل جريمة غسل الأموال، إلى عدم استقرار القطاع المصرفي، حيث يتم استخدام المؤسسات المصرفية كأدوات لنقل الأموال غير المشروعة، وهو ما يمكن أن يشكل خطرًا على السيولة، وقد يؤدي إلى مخاطر التركز والانكشاف Concentration & Exposure Risk ويزيد من التكلفة المالية للمؤسسات (Kulmie, et al ,2023) .

2. التأثير على الثقة:

تؤدي الجرائم المالية إلى فقدان الثقة في النظام المصرفي والمالي، مما قد يدفع المستثمرين والمودعين إلى سحب أموالهم وودائعهم أو تقليل استثماراتهم، كما قد يؤدي انخفاض الثقة إلى تراجع النشاط الاقتصادي بشكل عام، حيث تتردد المؤسسات والأفراد في القيام بالمعاملات المالية والمصرفية (Gupta, et al. , 2023).

ب. مخاطر السمعة Reputation Risks:

1. تأثير السمعة السلبية على الأعمال:

تعد سمعة المؤسسة المصرفية أحد الأصول الأساسية التي تعتمد عليها في جذب الأعمال والعملاء، ومن ثمَّ يمكن أن تؤدي أي أزمة ذات صلة بالسمعة إلى فقدان الثقة والعملاء، كما يمكن أن تتسبب الجرائم المالية في تدمير سمعة المؤسسات المصرفية، مما يؤثر على قدرتها على جذب كلا من العملاء والشركاء التجاريين والاستثماريين على حد سواء (Gupta, et al. , 2023).

2. زيادة التكاليف:

قد تضطر المؤسسات المصرفية التي تتعرض لجرائم مالية إلى استثمار مبالغ كبيرة في برامج تحسين السمعة والتسويق والعلاقات العامة لإعادة بناء الثقة مع العملاء والشركاء التجاريين والاستثماريين (Kulmie et al ,2023) .

ج. المخاطر القانونية والتنظيمية Legal & Regulatory Risks:

تشمل هذه المخاطر نوعين أو نمطين مختلفين، وذلك كالتالي:

1. العقوبات الإدارية والقانونية Admin & Legal Penalties:

قد تواجه المؤسسات المصرفية التي تتورط في الجرائم المالية عقوبات مالية وإدارية من جهات الإشراف والرقابة، كما قد تواجه عقوبات قانونية شديدة، بما في ذلك الغرامات والتعويضات والإجراءات القضائية، وهي العقوبات التي يمكن أن تؤدي إلى تراجع الأداء المالي وتقليل قدرة المؤسسة على النمو (Gupta et al. , 2023).

2. التعقيدات التنظيمية:

من أجل بقاء المؤسسات المصرفية متوافقة وممتثلة Compliant مع التشريعات والقوانين والقواعد التنظيمية المتطورة والمتزايدة المتعلقة بمكافحة الجرائم المالية، يجب على هذه المؤسسات ضخ استثمارات مستمرة في البنية التحتية والموارد البشرية مع القيام بعمليات تطوير تنظيمية مستمرة لبيئتها الداخلية، وهو ما يكبدها تكاليف إضافية قد تؤثر على ربحيتها بصورة كبيرة (Butt et al., 2022).

د. المخاطر الاجتماعية والاقتصادية والسياسية Social, Economic & Political Risks:

ترتبط هذه المخاطر بالمجتمع والدولة التي تقع فيها المؤسسات المصرفية وترتكب فيها الجرائم، وتتمثل هذه المخاطر فيما يلي:

1. المخاطر الاجتماعية Social Risks:

يؤدي ارتفاع معدلات ارتكاب الجرائم المالية إلى زيادة الفجوة الاجتماعية بين طبقات المجتمع المختلفة، ويعود السبب في ذلك إلى أن الفئات الضعيفة في المجتمع تعاني بشكل أكبر من الآثار السلبية لهذه الجرائم، مما يزيد من الفقر وعدم المساواة، كما قد تتسبب الجرائم المالية أيضًا في قلق عام وزيادة عدم الاستقرار الاجتماعي (Gupta et al. , 2023).

2. المخاطر الاقتصادية Economic Risks:

يمكن أن تؤدي الجرائم المالية إلى انخفاض في الاستثمارات الأجنبية في الدولة بشكل عام، حيث قد ينظر المستثمرون إلى الدول التي تعاني من انتشار هذه الجرائم وارتفاع معدلاتها على أنها غير مستقرة أو غير آمنة، ومن جانب آخر قد تؤدي هذه الجرائم أيضا إلى انكماش الأداء الاقتصادي العام، حيث تتراجع الأنشطة التجارية (Achim et al., 2021).

3. المخاطر السياسية Political Risks:

قد يتسبب ارتفاع معدلات الجرائم المالية في دولة ما في حدوث حالة من عدم الاستقرار السياسي بها، حيث يؤدي ذلك إلى تداعيات واضطرابات سياسية، كما قد تؤدي الجرائم المالية الممنهجة إلى فقدان الثقة في الحكومات والهيئات التنظيمية، مما يثير موجات من الإضرابات والاحتجاجات أو عدم الاستقرار (Achim, et al. , 2021).

سادسًا: إدارة مخاطر الجرائم المالية في القطاع المصرفي:

تعد عملية إدارة مخاطر الجرائم المالية في المؤسسات المصرفية جزءًا مهمًا من عمليات إدارة المخاطر الشاملة في هذه المؤسسات، حيث تحتاج المؤسسات المصرفية إلى تفعيل إستراتيجيات استباقية فعالة لتحديد وتقييم والتخفيف من هذه المخاطر، كما تتطلب إدارة مخاطر الجرائم المالية في القطاع المصرفي التزامًا مستمرًا من المؤسسات المالية لمعالجة هذه المخاطر بشكل فعال، وتتطلب هذه العملية استخدام أساليب تحليلية وتكنولوجيا حديثة، مما يمكن أن يسهم في تقليل الخسائر الناتجة عن هذه الجرائم والاحتفاظ بثقة العملاء في النظام المصرفي، علاوةً على ذلك يعد تعزيز ثقافة الامتثال والتدريب المستمر للموظفين عنصرين أساسيين في تعزيز مرونة المؤسسات المصرفية في مواجهة مخاطر الجرائم المالية، وفيما يلي شرح تفصيلي لمفهوم المخاطر وعملية الإدارة الخاصة بها (Tatineni & Mustyala, 2024).

1. تعريف مخاطر الجرائم المالية ومفهومها:

يعرف "**الخطر Risk** " عامة بأنه: النتيجة غير المتوقعة وغير المرغوب فيها التي تحدث بسبب عوامل مختلفة، ودائما ما يكون اتجاه الخطر معاكسا لاتجاه الهدف الذي يجب تحقيقه، أما "**المخاطرة**": فهي تُشير إلى احتمالية وقوع ذلك الخطر أو الحدث

غير المرغوب فيه، وما يترتب عليه من عواقب سلبية، بمعنى آخر: المخاطر هي تقدير لمدى احتمالية وقوع الخطر وحجم الضرر الذي قد يسببه (Sleimi, 2020)، وبالنسبة للمنظمات تعرف "**المخاطر Risks**" على أنها: تأثير أي حالة من عدم اليقين على أهداف المنظمة أو عواقب بعض الأحداث، سواء من داخل المنظمة أو خارجها (Azuma-Kotei & Ibrahim, 2024)، وفي سياق الجرائم المالية في المؤسسات المصرفية، تشير مخاطر الجرائم المالية إلى احتمالية أن تتعرض المؤسسة المصرفية لتهديد أو أنشطة غير مشروعة قد ينتج عنها خسائر أو عواقب سلبية تهدد نزاهتها واستقرارها وموثوقيتها(Berry et al., 2023).

2. تعريف إدارة مخاطر الجرائم المالية ومفهومها:

عرف (المغربي، 2020) إدارة المخاطر Risk Management بكونها نظامًا متكاملاً وشاملاً لتهيئة البيئة المناسبة والأدوات اللازمة لتوقع ودراسة المخاطر المحتملة، وتحديدها وقياسها، وتحديد مقدار آثارها المحتملة على أعمال المنظمة، وأصولها وإيراداتها، ووضع الخطط المناسبة لما يلزم وما يمكن القيام به لتجنب هذه المخاطر أو لكبحها والسيطرة عليها وضبطها، للتخفيف من آثارها إن لم يكن القضاء على مصادرها.

في حين عرف (النسور وبقيلة،2022) إدارة المخاطر في المؤسسات المصرفية in Banking Risk Management بأنها: عملية تقييم للمخاطر التي تواجه المؤسسات المصرفية والعمل على تطوير إستراتيجيات معاصرة لأجل إدارتها، تحتوي على تجنب هذه المخاطر والحد منها قدر الإمكان.

أما إدارة مخاطر الجرائم المالية في القطاع المصرفي in Banking Financial Crime Risk Management فتشير إلى الإطار الشامل للسياسات والإجراءات والضوابط التي تنفذها المؤسسات المصرفية لتحديد وتقييم وتخفيف ومراقبة المخاطر المرتبطة بالأنشطة المالية غير المشروعة والتي تتطلب في الوقت ذاته الامتثال للمعايير الدولية جنبا إلى جنب مع التكيف مع التهديدات الناشئة (Demekas et al., 2023).

3. مراحل عملية إدارة مخاطر الجريمة المالية في القطاع المصرفي:

وفقًا لـ (Demirović et al., 2022)، تتضمن عملية إدارة مخاطر الجرائم المالية Financial Crime Risk Management في مؤسسات القطاع المصرفي عادةً أربع مراحل رئيسية، وهي كما يلي:

أ. مرحلة تحديد الخطر Risk Identification:

يقصد بمرحلة تحديد المخاطر Risk Identification عملية بدء الإجراءات، وخلق الوعي، ووجهة النظر المشتركة والالتزامات، وكذلك توضيح التوقعات فيما يتعلق بالمخاطر، ويمكن تحقيق ذلك من خلال وضع القواعد لتحديد المخاطر، والتي تحاول تحديد مخاطر محددة من خلال عوامل الخطر (Sleimi, 2020)، كما عرفها (Kuntar & Sari, 2023) بأنها: عملية اكتشاف المخاطر التي قد تؤثر على أهداف أو أغراض المؤسسة، وهي خطوة أولى بالغة الأهمية في عملية إدارة المخاطر، حيث إنها تسمح للمؤسسات بالتعرف على التهديدات المحتملة قبل أن تؤثر على العمليات، وتتضمن تحديد المخاطر وتوثيقها بشكل منهجي لضمان إمكانية إدارتها والتخفيف منها بشكل فعال.

وفي هذه المرحلة يتم تحديد المخاطر الكامنة Inherent Risk، والتي تمثل مستوى الخطر الموجود قبل تطبيق أي ضوابط، حيث إن فهم المخاطر الكامنة أمر بالغ الأهمية لتنفيذ نهج قائم على المخاطر Risk-based Approach (Velez, 2024)، ويتم التعرف على المخاطر الكامنة المحتملة التي يمكن أن تؤثر على العمليات المصرفية من خلال عدة طرق، منها:

1. تحليل البيانات التاريخية ومراجعة الحالات السابقة للجرائم المالية داخل المؤسسة المصرفية ذاتها أو في القطاع المصرفي والمالي عمومًا (Clintworth, et al., 2023).
2. مراجعة ورصد الأنشطة أو المعاملات غير الطبيعية التي قد تشير إلى وجود مخالفات (Gaviyau & Sibindi, 2023).
3. التواصل مع إدارات الامتثال ومكافحة الجرائم المالية وجمع المعلومات من الفرق المختصة داخليًا (Tatineni & Mustyala, 2024).
4. استخدام تقارير الجهات التنظيمية محليا ودوليا والاستفادة من التحذيرات والتنبيهات الصادرة عنها (Berry et al., 2023).

5. التقييم الداخلي للمخاطر وعقد ورش عمل واستبانات لجمع رؤى العاملين في المؤسسة المصرفية حول مصادر المخاطر المحتملة (Berry et al., 2023).
6. الاستعانة بوسائل التكنولوجيا وأدوات تحليل البيانات لاكتشاف الأنماط المشبوهة (Yan & Juma'h, 2023).
7. مراقبة التغيرات في البيئات القانونية والاقتصادية والسياسية التي قد تؤثر على مستوى الجرائم المالية (Berry et al., 2023).

ب. مرحلة تحليل وتقييم الخطر Risk Analysis and Evaluation:

يقصد بتحليل وتقييم مستوى المخاطر Risk Analysis and Evaluation العملية المنهجية التي تهدف إلى فهم طبيعة المخاطر الكامنة المحتملة Possible Inherent Risk التي قد تواجه المؤسسة من خلال تحديد مصادرها، والأحداث المحتملة المرتبطة بها، وأسبابها، ومدى احتمالية حدوثها، بالإضافة إلى تقدير نتائجها المحتملة وتأثيرها على أداء المؤسسة، وتشمل هذه العملية استخدام أدوات وأساليب كمية ونوعية لقياس شدة هذه المخاطر وتقدير أثرها الفعلي في حال وقوعها، ويلي ذلك مقارنة مستوى المخاطر المُقدَّر بمعايير مرجعية أو حدود مقبولة مسبقًا، مثل المستويات المعيارية المعتمدة في القطاع المصرفي، وذلك بهدف تحديد مدى مقبوليتها، وما إذا كانت تتطلب تدخلاً أو إجراءات لمعالجتها، وتُستخدم نتائج هذا التقييم لتحديد أولويات الاستجابة للمخاطر وفقًا لتأثيرها المحتمل على أهداف المنظمة واستقرارها واستمراريتها (Bao et al 2024)، ويتم القيام بتحليل وتقييم المخاطر من خلال تبني العديد من الآليات، منها (Gaviyau & Sibindi, 2023):

1. **نماذج تصنيف المخاطر Risk Scoring Models:**

حيث يتم تحديد وتعيين درجات رقمية للأنواع والأنماط المختلفة من مخاطر الجرائم المالية بناءً على الاحتمالية Likelihood والأثر المحتمل Possible Consequence.

2. **تحليل السيناريوهات Scenario Analysis:**

حيث يتم بناء سيناريوهات افتراضية للمخاطر والجرائم المالية المختلفة المحتملة لاختبار استجابة المؤسسة، وفهم كيف يمكن أن يؤثر كل سيناريو عليها.

3. **تقييم التهديدات ونقاط الضعف Threat and Vulnerability Assessment:**

ويقصد به التعرف المنهجي على أكثر مجالات المؤسسة وعملياتها عرضة لمخاطر الجرائم المالية المختلفة من خلال دراسة العوامل التي قد تؤدي إلى حدوث الجرائم المالية والأسباب الجذرية المسببة لها.

4. **الخرائط الحرارية Heat Maps:**

وهي أدوات بصرية تُستخدم لعرض مستويات المخاطر المختلفة عبر وحدات أو عمليات المؤسسة بطريقة مبسطة وواضحة، وتعتمد الخرائط الحرارية عادةً على نظام الألوان (مثل الأحمر والأصفر والأخضر) لتوضيح شدة المخاطر، وتساعد هذه الخرائط الحرارية فرق إدارة المخاطر على تحديد المجالات أو العمليات الأكثر عرضة للخطر بشكل سريع، مما يمكّنهم من ترتيب الأولويات واتخاذ الإجراءات التصحيحية اللازمة بشكل أكثر فاعلية.

5. **مؤشرات المخاطر الرئيسية Key Risk Indicators (KRIs):**

وهي مقاييس كمية أو نوعية تُستخدم لرصد التغيرات المحتملة في مستوى المخاطر داخل المؤسسة، وتساعد في الكشف المبكر عن المخاطر قبل أن تتحول إلى مشكلات حقيقية، مما يتيح اتخاذ إجراءات استباقية لتخفيف الأثر، وعادةً ما تكون هذه المؤشرات مرتبطة بالمجالات الحرجة، مثل: الامتثال Compliance، والعمليات، والجرائم المالية، وتُحدد بناءً على طبيعة نشاط المؤسسة ومستوى المخاطر التي تواجهها.

6. **عمليات تدقيق الامتثال والمراجعات الداخلية Compliance Audits and Internal Reviews:**

وهي تقييمات دورية تقوم بها فرق التدقيق الداخلي في المؤسسة لقياس فاعلية إجراءات وضوابط مكافحة الجرائم المالية في هذه المؤسسة.

7. **المقارنة المعيارية مع الأقران Peer Benchmarking:**

وفيها يتم مقارنة مدى تعرض المؤسسة للمخاطر وجهود التخفيف منها وفقا لمعايير الصناعة أو المؤسسات المماثلة.

8. **التقييم القائم على رأي الخبراء Expert Judgment:**

وهو أسلوب يعتمد على توظيف المعرفة المتخصصة وخبرة خبراء الامتثال والقانون وإدارة المخاطر، لتقييم المخاطر المعقدة أو غير التقليدية التي قد تعجز النماذج الكمية أو التحليلية وحدها عن رصدها بدقة، ويتم اللجوء إلى هذه الأسلوب عادةً عندما تكون البيانات غير مكتملة أو عندما تتطلب طبيعة الخطر منظورًا تحليليًا أعمق لا توفره الأدوات التقليدية.

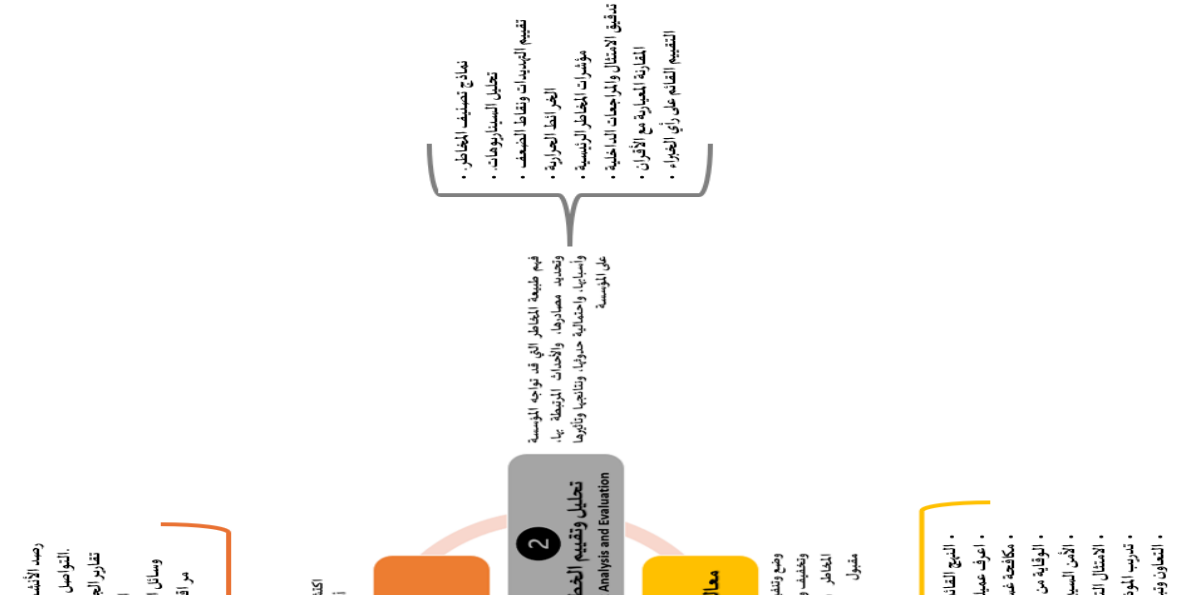
ج. **مرحلة معالجة وتخفيف الخطر Risk Mitigation:**

ويقصد بها ممارسة السيطرة على المخاطر، وهذه المرحلة هي التي يتم فيها وضع وتنفيذ إستراتيجيات وآليات الحد من وتخفيف ومعالجة المخاطر التي تم تحديدها وتحليلها وتقييمها، وذلك بهدف تقليل شدة المخاطر وتأثيراتها وعواقبها إلى مستوى مقبول (Khinvasara & Tzenios, 2023)، ويؤدي هذا الإجراء بدوره إلى تحديد المخاطر المتبقية Residual Risk، وهي ذلك الخطر الذي يبقى بعد تطبيق الضوابط الوقائية، ويتضمن تقييم المخاطر المتبقية Residual Risk تقييم فاعلية الضوابط الوقائية المطبقة وتحديد ما إذا كان الخطر المتبقي يقع ضمن نطاق تحمل المؤسسة المصرفية للمخاطر أم لا، وتعد هذه الخطوة حاسمة، حيث تتوقع الجهات التنظيمية من المؤسسات المصرفية أن تظهر فهمًا واضحًا لمخاطرها المتبقية وأن تتخذ الإجراءات المناسبة لمعالجتها (Baretzky & Partners, 2025)، وفيما يلي نستعرض بعضا من أهم الإستراتيجيات المستخدمة في معالجة وتخفيف المخاطر (Clintworth et al., 2023):

1. **النهج القائم على المخاطر Risk-based Approach (RBA):**

ويقصد به تصميم الضوابط بناءً على مستوى المخاطر المرتبطة بالعملاء، والمنتجات والخدمات، وقنوات تقديم الخدمة، والمناطق الجغرافية.

2. **تدابير اعرف عميلك (KYC) وإجراءات العناية الواجبة بالعملاء (CDD):** وتشمل كلا من:
   أ. التحقق من هوية العملاء باستخدام المستندات الرسمية والأدوات الرقمية المختلفة.
   ب. تطبيق العناية الواجبة المعززة (EDD) للعملاء ذوي المخاطر العالية، مثل الأشخاص ذوي المخاطر السياسية (PEPs).
   ج. المتابعة المستمرة وتحديث ملفات وسلوكيات العملاء.
3. **إجراءات مكافحة غسل الأموال (AML) وتمويل الإرهاب (CTF) :** وتشمل كلا من:
   أ. أنظمة مراقبة المعاملات تعتمد على التقنيات المتخصصة وتحليل السلوك.
   ب. الفحص على قوائم العقوبات الأممية والدولية والوطنية المختلفة.
   ج. تقديم تقارير المعاملات والأنشطة المشبوهة (SARs/STRs) إلى الجهات المختصة مثل وحدات المعلومات المالية.
4. **إجراءات وضوابط الوقاية من الاحتيال والكشف عنه Anti-fraud Controls :** وتشمل كلا من:
   أ. تحليلات سلوكية لاكتشاف الأنماط غير الاعتيادية في المعاملات.



شكل رقم (10): مراحل إدارة مخاطر الجرائم المالية في القطاع المصرفي وآلياتها المختلفة
المصدر: من إعداد الباحث بناء على مصادر الدراسة

5. **الأمن السيبراني وحماية البيانات Cyber Security:** وتشمل كلا من:
   أ. استخدام التشفير وتقنيات الترميز لحماية البيانات المالية الحساسة.
   ب. تأمين أجهزة المستخدمين الطرفية المشاركة في العمليات المصرفية.
   ج. تدريب الموظفين على تجنب الأساليب الاحتيالية السيبرانية المختلفة.

6. **الامتثال التنظيمي وحوكمة المخاطر Compliance Auditing and Risk Governance** وتشمل كلا من:
   أ. الالتزام بالقوانين الوطنية والتشريعات والمعايير الدولية المختلفة، مثل توصيات مجموعة العمل المالي FATF .
   ب. إجراء تدقيق ومراجعات داخلية وتقييمات مستقلة للتأكد من فاعلية الضوابط.
   ج. تقديم التقارير الإلزامية للجهات التنظيمية في الوقت المحدد.

7. **تدريب الموظفين والإبلاغ الداخلي Staff Training and Internal Reporting** وتشمل كلا من:
   أ. ورش عمل ودورات تدريبية منتظمة حول مكافحة الجرائم المالية في القطاع المصرفي بأنماطها المختلفة والتعرف على الأنماط المشبوهة.
   ب. إنشاء قنوات آمنة للإبلاغ الداخلي لتلقي البلاغات من قبل الموظفين عن السلوكيات المخالفة أو المشتبه بها.

8. **التعاون وتبادل المعلومات Information Exchange** وتشمل كلا من:
   أ. شراكات متنوعة بين القطاعين العام والخاص لتبادل المعلومات وفق القوانين والآليات المعتمدة.
   ب. الانخراط في المنتديات الدولية لتبادل أفضل الممارسات والخبرات.

د. مرحلة مراقبة ومراجعة الخطر Monitoring & Review Risk:

ويطلق عليها أحيانا **متابعة ومراجعة المخاطر** Risk Monitoring & Review، ويقصد بها: التتبع والتقييم المستمر للمخاطر التي تم التعرف عليها وتحديدها وتحليلها وتقييمها ومعالجتها، فضلاً عن ضمان فاعلية إجراءات وتدابير معالجة المخاطر من خلال التحديث

المستمر لها، لضمان أن تظل إستراتيجية إدارة المخاطر في المؤسسة ذات صلة وحديثة وتحديد مجالات التحسين (Efe, 2023)، وفي هذه المرحلة يتم استخدام العديد من الأساليب، منها على سبيل المثال (Clintworth et al., 2023):

1. **المراجعات الدورية:**

حيث يتم إجراء مراجعات دورية للسياسات والتدابير المخصصة لمعالجة المخاطر المتخذة لضمان فعاليتها، وكذا مراجعتها بشكل دوري بشأن المعاملات عالية المخاطر.

2. **تحديث المخاطر:**

وفيها يتم مراجعة وإعادة تقييم وتحديث المخاطر بشكل دوري وتحديد الأنشطة التي تنحرف عن التوقعات وتثير المخاوف عند الحاجة لضمان بقاء المؤسسة محصنة ضد التهديدات المتغيرة أو الناشئة.

3. **إعداد تقارير المخاطر:**

حيث يتم تقديم تقارير دورية للإدارة العليا حول حالة المخاطر وإجراءات معالجة وتخفيف المخاطر.

4.العوامل التي يجب مراعاتها في عملية تقييم المخاطر:

يُشكّل تقييم المخاطر ركيزة أساسية في إدارة مخاطر الجرائم المالية Financial Crime Risk Management بالقطاع المصرفي، حيث يهدف إلى تحليل شامل لمختلف العوامل المؤثرة لتمكين المؤسسات من تحديد التهديدات المحتملة وتقديرها بدقة، ويجب أن يتميز هذا التقييم بالشمولية لاستيعاب كافة المتغيرات التي تحدد مستوى تعرض المؤسسة المصرفية للمخاطر المالية، ويسهم الفهم العميق لهذه العوامل في تمكين المؤسسات المصرفية من صياغة إستراتيجيات فعّالة لإدارة المخاطر، وتعزيز آليات الوقاية والاحتواء، والحفاظ على الاستقرار المالي، وضمان سلامة النظم التشغيلية، وفي هذا الإطار نستعرض فيما يلي أهم العوامل الواجب مراعاتها عند إجراء تقييم مخاطر الجرائم المالية في القطاع المصرفي (Clintworth et al., 2023):

أ. **مخاطر العملاء Customer Risk:**

وتشير إلى التهديد المحتمل الذي يشكله العملاء، والناشئ عن ملفات تعريفهم وسلوكياتهم، وغالبًا ما يشمل: العملاء ذوو الخطورة العالية، والشخصيات السياسية البارزة (PEPs)، والأفراد غير المقيمين، أو أولئك الذين لديهم هياكل ملكية معقدة، وتُعدّ إجراءات العناية الواجبة المعززة أو المشددة EDD ضرورية لهذه الفئات للتخفيف من المخاطر المرتبطة بها (Korzeb et al., 2024)، وتشمل عملية تقييم هذه المخاطر الإجراءات التالية:

1. **دراسة تاريخ العميل:**

ويشمل ذلك دراسة تاريخ المعاملات المالية للعميل، بما في ذلك سجلات الائتمان، والمشكلات المالية السابقة، وحالات التهرب من الديون (Salamah,2023).

2. **دراسة طبيعة نشاط العميل:**

يجب النظر في نوعية الأعمال أو الأنشطة التي يقوم بها العميل، فالأنشطة العالية المخاطر في بعض القطاعات يمكن أن تزيد من المخاطر المرتبطة بالعميل (Qi et al., 2023).

3. **دراسة الملف المالي للعميل:**

يتم تحليل المعلومات المالية للعميل، مثل الدخل والأصول والالتزامات، لتقييم قدراته المالية المختلفة، مثل القدرة على السداد ومدى تمتعه بالاستقرار المالي (Qi et al., 2023).

4. **دراسة أنماط ومر اقبة سلوك العميل:**

يتم مراقبة سلوك العميل في استخدام المنتجات والخدمات التي تقدمها المؤسسة، خاصة إذا كانت هناك تغيرات سلوكية مفاجئة قد تشير إلى احتمال حدوث مخاطر (Clintworth et al., 2023).

ب. **المخاطر الجغر افية Geography Risks:**

ويطلق عليها أحيانا مخاطر دوائر الاختصاص أو الولايات القضائية، ويقصد بها تلك المخاطر التي تأخذ في الاعتبار تداعيات العمل في مناطق جغرافية ما، حيث قد تواجه المؤسسات المصرفية العاملة في مثل هذه المناطق مخاطر متزايدة تتعلق بالامتثال أو الاضطرابات التشغيلية، مما يزيد من احتمالات تعرضها لمخاطر الجرائم المالية؛ ولذا يجب أن تظل المؤسسات المصرفية يقظة فيما يتعلق بهذه المخاطر، كما قد يتعين عليها أحيانا أن تقيد التفاعلات مع الأفراد أو الكيانات من هذه المناطق للتخفيف من التهديدات المحتملة (Adel & Naili, 2024)، وتشمل عملية تقييم هذه المخاطر النظر في العديد من العوامل، من أهمها(Gaganis, et al. 2023):

1. **الموقع الجغرافي:**

قد تتأثر مخاطر الجرائم المالية بالموقع الجغرافي للعميل، ذلك إن بعض المناطق الجغرافية قد تكون أكثر عرضة للجرائم المالية من مناطق أخرى، فعلي سبيل المثال قد يكون وقوع العميل في دولة مجاورة لأخرى خاضعة للعقوبات الأممية أو الدولية، كالجزاءات المالية المستهدفة من عوامل رفع من مخاطر تمويل الإرهاب أو تمويل الانتشار أو مخاطر خرق قرارات العقوبات والجزاءات المالية المستهدفة.

2. **الأبعاد القانونية والتنظيمية:**

عند تقييم المخاطر الجغرافية يجب أن يؤخذ في الاعتبار القوانين المحلية واللوائح التي تنظم الأنشطة المصرفية، كقوانين السرية المصرفية مثلا، أو تلك التي تكافح الجرائم المالية، كقوانين مكافحة غسل الأموال، وقوانين مكافحة الفساد، حيث تختلف القوانين وشدتها ومدى فاعلية تطبيقها من دولة إلى أخرى.

3. **الاستقرار الاقتصادي:**

إن معاناة بعض المناطق الجغرافية من ارتفاع معدلات البطالة والتضخم أو عدم الاستقرار الاقتصادي، يمكن أن يزيد من مخاطر الجرائم المالية في تلك المناطق.

4. **الاستقرار السياسي:**

تعد المناخات السياسية غير المستقرة أو المعروفة بمستويات عالية من الفساد أو مناطق نشوب النزاعات من العوامل التي تزيد من مخاطر وقوع وارتكاب الجرائم المالية.

ج. مخاطر المنتجات Product Risk:

تتعلق مخاطر المنتجات بنقاط الضعف الكامنة المرتبطة بمنتجات أو خدمات مصرفية محددة، ذلك أن بعض هذه المنتجات تكون أكثر عرضة للإساءة في الجرائم المالية من البعض الآخر (Korzeb et al., 2024)، وتشمل العوامل المستخدمة في تقييم مخاطر المنتجات في القطاع المصرفي ما يلي (Gaganis et al. 2023):

1. **تعقيد المنتج:**

كلما زاد تعقيد المنتج وتعددت الأطراف المشاركة في معاملاته، ارتفعت مخاطر إساءة استخدامه في الجرائم المالية، كما هو الحال في خدمات التمويل التجاري Trade Finance والتي تنطوي على درجة عالية من التعقيد، مما يزيد من خطر استخدامها في جرائم مثل غسل الأموال أو تمويل الانتشار أو خرق قرارات الجزاءات المالية المستهدفة.

2. **سرعة إجراء المعاملات:**

كلما زاد معدل سرعة إجراء المعاملة المرتبطة بالمنتج بما يمكن العميل من القيام بالمعاملة أو عدد كبير من المعاملات بسرعة كبيرة، ارتفع مستوى المخاطر المرتبطة بهذا المنتج، وهذا ما نراه جليا في خدمات تحويل الأموال السريعة Speed Cash ومنها مثلا: ويسترن يونيون Western Union عالميا، وفورًا Fawran، وآني Aani و إنستاباي Insta Pay عربيا.

3. **حجم المعاملات:**

ترتفع مخاطر إساءة استغلال المنتجات والخدمات التي تتمتع بقيمة معاملات أو استثمارات عالية في ارتكاب الجرائم المالية، فعلى سبيل المثال ترتفع مخاطر إساءة استغلال الخدمات المصرفية الخاصة Private Banking لأغراض ارتكاب جريمة غسل الأموال نظرا لارتفاع مبالغ وحجم المعاملات في هذه الخدمات.

4. **قناة التوزيع أو التسليم:**

تختلف مستويات المخاطر اعتمادًا على ما إذا كانت المنتجات تُباع عبر المنصات الرقمية أو الفروع المادية أو وكلاء خارجيين، فبعض المنتجات أو الخدمات قد تكون أكثر عرضة لمخاطر لجرائم المالية، خاصة إذا كانت تتيح إخفاء الهوية أو تقدم مستويات ملحوظة من عدم التأكد من شخصية المستخدمين، مثل الخدمات المقدمة عبر شبكة الإنترنت التي تتم عبر التسجيل على موقع المؤسسة المصرفية بدون تحقق فعلي.

د. مخاطر البنية التقنية Technology Risks:

وتركز هذه المخاطر على البنية التحتية التقنية Technology Infra-structure للمؤسسات المصرفية، والوسائط التقنية التي يتم من خلالها تقديم الخدمات المصرفية والتي يمكن أن تشكل أيضًا نقاط ضعف، فقد أدى صعود وانتشار الخدمات المصرفية الرقمية Digital Banking إلى ظهور تهديدات أمن سيبراني جديدة، فعلى سبيل المثال قد يتم استهداف المنصات الرقمية للمؤسسات المصرفية من أجل ارتكاب جرائم الاحتيال الإلكتروني Cyber Fraud بما في ذلك هجمات التصيد الاحتيالي Phishing والبرمجيات الخبيثة Malware التي قد تعرض بيانات العملاء والأصول المالية للخطر، أو يمكن المجرمين من القيام بالمعاملات غير المصرح بها (Waliullah et al., 2025)، ومن أجل تقييم هذه المخاطر يجب النظر في العديد من العوامل من أهمها (Dawodu et al., 2023):

1. **قوة البنية التحتية التقنية:**

يجب مراعاة قوة نظم المعلومات والأمان الإلكتروني، حيث إن وجود بنية تحتية تكنولوجية قوية يمكن أن يقلل من التعرض للمخاطر الإلكترونية والجرائم المالية.

2. **كفاءة حماية البيانات:**

يجب حماية البيانات بواسطة أحدث البرمجيات، حيث إن مخاطر البيانات وعمليات الاختراق قد تؤثر على وضع المخاطر الكلية للمؤسسة، كما أن سوء إدارة البيانات قد يؤدي إلى فقدان الثقة والسمعة.

سابعا: إستراتيجيات إدارة المخاطر للجرائم المالية:

تلعب إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي دورًا حيويًا في حماية هذه المؤسسات والحفاظ على سلامتها المالية واستقرارها، وتتطلب إدارة مخاطر الجرائم المالية استخدام إستراتيجيات متنوعة، حيث يتطلب كل نوع من المخاطر نهجًا فريدًا لعلاجها، وتشمل هذه الإستراتيجيات: تخفيف المخاطر Risk Mitigation، وقبول المخاطر Risk Acceptance، ونقل المخاطر Risk Transfer، وتجنب المخاطر Risk Avoidance، وفيما يلي شرح واف لهذه الإستراتيجيات Dawodu et al., (2023):

أ. تخفيف المخاطر Risk Mitigation:

يقصد بتخفيف المخاطر Risk Mitigation تلك الإستراتيجية التي تهدف إلى الحد من تأثير أو تعرض المؤسسات المصرفية للجرائم المالية أو للتقليل من الآثار السلبية الناتجة عن هذه الجرائم، ويتضمن تخفيف المخاطر تنفيذ إجراءات استباقية تسعى إلى تقليل نقاط الضعف وتعزيز مرونة المؤسسة ضد عوامل المخاطر المختلفة (Gao & Liu, 2023)، وتشمل هذه الإجراءات الاستباقية القيام بما يلي:

1. **تطوير السياسات والإجراءات والضوابط الداخلية:**

ويتم ذلك من خلال إنشاء وتطبيق سياسات وإجراءات وضوابط داخلية لإدارة مخاطر الجرائم المالية، ومنها برامج مكافحة غسل الأموال وبرامج مكافحة الاحتيال (Scott et al., 2024).

2. **تدريب الموظفين:**

حيث يتعين على المؤسسات المصرفية توفير برامج تدريب وتوعية مناسبة ومستمرة للموظفين حول كيفية التعرف على الأنشطة المشبوهة والأساليب المستخدمة في ارتكاب الجرائم المالية (Fatmawati, & Bebasari, 2023).

3. **تطوير تقنيات مراقبة المعاملات**:

ويتم ذلك من خلال استخدام أنظمة تقنية المعلومات المتطورة الخاصة بمراقبة المعاملات وتحليل البيانات للكشف عن الأنماط غير المعتادة من معاملات وسلوكيات العملاء (Scott et al., 2024).

4. **تقييم الشراكات**:

حتى يتم تقييم علاقات العمل مع العملاء والشركاء الخارجيين والأطراف الثالثة عموما بشكل دوري، والتأكد من أنهم يتبعون معايير الامتثال والإفصاح والشفافية (Fatmawati, & Bebasari, 2023).

ب. **قبول المخاطر Risk Acceptance**:

يُشير قبول المخاطر إلى القرار الواعي للمؤسسة بالمضي قدما في القيام ببعض المعاملات رغم وجود مخاطر معروفة مرتبطة بها، وقبول هذه المخاطر دون اتخاذ إجراءات تخفيفية، وذلك عندما تتجاوز تكلفة معالجة هذه المخاطر الأثر المحتمل الناتج عنها، أو أن تكون المخاطر ضمن حدود تحمل المؤسسة للمخاطر، أو أنها تشمل مخاطر تشغيلية بسيطة أو تقلبات سوقية معتدلة، ويتطلب هذا النهج فهمًا دقيقًا لمستوى تحمل المؤسسة للمخاطر، مع ضرورة المراقبة المستمرة لهذه المخاطر (Raza, 2023)، ويعتمد قبول المخاطر على تقييم دقيق لاختيارات التوازن بين المخاطر والعوائد من خلال الخطوات التالية:

1. **تحليل التكلفة والعائد**:

حيث يتم إجراء تحليل لتحديد ما إذا كانت العوائد المحتملة تفوق المخاطر المحتملة، وإذا كانت التكاليف الناجمة عن الجرائم المالية المحتملة أقل من العوائد المحتملة من النشاط يمكن قبول المخاطر (Scott et al., 2024).

2. **تقييم الحدود المقبولة**:

حيث يجب على المؤسسة تحديد مستويات معينة من المخاطر التي تُعدّ مقبولة في إطار إستراتيجياتها التجارية، بناءً على أهدافها (Fatmawati, & Bebasari, 2023).

3. **مراقبة النتائج**:

ويعني ذلك متابعة نتائج الأنشطة المعنية دوريا لضمان عدم تحول المخاطر المحتملة إلى مشكلات كبيرة (Scott et al., 2024).

ج. **نقل المخاطر Risk Transfer**:

تتمثل هذه الإستراتيجية في تحويل الأثر المحتمل للمخاطر أو تحويل مسئولية اتخاذ تدابير إدارة هذه المخاطر من المؤسسة إلى طرف ثالث، ويستلزم تطبيق هذه الإستراتيجية تقييمًا دقيقًا لموثوقية الطرف الثالث وشروط اتفاقيات النقل (Gao & Liu, 2023)، وتختلف طرق وأساليب نقل المخاطر إلى طرف ثالث، حيث يمكن أن تشمل ما يلي (Bocola, & Lorenzoni, 2023):

1. **التأمين**:

ويتم ذلك من خلال استخدام منتجات التأمين لنقل المخاطر، مثل التأمين ضد الاحتيال وحماية الديون، مما يتيح للمؤسسة تقليل الأثر المالي للجرائم المالية عليها.

2. **عمليات الاسناد الخارجي**:

حيث يتم اسناد وتحويل بعض العمليات أو الأنشطة إلى جهات خارجية تتمتع بخبرة أكبر في الأمن والنظم المالية، مما يقلل من الأعباء والمخاطر على المؤسسة.

3. **الشراكات**:

إذ يسهم تكوين شراكات مع شركات متخصصة في تقديم حلول أمنية وقائية ويعزز من أمن المعلومات، مما يساعد في تعزيز جهود المؤسسة في إدارة المخاطر.

د. تجنب المخاطر Risk Avoidance:

تعني هذه الإستراتيجية الامتناع الكامل عن الأنشطة التي تنطوي على مخاطر غير مقبولة، مع اتخاذ تدابير لتجنب الدخول في مواقف قد تعرض المؤسسة لمخاطر الجرائم المالية، ورغم فاعلية هذه الإستراتيجية في الحد من الخسائر المحتملة، إلا أنها قد تقيد أحيانا فرص النمو والربحية، مما يستدعي الموازنة الدقيقة بين المخاطر والعوائد المتوقعة (Josyula, 2023)، ويتم تجنب المخاطر من خلال تبني عدة آليات منها (Kedarya et al. 2023):

1. **مراجعة المنتجات والخدمات:**

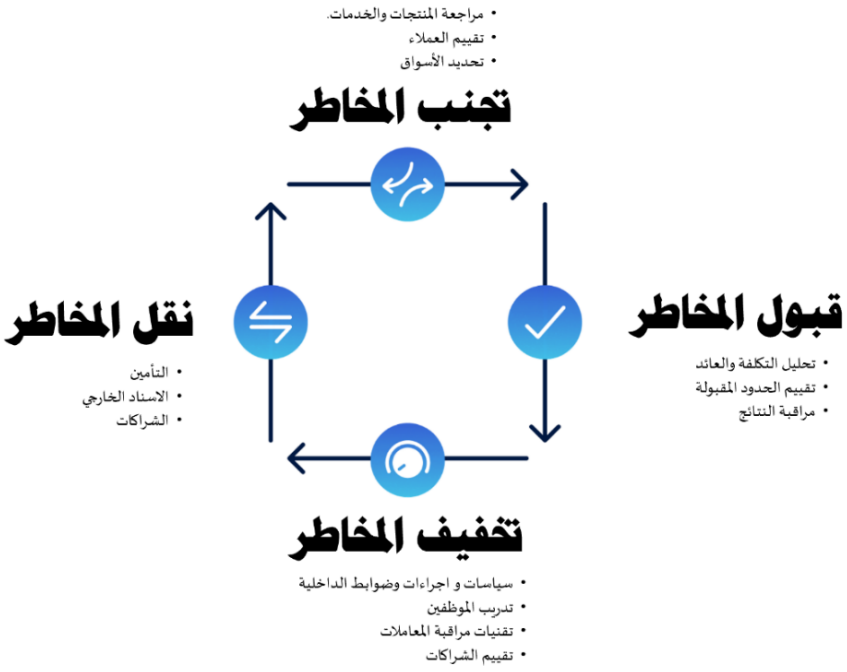
حيث يتم تحليل أنواع المنتجات والخدمات المقدمة لتحديد أي منها يمكن أن يحمل مخاطر عالية، ثم اتخاذ قرار بعدم تقديم أو إزالة تلك المنتجات، كتجنب التعامل بالأدوات المالية غير الشفافة.

2. **تقييم العملاء:**

يتم إجراء تقييم شامل لملفات العملاء قبل الموافقة عليهم، حيث يمكن أن يؤدي تجنب التعامل مع العملاء الذين لديهم سجلات غير سليمة إلى تقليل المخاطر، كمنع التعامل مع العملاء ذوي التاريخ الائتماني غير الجيد.

3. **تحديد الأسواق:**

يمكن أن يكون التحديد الدقيق لأسواق المنافسة وسيلة لتقليل التعرض للمخاطر، ففي هذه الحالة يتم عزل أسواق معينة وفقا لعدة عوامل، ككونها تعاني - مثلا - من عدم الاستقرار، أو من ارتفاع نسبة الشكوك القانونية أو التنظيمية المحيطة بها، ومنها عدم الدخول إلى أسواق تتميز بعدم الاستقرار السياسي، وهكذا.



شكل رقم (11): إستراتيجيات إدارة مخاطر الجرائم المالية في القطاع المصرفي وآلياتها المختلفة

المصدر: من إعداد الباحث بناء على مصادر الدراسة

ثامنًا: ضوابط إدارة المخاطر للجرائم المالية:

تتطلب إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي تطبيق إطار شامل ومتكامل من الضوابط الرقابية المصممة للحد من وتخفيف التهديدات المحتملة وتعزيز كفاءة آليات الرقابة الداخلية، وتشمل هذه الضوابط خمس فئات رئيسة

هي: الضوابط الوقائية Preventive Controls، والضوابط التوجيهية Directive Controls، والضوابط الكشفية Detective Controls، والضوابط التصحيحية Corrective Controls، والضوابط الإضافية أو التعزيزية Supporting or Reinforcing، وتُعد هذه الضوابط ضرورية لضمان الامتثال التنظيمي وتقليل التعرض للمخاطر التشغيلية والامتثال المرتبطة بالجرائم المالية (Velez, 2024)، وفيما يلي نستعرض بشيء من التفصيل أهم ضوابط إدارة مخاطر الجرائم المالية في القطاع المصرفي:

1. الضوابط الوقائية Preventive Controls:

تهدف الضوابط الوقائية Preventive Controls إلى منع حدوث الجرائم المالية وأي ممارسات غير قانونية قبل وقوعها، من خلال تبني مجموعة متنوعة من الضوابط (Gupta et al.,2023)، وتشمل هذه الضوابط تنفيذ السياسات والإجراءات الصارمة التي تمنع أو تحد من الأنشطة المشبوهة، ومنها على سبيل المثال (Southworth& Levi, 2024):

أ. **التحقق من هويات العملاء – اعرف عميلك (KYC):**

ويتم ذلك من خلال إجراء فحوصات شاملة للتحقق من هويات العملاء من خلال الوثائق الرسمية والمعلومات الشخصية، حيث يساعد ذلك في التأكد من أن العميل ليس له تاريخ من الأنشطة المشبوهة.

ب. **إجراءات تقييم المخاطر:**

ويتم ذلك من خلال تبني وسائل عملية لتقييم مخاطر العملاء والشركاء وباقي أطراف العلاقة المحتملين، بناءً على عوامل مثل: الموقع الجغرافي، ومجال العمل أو النشاط التجاري، ونوع الخدمات أو المنتجات المطلوبة، وقناة تقديم الخدمة.

ج. **تدريب الموظفين:**

ويتم ذلك من خلال توفير برامج تدريب دورية للموظفين حول كيفية التعرف على الأنشطة المشبوهة وكيفية التعامل معها.

د. **تطوير السياسات والإجراءات الداخلية:**

ومن الأمثلة على ذلك تطوير السياسات والإجراءات المتعلقة بالامتثال ومكافحة الجرائم المالية، مثل سياسات وإجراءات مكافحة غسل الأموال (AML) وتمويل الإرهاب (CFT) وإجراءات السلامة العامة.

2. الضوابط التوجيهية Directive Controls:

وتشمل الضوابط التوجيهية Directive Controls تطوير السياسات والإجراءات التي تحدد بوضوح الأدوار والمسؤوليات داخل المؤسسة، والتي تعمل على توجيه الموظفين نحو السلوكيات والممارسات الصحيحة والمتوافقة مع القوانين والقواعد المعتمدة المعمول بها لإدارة مخاطر الجرائم المالية، بما يضمن أن الموظفين على دراية بالتزاماتهم ومسئولياتهم فيما يتعلق بالامتثال ومكافحة الجرائم المالية (Gupta et al.,2023)، وتشمل الضوابط التوجيهية القيام بتنفيذ الإجراءات التالية Levytska et al.,2022):

أ. **تطوير السياسات والإجراءات المكتوبة:**

من خلال العمل على وجود منظومة شاملة من السياسات والإجراءات المعتمدة التي يجب اتباعها، مما يسهل العودة إليها عند الحاجة.

ب. **الفحص الدوري للسياسات والإجراءات:**

يجب أن يتم ضمان الفحص الدوري للسياسات والإجراءات والتأكد من تحديثها وفقًا للتغيرات في القوانين والقواعد والتوجيهات ذات الصلة.

ج. **توزيع المعلومات والتوجيهات الضرورية بشكل دوري:**

يجب العمل على توصيل المعلومات الضرورية للموظفين والتذكير بها بشكل دوري، وبالأخص التوجيهات المتعلقة بالتحديثات القانونية المحلية والدولية لإدارة مخاطر الجرائم المالية.

3. الضوابط الكشفية Detective Controls:

تعد الضوابط الكشفية Detective Controls من المكونات الأساسية لنظم إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي، حيث تهدف هذه الضوابط إلى اكتشاف وتحديد الأنشطة غير القانونية أو المشبوهة في الوقت المناسب، مما يسمح بالكشف المبكر عن الأنماط المشبوهة أو غير العادية أو الاحتيالية ويمنع وقوعها (Gupta et al.,2023)، وتشمل الضوابط الكشفية تبني وتنفيذ العديد من الإجراءات والأنظمة المتنوعة، ومنها ما يلي (Zarpala & Casino, 2021):

أ. **أنظمة مر اقبة المعاملات المالية:**

وتشمل هذه الأنظمة استخدام تقنيات تحليل البيانات لرصد وتحديد الأنماط غير العادية في حركة الأموال.

ب. **أساليب منع الجر ائم المالية والكشف عنها:**

حيث يتم تصميم وتنفيذ أدوات وبرامج متخصصة في كشف الجرائم المالية، وتصميم وتطبيق التحليلات الاستباقية للتحقق من صحة المعاملات.

ج. **التحليل الدوري للبيانات:**

حيث يتم إجراء تحليلات منتظمة وبصورة دورية على البيانات لرصد الأنماط التي قد تشير إلى وجود مخاطر أو ترجح احتمال حدوث جرائم مالية، فيتم رصدها والتعامل معها بصورة سريعة.

د. **رفع التقاريروالابلاغ عن الأنشطة المشبوهة:**

حيث يتم وضع إجراءات تسهل من تقديم تقارير عن الأنشطة التي تظهر عليها علامات أو مؤشرات الاشتباه، والتي تُعدّ علامتها تحذيرًا لخطر محتمل.

4. الضو ابط التصحيحية Corrective Controls:

تشكل الضوابط التصحيحية Corrective Controls أحد العناصر الحاسمة للنظام المتكامل لإدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي (Zarpala & Casino, 2021)، حيث تفعّل هذه الضوابط عند اكتشاف خلل أو حادث، وتشمل الضوابط التصحيحية اتخاذ إجراءات مثل التحقيقات الداخلية، وتقديم التقارير إلى السلطات التنظيمية، حيث تستهدف تعديل الإجراءات وتنفيذ إجراءات تصحيحية لمنع تكرار الحوادث (Velez, 2024)، وتشمل الضوابط التصحيحية تبني وتنفيذ العديد من الإجراءات والأنظمة المتنوعة، ومنها ما يلي (Cheng et al., 2021):

أ. **إجراءات التصحيح بعد الحوادث:**

حيث يتم وضع خطة شاملة للتعامل مع الحوادث، تتضمن اتخاذ إجراءات تصحيحية فورية لضمان عدم تكرار الحادث.

ب. **التحقيقات الداخلية:**

حيث يتم إجراء تحقيقات داخلية شاملة بعد وقوع حادث ما للكشف عن الأسباب الجذرية للحوادث وتقديم توصيات لتحسين إدارة المخاطر مستقبلا.

ج. **تعديل السياسات والإجراءات:**

بعد التحقيقات الداخلية والتوصل للأسباب التي أدت إليها، يتم تعديل السياسات والإجراءات المتبعة، وذلك استجابة لنتائج هذه التحقيقات والتوصيات التي تم التقدم بها؛ وذلك لضمان فاعلية الإجراءات والسياسات مستقبلا.

شكل رقم (12): ضوابط إدارة مخاطر الجرائم المالية في القطاع المصرفي موزعة على مراحل إدارة مخاطر الجرائم المالية
المصدر: من إعداد الباحث بناء على مصادر الدراسة

5. الضوابط الإضافية أو التعزيزية Supporting or Reinforcing Controls:

تُعدّ الضوابط الإضافية أو التعزيزية Supporting or Reinforcing Controls تدابير داعمة تعزز من فاعلية النظام العام لإدارة مخاطر الجرائم المالية، وتساعد في تقديم مستوى إضافي من الحماية (Tahiri & El Arif, 2024)، وتشمل الضوابط الإضافية أو التعزيزية تبني وتنفيذ العديد من الإجراءات المتنوعة، ومنها ما يلي (Cheng et al., 2021):

أ. **نظام التقارير الداخلية:**

حيث تقوم المؤسسات المصرفية بإنشاء نظام تقارير داخلية لتبادل المعلومات حول التعرض لمخاطر الجرائم المالية بانتظام.

ب. **الدعم الخارجي لجهود الامتثال:**

حيث تقوم المؤسسات المصرفية بالعمل مع الجهات التنظيمية والإشرافية ومستشارين خارجيين لضمان التزام المؤسسة بكافة القوانين والقواعد المحلية والدولية.

ج. **استخدام أدوات التكنولوجيا المتطورة:**

تقوم المؤسسات المصرفية بتبني واستخدام أدوات التقنية المالية والبرمجيات المتطورة لأغراض تحليل البيانات وكشف الاحتيال والجرائم المالية.

د. **دعم ضوابط التقييم الذاتي:**

حيث تقوم الفرق والوحدات والإدارات المختصة في المؤسسات المصرفية إجراء تقييمات دورية داخلية لضمان فاعلية الضوابط والقواعد المعمول بها.

تاسعًا: مقاييس فاعلية إدارة مخاطر الجرائم المالية في القطاع المصرفي:

كما أسلفنا، تُعدّ **إدارة مخاطر الجرائم المالية** في القطاع المصرفي عنصرًا حيويًا لضمان الامتثال التنظيمي والحفاظ على سلامة العمليات المالية، ومن هنا يمكن القول: إن تحديد مقاييس فاعلية نظام إدارة هذه المخاطر في المؤسسات المصرفية هو أيضا عملية حيوية تسهم في تعزيز الأداء المؤسسي لهذه المؤسسات وتوفير بيئة عمل آمنة ومستقرة لها، فمن خلال فهم هذه المقاييس وتطبيقها بشكل فعّال، يمكن للمؤسسات المصرفية أن تظل قادرة على مواجهة التحديات المعقدة والمتطورة للجرائم المالية، وتقديم خدماتها بكفاءة وفاعلية (Isomiddinovich., & Sunnatillo, 2024).

وتتوزع مقاييس فاعلية نظام إدارة مخاطر الجرائم المالية في المؤسسات المصرفية على عدة محاور، منها: القدرة على تحديد المخاطر المحتملة بدقة، وكذا القدرة على تقييم تأثير هذه المخاطر على الأداء المصرفي، وأيضا القدرة على تنفيذ إستراتيجيات فعالة للحد من هذه المخاطر والتخفيف منها، بالإضافة إلى ذلك يجب أن تشمل هذه المقاييس أيضا تحديد مدى التزام المؤسسات المصرفية بالمعايير والممارسات الدولية السارية والمعتمدة، مثل تلك التي وضعتها لجنة بازل للرقابة والإشراف المصرفي Basel Committee for Banking Supervision، وأيضا مدى التزام هذه المؤسسات بالتشريعات والقوانين والقواعد الوطنية ذات الصلة، مثل قوانين مكافحة غسل الأموال وتمويل الإرهاب، وغيرها (Harb, et al., 2023).

ومن خلال تحديد هذه المقاييس يمكن للمؤسسات المصرفية أن تحسن من قدرتها على التنبؤ بالمخاطر والتعامل معها بذكاء، كما يمكن أن تساعد هذه المقاييس في تعزيز الشفافية والثقة لدى المستثمرين والعملاء وجميع أطراف العلاقة، مما ينعكس إيجابًا على استقرار المؤسسة المصرفية ونموها (Harb, et al., 2023)، وفيما يلي نستعرض مجموعة من أهم مقاييس فاعلية نظام إدارة المخاطر المالية في مؤسسات القطاع المصرفي (Velez, 2024):

1. **عدد تقارير العمليات والأنشطة المشبوهة (SARs/STRs) وجودتها:**

يُعد تحليل عدد تقارير العمليات والأنشطة المشبوهة SARs/STRs وجودتها مؤشرًا على كفاءة أنظمة الكشف والرصد في المؤسسة، ومستوى جودة تدريب ووعي الموظفين وقدرتهم على تحديد المعاملات المشبوهة، وكذا مدى امتثالهم لمتطلبات الإبلاغ الداخلي Internal Reporting Requirements .

2. **معدل الكشف الإيجابي مقابل الإنذارات الكاذبة False Positives:**

ويُقاس هذا المعدل من خلال حساب نسبة التنبيهات الحقيقية True Positive Alerts إلى إجمالي التنبيهات الصادرة عن أنظمة المراقبة، مما يعكس فاعلية هذه الأنظمة في التمييز بين الأنشطة المشبوهة والحالات العادية.

3. **زمن الاستجابة للحالات المشبوهة Response Time:**

ويقصد به الوقت المستغرق منذ اكتشاف العملية المشبوهة وحتى التحقق منها وإعداد التقرير الخاص بها، ويدل تقليل هذا الزمن على كفاءة العمليات الداخلية وسرعة الاستجابة.

4. **نتائج التدقيق الداخلي والخارجي Internal & External Audits Findings:**

وتشمل العديد من الجوانب، من أهمها: مدى توافق عمليات إدارة مخاطر الجريمة المالية مع التشريعات والقوانين المحلية والمعايير الدولية المختلفة ذات الصلة، مثل توصيات مجموعة العمل الماليFATF، ومعايير لجنة بازل للإشراف والرقابة المصرفية Basel Committee وغيرها، وتُعد مؤشرًا على فاعلية الضوابط الداخلية.

5. **نسبة العملاء المكتملة ملفاتهم حسب معايير وتدابير اعرف عميلك(KYC) والعناية الواجبة بالعملاء (CDD):**

وتعكس هذه النسبة فاعلية عمليات التحقق من الهوية والعناية الواجبة، وتُعد ضرورية لتحديد العملاء ذوي المخاطر العالية.

6. **عدد الانتهاكات التنظيمية والغرامات المفروضة Enforcement Actions:**

وهي الغرامات التي يتم فرضها من قبل الهيئات التنظيمية والإشرافية في القطاع المصرفي على المؤسسة المصرفية، ويعكس انخفاض هذه الأرقام فاعلية الضوابط الداخلية في المؤسسة المصرفية ومدى امتثالها للوائح التنظيمية.

7. **مؤشرات المخاطر الرئيسية (KRIs):**

وتشمل مؤشرات مثل عدد المعاملات في دول عالية المخاطر، أو عدد العملاء المصنّفين كأشخاص ذوي المخاطر السياسية **(PEPs)**، وتُستخدم هذه المؤشرات لتقييم مستوى المخاطر الحالي.

8. **مستوى التزام الموظفين بالتدريب الدوري على مكافحة الجرائم المالية:**

تعكس نسبة حضور الدورات التدريبية ونتائج تقييم المعرفة والامتثال مدى وعي الموظفين والتزامهم بالسياسات والإجراءات.

9. **نتائج اختبارات السيناريوهات وتحليل الثغرات Gap Analysis:**

وتُستخدم لتقييم جاهزية الأنظمة لمواجهة محاولات القيام بالجرائم المالية المختلفة، وتحديد نقاط الضعف المحتملة في هذه الأنظمة.

10. **مؤشرات الالتزام الزمني بالتقارير الرقابية Regulatory Reporting Timeliness:**

مدى التزام المؤسسة المصرفية بتقديم التقارير الرقابية في المواعيد المحددة لذلك، مما يعكس كفاءة العمليات والامتثال التنظيمي.

ثالثا: دور الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي

مقدمة:

في العقد الأخير برز الذكاء الاصطناعي (AI) كقوة تحويلية كبيرة في القطاع المصرفي، مما أحدث ثورة غير مسبوقة في الكفاءة التشغيلية وخدمة العملاء وإدارة المخاطر، وكان لتقنيات الذكاء الاصطناعي، بما في ذلك تعلم الآلة Machine Learning، والتعلم العميق Deep Learning، ومعالجة اللغة الطبيعيةNLP، إسهاما كبيرًا في تمكين مؤسسات القطاع المصرفي من معالجة كميات هائلة من البيانات في الوقت الفعلي Real Time Data Processing، وأتمتة المهام الروتينية، وتعزيز عمليات اتخاذ القرار، مما أدى إلى تحسين الدقة في تقييمات الائتمان، وتحسين تجربة العملاء، وزيادة الكفاءة التشغيلية، وإدارة الاستثمار والامتثال للقواعد التنظيمية (Bi & Bao, 2024; Gafsi, 2025; Wang et al., 2024).

وفي مجال إدارة مخاطر الجرائم المالية في القطاع المصرفي، يلعب الذكاء الاصطناعي دورًا محوريًا في زيادة كفاءة وفاعلية هذه الجهود، من خلال تقديم أدوات متطورة للكشف عن الجرائم المالية والأنشطة غير المشروعة والحد منها، وغالبًا ما تواجه الأنظمة التقليدية القائمة على القواعد Rule-based صعوبة في مواكبة التكتيكات المتطورة للمجرمين الماليين، بينما على النقيض من ذلك يمكن للحلول المدعومة بالذكاء الاصطناعي AI-based Solutions التكيف مع التهديدات الجديدة من خلال التعلم من البيانات التاريخية Historical Data، وتحديد الشذوذ في المعاملات Anomaly Detection والذي بدوره قد يشير إلى سلوك احتيالي (Bi & Bao, 2024; Kovacevic et al., 2024)، وتعزز هذه الأنظمة فاعلية جهود مكافحة الجرائم المالية من خلال أتمتة مراقبة المعاملات ووضع علامة على الأنشطة المشبوهة لمزيد من التحقيق (Johannessen & Jullum, 2023, Ali et al., 2022)، وعلاوة على ذلك يسهل الذكاء الاصطناعي الامتثال للمتطلبات التنظيمية من خلال تبسيط إجراءات "اعرف عميلك (KYC)" وضمان الإبلاغ عن الجرائم المالية في الوقت المناسب (Cardoso et al., 2022; Yu et al., 2024).

وعلى الرغم من هذه الفوائد الكبيرة، فإن تبني تقنيات الذكاء الاصطناعي في مؤسسات القطاع المصرفي يطرح أيضًا تحديات كبيرة، لا سيما فيما يتعلق بخصوصية البيانات، والتحيز الخوارزمي، والحاجة إلى نماذج ذكاء اصطناعي قابلة للتفسير، ويعد ضمان الشفافية والمساءلة في القرارات المدعومة بالذكاء الاصطناعي أمرًا بالغ الأهمية للحفاظ على الثقة بين أصحاب المصلحة والامتثال للمعايير التنظيمية (Ghasemaghaei & Kordzadeh, 2024, Kovacevic et al, 2024)؛ لذلك يجب على مؤسسات القطاع المصرفي اعتماد أطر حوكمة قوية والاستثمار في تطوير ممارسات ذكاء اصطناعي أخلاقية لاستغلال إمكانات الذكاء الاصطناعي بالكامل مع التخفيف من المخاطر المرتبطة به (Castelnovo, 2024, Högberg, 2024).

وتهدف هذه الدراسة إلى استكشاف تأثير الذكاء الاصطناعي وتطبيقاته على إدارة مخاطر الجرائم المالية في القطاع المصرفي Financial Crime Risk Management، وتسعى الدراسة إلى القيام بذلك من خلال التعرف على وتحديد أنظمة وتطبيقات الذكاء الاصطناعي المتخصصة في اكتشاف والحد من الجرائم المالية المختلفة، وتقييم فاعلية هذه الأنظمة والتطبيقات في تحسين قدرات اكتشاف هذه الجرائم والحد منها، وتحليل الاعتبارات الأخلاقية والتنظيمية ذات الصلة باستخدام هذه الأنظمة والتطبيقات في إدارة مخاطر الجريمة المالية، وكذا التوصل إلى المعوقات والتحديات التي تواجه استخدام هذه الأنظمة والتطبيقات في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي، ومن ثم تخلص الدراسة إلى وضع توصيات وإرشادات لمؤسسات القطاع المصرفي لتفعيل تأثير وتعظيم العائد على استخدام أنظمة وتطبيقات الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي.

وعملا على تحقيق هذه الأهداف، سيقوم الباحث بدراسة أنظمة وتطبيقات الذكاء الاصطناعي المستخدمة في إدارة مخاطر الجرائم المالية بالتفصيل من خلال دراسة العناصر التالية:

أولاً: نظرة على استخدامات وتطبيقات الذكاء الاصطناعي في القطاع المصرفي بشكل عام.

ثانيًا: تطبيقات الذكاء الاصطناعي ودورها في إدارة مخاطر الجرائم المالية.
ثالثًا: فوائد الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي.
رابعًا: التحديات المرتبطة بتبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي.
خامسًا: الآليات المقترحة لمعالجة التحديات المرتبطة بتبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي.
سادسًا: الاتجاهات والتطورات المستقبلية لتوظيف الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي.
سابعًا: استعراض تطبيقات عملية للذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي.

أولاً: نظرة على استخدامات وتطبيقات الذكاء الاصطناعي في القطاع المصرفي بشكل عام:

يُشكّل الذكاء الاصطناعي AI حجر الأساس في تحوّل العديد من قطاعات الأعمال، لا سيما القطاع المصرفي، والذي يحصد فوائد جمة من تبني تطبيقاته، حيث يعمل الذكاء الاصطناعي AI على رفع كفاءة العمليات المصرفية، وإثراء تجارب العملاء، وتعزيز معايير الأمن والسلامة المالية، وفي ظل التسارع التكنولوجي المتواصل يتوقع الخبراء توسعًا كبيرًا في نطاق استخدامات الذكاء الاصطناعي AI في القطاع المصرفي، مما يفتح آفاقًا جديدة لمستقبل مصرفي أكثر كفاءة وذكاءً، وفي السطور التالية يستعرض الباحث بشكل عام بعض الاستخدامات والتطبيقات الرئيسية للذكاء الاصطناعي AI في القطاع المصرفي:

1. **تحليل البيانات الكبيرة Big Data Analysis**:

يمكن للذكاء الاصطناعي AI معالجة كميات ضخمة من البيانات المالية والتاريخية بشكل أسرع وأكثر دقة من البشر، مما يساعد في اتخاذ قرارات مبنية على معلومات دقيقة (Fares, et al., 2023).

2. **التنبؤ بالاتجاهات Trend Forecasting:**

باستخدام خوارزميات تعلم الآلة Machine Learning يمكن للمؤسسات المصرفية تحليل السوق والاتجاهات المستقبلية له، وتوقع نتائج الاستثمار، مما يساعدها على إدارة المحافظ الاستثمارية بكفاءة أعلى، واتخاذ قرارات استثمارية أفضل (Smit, et al., 2023).

3. **الدردشات الآلية Chatbots:**

تتيح تطبيقات روبوتات المحادثة المدعومة بالذكاء الاصطناعي (الدردشات الآلية) **Chatbots** للمؤسسات المصرفية توفير الدعم للعملاء على مدار الساعة، حيث يمكن للدردشات الآلية **Chatbots** الإجابة عن الأسئلة الشائعة وحل المشكلات الأساسية للعملاء لحظيا وفي أي وقت من أوقات اليوم (Fares, et al., 2023).

4. **تحليل مشاعر العملاء Customer Emotion Analytics:**

يمكن استخدام تقنيات الذكاء الاصطناعي AI لتحليل مشاعر العملاء من خلال تعليقاتهم على وسائل التواصل الاجتماعي المختلفة، وهو ما يساعد المؤسسات المصرفية على تحسين خدماتها وأداء موظفيها (Fares, et al., 2023).

5. **التسويق المستهدف Targeted Marketing**:

يمكن للمؤسسات المصرفية استخدام تطبيقات الذكاء الاصطناعي AI لتحليل تفضيلات العملاء وسلوكياتهم المتنوعة، وذلك سعيا لتقديم منتجات مالية مخصصة تلبي احتياجات كل عميل من المنتجات والخدمات بشكل دقيق ومفصل حسب رغبته (Paramesha, et al., 2024).

6. **التوصيات المالية Financial Recommendations**:

يمكن للمؤسسات المصرفية استخدام التطبيقات القائمة على الذكاء الاصطناعي AI-based Applications لتقديم مشورة مالية مخصصة، مثل استثمار الأموال أو إعادة توزيعها بناءً على الأهداف المالية المختلفة والمحددة لكل عميل من العملاء (Fares, et al., 2023).

7. **أتمتة العمليات الروبوتية RPA:**

يمكن استخدام الذكاء الاصطناعي AI لأتمتة المهام المتكررة، مما يمكن المؤسسات المصرفية من تقليل التكاليف وزيادة كفاءة عملياتها وأنشطتها (Smit, et al., 2023).

8. **تحسين التدفقات النقدية Cash Flow Optimization:**

تساعد أنظمة الذكاء الاصطناعي AI المؤسسات المصرفية في تحليل تدفقات النقد Cash Flow لديها وتحسين إدارة هذه التدفقات (Smit, et al., 2023).

ثانيًا: تطبيقات الذكاء الاصطناعي ودورها في إدارة مخاطر الجرائم المالية:

في العقد الأخير أصبح الذكاء الاصطناعي AI أداة لا غنى عنها في إدارة مخاطر الجرائم المالية في القطاع المصرفي، حيث تعاني النظم التقليدية القائمة على القواعد Rule-based Systems من صعوبة في مواكبة الأساليب المتطورة للمجرمين الماليين واللحاق بها، في حين تتميز الحلول القائمة على الذكاء الاصطناعي AI-based Solutions بقدرتها على التكيف مع التهديدات الجديدة؛ إذ يمكن لهذه الأنظمة تحليل مجموعات البيانات المعقدة للكشف عن الأنماط الدالة على أنشطة غير مشروعة وتمكين اعتماد إستراتيجيات استباقية للتخفيف من المخاطر (Johora et al., 2024)، كما أسهم دمج تقنيات الذكاء الاصطناعي مثل تعلّم الآلة (ML) والتعلّم العميق (DL) ومعالجة اللغة الطبيعية (NLP) في تعزيز قدرة المؤسسات المالية بشكل كبير على تحديد وكشف ومنع الأنشطة غير المشروعة، حيث تقوم هذه الأنظمة بمعالجة وتحليل كميات هائلة من المعاملات المالية بشكل فوري لتحديد الأنماط المشبوهة قبل تصاعدها إلى خروقات أمنية كبرى (Abbasov, 2024)، وفيما يلي نستعرض تطبيقات الذكاء الاصطناعي المختلفة ودورها في إدارة مخاطر الجرائم المالية في القطاع المصرفي وفق كل مرحلة من مراحل هذه العملية.

1. **تطبيقات الذكاء الاصطناعي ودورها في مرحلة تحديد المخاطر Risk Identification:**

عزز الذكاء الاصطناعي (AI) بشكل ملحوظ قدرات المؤسسات المصرفية على تحديد مخاطر الجرائم المالية من خلال تحسين دقة الكشف وكفاءته، وتُبرز الدراسات الحديثة قدرة الذكاء الاصطناعي على تحليل مجموعات البيانات الضخمة، والتعرف على الأنماط المشبوهة، وتقليل الاعتماد على الأنظمة التقليدية القائمة على القواعد، والتي غالبًا ما تُولّد معدلات عالية من النتائج الإيجابية الكاذبة False Positives، وهو ما يعزز من قدرة المؤسسات المصرفية على توقع المخاطر والتهديدات المحتملة (Abbasov, 2024)، وفيما يلي سنستعرض بالتفصيل دور تطبيقات الذكاء الاصطناعي في مرحلة تحديد المخاطر:

أ. **التنبؤ بالمخاطر والتهديدات المحتملة Anticipate Potential Risks and Threats**

يعتمد الذكاء الاصطناعي (AI) على تحليل البيانات الضخمة Big Data Analysis والنماذج التنبؤية Predictive Models للتعرف على المخاطر المحتملة قبل وقوعها، فمن خلال تقنيات تعلم الآلة Machine Learning، يمكن التعرف على أنماط سلوكية غير معتادة تشير إلى احتمالية حدوث خطر مستقبلي، مما يُعزز قدرة المؤسسات المصرفية على التصرف الاستباقي (Wang, 2024)، ويتم ذلك من خلال العديد من الأساليب منها:

1. **تحليل البيانات الضخمة Big Data Analysis** :

يستطيع الذكاء الاصطناعي تحليل بيانات المعاملات المصرفية والعملاء للتعرف على التوجهات غير الاعتيادية التي قد تنطوي على مخاطر مالية (Wang, 2024).

2. **النمذجة التنبؤية للمخاطر Predictive Risk Modeling:**

تستخدم المؤسسات المصرفية نماذج إحصائية وذكاء اصطناعي متقدمة للتنبؤ بمخاطر، مثل العجز عن السداد، مما يدعم اتخاذ قرارات ائتمانية مستنيرة (Paramesha et al., 2024).

ب. كشف الاحتيال المالي Financial Fraud Detection:

تُستخدم تقنيات الذكاء الاصطناعي (AI) مثل الشبكات العصبية الاصطناعية ANN وخوارزميات اكتشاف الشذوذ في مراقبة الأنشطة والمعاملات المصرفية لحظيا (في الوقت الحقيقي للمعاملات) Real Time Monitoring، مما يسهم في تقليل عمليات الاحتيال المالي (Ukride et al., 2024)، ويتم ذلك من خلال عدة أساليب منها:

1. **اكتشاف الأنماط غير الطبيعية Anomaly Detection :**

تستطيع خوارزميات تعلم الآلة Machine Learning التمييز بين السلوكيات المعتادة وغير المعتادة للعملاء، ورصد المعاملات المشتبه بها، كالمعاملات الكبيرة غير المعتادة أو الأنماط الغريبة في سلوك العملاء، مما يعزز إدارة مخاطر الاحتيال والحد منه وكشفه.

2. **التعلم المستمر Ongoing Learning:**

تقوم الأنظمة الذكية بالتعلم المستمر وتحديث قواعدها بشكل دائم استنادًا إلى البيانات الجديدة المستمدة من كل عملية أو معاملة جديدة، ما يعزز دقة الكشف مع مرور الوقت.

ج. مكافحة غسل الأموال Anti-Money Laundering:

تلعب تطبيقات الذكاء الاصطناعي دورًا فعّالاً في مجال مكافحة غسل الأموال Anti-Money Laundering من خلال القدرة على معالجة وتحليل بيانات من مصادر متنوعة وتحديد المعاملات المشبوهة Suspicious Transactions وذلك من خلال القيام بما يلي (Majumder, 2024):

1. **تحليل البيانات المتعدد المصدر:**

يقوم الذكاء الاصطناعي (AI) بجمع البيانات من نظم متعددة للكشف عن ارتباطات قد تشير إلى أنشطة مشبوهة متعلقة بجريمة غسل الأموال.

2. **أنظمة الإنذار المبكر:**

يقوم الذكاء الاصطناعي (AI) بإصدار تحذيرات استباقية عند التعرف على سلوكيات مالية عالية المخاطر أو غير نمطية من المحتمل أن تكون مرتبطة بغسل الأموال، مما يساعد المؤسسات على اتخاذ إجراءات فورية لمواجهة غسيل الأموال.

د. كشف الهجمات السيبرانية Detecting Cyber Attacks:

يستخدم الذكاء الاصطناعي (AI) لرصد التهديدات السيبرانية Cyber Threats التي تستهدف البنية التحتية للمؤسسات المصرفية قبل أن تتسبب في أضرار لها أو لأطراف العلاقة معها، بما في ذلك هجمات البرمجيات الخبيثة Malware، والتصيّد الاحتيالي Phishing، وغيرها من أشكال الهجمات السيبرانية، ويتم القيام بذلك من خلال استخدام أدوات تحليل متقدمة تعمل على اكتشاف وتحليل الأنماط غير المألوفة في الشبكات؛ مما يمكّن هذه المؤسسات من تحديد الهجمات المحتملة في مراحلها المبكرة وتعزيز أمن المعلومات بشكل استباقي، وهو ما يسهم في حماية الأنظمة والبنية التحتية الرقمية وتقليل المخاطر المرتبطة بالجرائم السيبرانية Cyber Crimes (Wang, 2024).

هـ. الامتثال لمتطلبات اعرف عميلك (KYC):

يسهم الذكاء الاصطناعي (AI) في تسريع إجراءات التحقق من الهوية ID Verification وتحليل الوثائق المقدمة من العملاء، مما يعزز من الامتثال التنظيمي ويحد من مخاطر الجرائم المالية المرتبطة بانتحال الهوية (Majumder, 2024)، ويتم ذلك من خلال:

1. **تحليل البيانات الشخصية للعملاء:**

يمكن للأنظمة الذكية معالجة بيانات الهوية والتحقق من صحتها بشكل تلقائي، وهو ما يساعد على اكتشاف وتحديد العديد من الجرائم المالية قبل وقوعها، مثل الاحتيال القائم على انتحال الشخصية وسرقة الهوية، ويتم القيام بهذه الإجراءات في أثناء قبول وتسجيل عملاء جدد عبر القنوات الرقمية.

2. **التحقق من الوثائق والمستندات:**

باستخدام تقنيات التعرف على الصوت والصورة Voice & Image Recognition، يمكن لتطبيقات الذكاء الاصطناعي (AI) تقييم صحة المستندات والبيانات البيومترية الخاصة بالعملاء.

و. المراقبة اللحظية للمعاملات Realtime Transaction Monitoring :

يلعب الذكاء الاصطناعي دورًا حيويًا في مراقبة المعاملات المالية لحظيًا **Realtime Transaction Monitoring**، حيث تُستخدم أنظمته المتقدمة لتحليل المعاملات لحظيا فور حدوثها بهدف الكشف عن أي سلوك مشبوه أو غير طبيعي، وذلك من خلال خوارزميات معقدة مثل تقنيات تحليل اللغة الطبيعية **NLP**، وتمكن هذه الأنظمة المؤسسات المصرفية من رصد المعاملات غير المعتادة أو الأنماط غير المألوفة والكشف الفوري عن الأنشطة المالية المشبوهة، مما يعزز من فاعلية كشف الجرائم المالية والحد منها (Ukride et al, 2024).

2. تطبيقات الذكاء الاصطناعي ودورها في مرحلة تحليل وتقييم المخاطر Risk Analysis and Evaluation :

تُعد مرحلة تحليل وتقييم المخاطر Risk Analysis and Evaluation من المراحل الجوهرية في إدارة المخاطر المؤسسية، ومن الركائز الأساسية في إدارة مخاطر الجريمة المالية في القطاع المصرفي؛ إذ تهدف إلى تقدير درجة خطورة كل خطر محتمل، وتحديد مدى تأثيره واحتمالية وقوعه، وتحديد أولويات الاستجابة له بما يدعم تحقيق أهداف المؤسسة، وقد أسهم الذكاء الاصطناعي (AI) في إحداث نقلة نوعية في هذه المرحلة من خلال تعزيز القدرة على معالجة البيانات وتحليل الأنماط، وتطوير نماذج تنبؤية دقيقة، وأدوات تحليلية متقدمة تسهم في تحسين جودة القرار وتقليل الفجوات الناتجة عن التقدير البشري للمخاطر (El Hajj & Hammoud, 2023)، وفيما يلي نستعرض أبرز التطبيقات التفصيلية للذكاء الاصطناعي في هذه المرحلة (Ahmed et al., 2023):

أ. التحليل الكمي للمخاطر باستخدام الذكاء الاصطناعي:

تعتمد الأنظمة المدعومة بالذكاء الاصطناعي على تحليل كميات ضخمة من البيانات التاريخية واللحظية لتقدير مستوى الخطورة المرتبطة بكل خطر، حيث تُستخدم تقنيات مثل الشبكات العصبية الاصطناعية ANN والنماذج التنبؤية Predictive Models للتعرف على العلاقات غير المباشرة بين المتغيرات التي قد تؤدي إلى تفاقم المخاطر(Palakurti, 2025) .

1. **نمذجة المخاطر المعقدة Complex Risk Modeling** :

تتيح تقنيات الذكاء الاصطناعي بناء نماذج تأخذ في الاعتبار مئات العوامل والمتغيرات للتنبؤ بالمخاطر بطريقة أكثر دقة مقارنة بالطرق التقليدية.

2. **تحليل السيناريوهات Scenario Analysis** :

تستخدم أنظمة الذكاء الاصطناعي لمحاكاة سيناريوهات مختلفة لتطور المخاطر وقياس أثرها المالي والزمني؛ مما يساعد متخذي القرار في وضع إستراتيجيات مناسبة للتعامل مع كل سيناريو.

ب. التنبؤ بحدوث المخاطر وتقدير تكرارها:

يساعد الذكاء الاصطناعي في التنبؤ بحدوث أنواع محددة من المخاطر بناءً على الأنماط التاريخية، مما يدعم تحديد أولويات المعالجة، كما تُستخدم خوارزميات التصنيف مثل خوارزمية الغابة العشوائية Random Forests وخوارزمية الانحدار اللوجستي Logistic Regression لتقدير احتمالية وتكرار المخاطر وتصنيفها بدقة (Srivastava et al., 2024).

ج. تقييم الأثروتحديد الأولويات:

يسهم الذكاء الاصطناعي في تقييم الأثر المالي والتشغيلي للمخاطر من خلال دمج التحليل الكمي مع أدوات تصور البيانات التفاعلية، وينتج عن ذلك رؤى أكثر عمقًا تساعد على ترتيب المخاطر حسب الأولوية، واتخاذ قرارات أكثر استنارة، كما تشير الدراسات إلى أن استخدام تطبيقات الذكاء الاصطناعي يقلل من التحيزات البشرية، ويزيد من دقة تقييم المخاطر وتحديد أولوياتها (Kuo & Hsu, 2024).

د. اكتشاف الأنماط والتناقضات:

تُستخدم تقنيات تعلم الآلة Machine Learning والتعلم العميق Deep Learning للكشف عن الأنماط المتكررة والسلوكيات غير الاعتيادية التي قد تمثل إشارات مبكرة لمخاطر محتملة (Wang, 2024)، ويتم ذلك من خلال:

1. **تحديد وتحليل الأنماط Pattern Recognition and Analysis** :

يمكن أن تكشف خوارزميات الذكاء الاصطناعي (AI) عن أنماط متكررة تشير إلى وجود مخاطر معينة في المعاملات المصرفية، على سبيل المثال في مجال التمويل يمكن للنماذج أن تجد أنماطًا مرتبطة بعمليات الاحتيال، ومن ثم تقوم بتحليلها بشكل متعمق (Ahmed et al., 2023).

2. **اكتشاف التناقضات Anomaly Detection:**

يمكن للذكاء الاصطناعي (AI) من خلال تحليل البيانات بشكل متعمق، الكشف عن التناقضات والفجوات في البيانات التي قد تشير إلى مخاطر محتملة، فعلى سبيل المثال يمكن أن تكشف الأنظمة عن بيانات غير متطابقة أو معلومات مفقودة تؤثر على دقة التقييمات (Wang, 2024).

هـ. تحسين وتعزيز نماذج تقييم المخاطر:

يمكن للذكاء الاصطناعي (AI) تحسين نماذج تقييم المخاطر المصرفية من خلال ما يلي (El Hajj & Hammoud, 2023):

1. **المعالجة الفورية للبيانات:**

يمكن للذكاء الاصطناعي (AI) تحليل وتفسير كميات هائلة من البيانات الضخمة Big Data لحظيا (في الوقت الفعلي) Real Time، مما يسهم في اتخاذ قرارات تقييم المخاطر بشكل أسرع وأكثر دقة.

2. **تعديل النماذج:**

يمكن للأنظمة الذكية من خلال التعلم من النتائج السابقة، تعديل خوارزميات تقييم المخاطر لتحسين دقتها، وباستمرار التدريب على البيانات الجديدة، يمكن أن تصبح النماذج أكثر كفاءة وملاءمة.

3. **الاستخدام الذكي للبيانات:**

يمكن للذكاء الاصطناعي (AI)دمج مصادر بيانات متعددة (مثل المعلومات الاقتصادية، والاجتماعية، والفنية وغيرها) للحصول على صورة أوضح للمخاطر التي يمكن مواجهتها.

و. دعم اتخاذ القراروتقديم التوصيات:

يلعب الذكاء الاصطناعي دورًا محوريًا في دعم اتخاذ القرارات وتقديم التوصيات بشأن المخاطر من خلال (Wang, 2024):

1. **التوقع والتحليل:**

استخدام تقنيات مثل النمذجة الإحصائية والتنبؤات لإنشاء سيناريوهات للمخاطر المحتملة والمتوقعة، كما يمكن للذكاء الاصطناعي تقدير الأثر المحتمل للمخاطر المختلفة على الأعمال التجارية ومعاملات المؤسسات المصرفية.

2. **الاستجابة السريعة وتقديم التوصيات:**

عند حدوث أي تهديد، ومن خلال تحليل البيانات والتعلم من التجارب السابقة، يمكن لأنظمة الذكاء الاصطناعي تقديم توصيات موجهة بشأن التدابير المقترحة، ويمكن أن يتضمن ذلك إطلاق تنبيهات مبكرة للفرق المعنية بشأن المخاطر المتوقعة.

3. تطبيقات الذكاء الاصطناعي ودورها في مرحلة تخفيف ومعالجة المخاطر Risk Mitigation:

تُعد مرحلة التخفيف والمعالجة Risk Mitigation من أهم مراحل إدارة المخاطر، حيث تهدف إلى تقليل الأثر السلبي للمخاطر المحتملة على المؤسسات، وفي هذا السياق تلعب تطبيقات الذكاء الاصطناعي دورًا محوريًا في تعزيز قدرات المؤسسات على معالجة المخاطر والتخفيف منها والتعامل معها بفاعلية، وذلك من خلال:

أ. **التنبؤ بالسيناريوهات البديلة:**

تُستخدم نماذج الذكاء الاصطناعي لمحاكاة سيناريوهات متعددة لتطور المخاطر، مما يتيح للمؤسسة الاستعداد المسبق ووضع خطط بديلة لتخفيف الأثر المحتمل (Kuo & Hsu, 2024).

ب. **أتمتة العمليات والاستجابة التلقائية للحوادث:**

تعتمد هذه الأنظمة على آليات الذكاء الاصطناعي لرصد مؤشرات التهديد وتفعيل إجراءات تلقائية لمعالجتها من خلال أتمتة بعض العمليات، مما يقلل من زمن الاستجابة ويحد من انتشار آثار الخطر ويقلل من الأخطاء البشرية، وهو ما يسمح باتخاذ قرارات أسرع وأكثر فاعلية (Palakurti, 2025).

ج. **تحليل الأسباب الجذرية للمخاطر:**

تُمكِّن تقنيات التحليل العميق الذكاء الاصطناعي من الكشف عن الأسباب الفعلية لوقوع المخاطر، وهو ما يسهم في معالجة مصدر المشكلة بدلاً من الاكتفاء بعلاج الأعراض (Zhao, Chen, & Li, 2024).

د. **تحسين تخصيص الموارد الوقائية:**

تسهم التحليلات الذكية في توجيه الموارد البشرية والتقنية إلى المناطق ذات الأولوية، بناءً على تقييم واقعي لاحتمالية التأثر وشدة الخطر (Kuo & Hsu, 2024).

هـ. **الرصد المستمر للتهديدات الديناميكية:**

تتيح آليات تعلم الآلة تحديث نماذج التهديد باستمرار بما يتوافق مع البيانات المستجدة، ما يعزز مرونة المؤسسة وقدرتها على التكيف مع المتغيرات (Srivastava et al., 2024).

و. **دعم اتخاذ القرار في بيئات عالية التغيير:**

توفر نظم الذكاء الاصطناعي أدوات تحليل فوري للبيانات المعقدة، مدعومة بتوصيات مدروسة، وهو ما يعين صناع القرار على التحرك بثقة وفاعلية في ظل الظروف الطارئة (Palakurti, 2025).

4. تطبيقات الذكاء الاصطناعي ودورها في مرحلة مر اقبة ومراجعة المخاطر Monitoring & Review Risk:

تُعد مرحلة مراقبة ومراجعة المخاطر Monitoring & Review Risk من الخطوات الحاسمة في دورة إدارة مخاطر الجرائم المالية، حيث تضمن هذه المرحلة التحقق المستمر من كفاءة الإجراءات المُتخذة وتحديث التقييمات بناءً على تغيّر المعطيات والبيئة التشغيلية، وفي هذا السياق توفّر تطبيقات الذكاء الاصطناعي (AI) أدوات فعّالة تمكّن المؤسسات من مراقبة المخاطر بشكل لحظي، وتحليل اتجاهاتها، واكتشاف التغيرات غير المتوقعة بسرعة وكفاءة كما يلي (Giudici et al., 2024):

أ. **الرصد اللحظي للمخاطر Real-Time Risk Monitoring:**

تُتيح تقنيات الذكاء الاصطناعي AI مراقبة العمليات المالية والتشغيلية لحظيا Real Time من خلال استخدام خوارزميات تعلم الآلة ML ومعالجة البيانات المستمرة، مما يُسهم في الكشف المبكر عن الانحرافات والمؤشرات الدالة على مخاطر جديدة (Bezshtank, 2025)، ويتم ذلك من خلال:

1. **أنظمة التنبيه المبكر Early Warning Systems :**

تعتمد هذه الأنظمة على الذكاء الاصطناعي لرصد إشارات التحذير المبكر التي قد تشير إلى تفاقم مخاطر معينة.

2. **التعلم التكيفي Adaptive Learning:**

تسمح هذه الميزة للأنظمة بتحديث نماذجها بشكل مستمر بناءً على المدخلات الجديدة، مما يرفع من دقة الرصد والاستجابة.

ب. **تحليل الاتجاهات ومراجعة المخاطر Trend Analysis and Risk Review:**

تستخدم تطبيقات الذكاء الاصطناعي لتحليل البيانات الزمنية Time Series Analysis والتغيرات في مؤشرات الأداء والمخاطر، بهدف التحقق من فاعلية الضوابط الحالية وتحديد الحاجة لإعادة تقييم أو تعديل الخطط الإستراتيجية (Srivastava et al., 2024).

1. **تحليل الاتجاهات Trend Analysis**:

تمكن خوارزميات الذكاء الاصطناعي من تتبع تطور المخاطر بمرور الوقت، واكتشاف الأنماط الدورية أو الموسمية التي قد تؤثر على مستوى الخطر.

2. **مراجعة مستمرة للنماذج Model Reevaluation**:

تساعد خوارزميات التعلم العميق Deep Learning على مراجعة نماذج التقييم بشكل دوري لتحسين أدائها بناءً على الأداء الفعلي.

ج. **دعم اتخاذ القرارات التصحيحية:**

توفر تطبيقات الذكاء الاصطناعي لوحات معلومات تحليلية تعرض البيانات بشكل مرئي وتفاعلي، ما يُمكّن مديري المخاطر من اتخاذ قرارات مبنية على بيانات حديثة ودقيقة من خلال القيام بما يلي (Palakurti, 2025):

1. **التوصيات الذكية Prescriptive Analytics**:

تولّد أنظمة الذكاء الاصطناعي اقتراحات تلقائية حول الإجراءات التصحيحية بناءً على التحليلات المستمرة التي تقوم بها.

2. **أتمتة التقارير Automated Reporting :**

تستخدم تقنيات الذكاء الاصطناعي في إعداد تقارير المخاطر بشكل دوري دون تدخل بشري، مما يُقلل الأخطاء ويوفر الوقت.

ثالثا: فوائد الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي:

أصبح الذكاء الاصطناعي(AI) أداة إستراتيجية متقدمة في مكافحة الجرائم المالية داخل القطاع المصرفي، حيث يُسهم في تعزيز الكفاءة التشغيلية، وتحسين دقة الكشف عن الأنشطة غير المشروعة، والامتثال للتنظيمات القانونية، مع تقليل التكاليف التشغيلية، ويمكن تحديد أهم فوائد الذكاء الاصطناعي وتطبيقاته في هذا المجال في النقاط التالية:

1. **تحسين الدقة والسرعة:**

تُتيح تقنيات الذكاء الاصطناعي (AI)، خاصة خوارزميات تعلم الآلة Machine Learning، تحليل كميات ضخمة من البيانات بسرعة ودقة، مما يُمكّن من اكتشاف الأنماط غير المعتادة في المعاملات المالية، ومن ثمَّ الكشف المبكر عن الأنشطة الاحتيالية أو الجرائم المالية المحتملة، وقد أظهرت الدراسات المتعددة أن هذه التقنيات تتفوق على الأنظمة التقليدية في تحديد العمليات المشبوهة بدقة أعلى (Gupta et al., 2023).

2. **تعزيز إدارة المخاطر:**

من خلال تحليل سلوك العملاء، والأنماط التاريخية للمعاملات، يُمكن للذكاء الاصطناعي (AI) تصنيف مخاطر الجرائم المالية بشكل أكثر دقة، وتُساعد هذه الميزة المؤسسات المصرفية على تطوير إستراتيجيات فعّالة لإدارة وتقييم ومتابعة هذه المخاطر (Al-Dosari et al., 2024) .

3. **تقليل التكاليف التشغيلية:**

يُسهم تطبيق الذكاء الاصطناعي (AI) في أتمتة عمليات رصد وتحليل البيانات، مما يؤدي إلى تقليل الحاجة للعمليات اليدوية، ومن ثمَّ خفض التكاليف المرتبطة بالتحقيقات والتقاضي الناتج عن الجرائم المالية (Gupta et al., 2023).

4. **التوسع والتكيف مع التغيرات:**

تتميز الأنظمة المعتمدة على الذكاء الاصطناعي (AI) بالقدرة على التكيف مع التغيرات في سلوك السوق، حيث يمكنها تعديل نماذجها بناءً على التحديثات في البيانات أو ظهور أنماط جديدة للجرائم المالية، مما يُعزز من قدرة المؤسسات المصرفية على مواكبة المتغيرات بسرعة وكفاءة (Al-Dosari et al., 2024).

5. **تحسين جودة البيانات:**

تسهم تقنيات الذكاء الاصطناعي (AI) في تنظيف البيانات وتحسين جودتها، مما يؤدي إلى توافر بيانات أكثر دقة وشمولية لدعم اتخاذ القرار، ومن ثمَّ تعزيز فاعلية الأنظمة المتعلقة بمكافحة الجرائم المالية (Gupta et al., 2023).

6. **الامتثال للقواعد القانونية و المعايير التنظيمية:**

تُساعد تقنيات الذكاء الاصطناعي (AI) المؤسسات المصرفية على الالتزام بالقواعد القانونية المتعلقة بمكافحة الجرائم المالية، من خلال توفير أدوات لرصد الأنشطة غير المشروعة والانتهاكات القانونية، مما يُعزز من قدرة هذه المؤسسات على الامتثال للمعايير التنظيمية (Srivastava et al., 2024).

7. **تبسيط العمليات:**

يُسهم الذكاء الاصطناعي (AI) وتطبيقاته المختلفة في تبسيط العمليات المعقدة عبر أتمتة المهام الروتينية وتحسين سير العمل، مما يضمن فاعلية أكبر في الأداء ويساعد الموظفين على التركيز على الأنشطة الأكثر إستراتيجية بدلاً من الانغماس في الأمور التشغيلية اليومية (Srivastava et al., 2024).

8. **الحد من الأخطاء اليدوية:**

تُقلل أنظمة الذكاء الاصطناعي (AI) من احتمالية حدوث الأخطاء الناتجة عن التدخل البشري، كما تُعزز التقارير المعتمدة على الذكاء الاصطناعي (AI) من الدقة وتُساعد على التحقق من المعلومات بشكل أوتوماتيكي، مما يُقلل من الحاجة إلى التحقق اليدوي المتكرر (Srivastava et al., 2024).

9. **تعزيز الكفاءة التشغيلية:**

باستخدام الذكاء الاصطناعي (AI) يمكن للمؤسسات المصرفية تحقيق كفاءة تشغيلية أعلى، حيث توفر الأنظمة الذكية القدرة على تحليل كميات ضخمة من المعلومات بطرق غير ممكنة سابقًا، مما يُعزز من سرعة اتخاذ القرارات وكفاءة العمليات الكبرى، ومن ثم زيادة الإنتاجية (Al-Dosari et al., 2024).

رابعًا: التحديات المرتبطة بتبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي:

على الرغم من أن تبني أنظمة الذكاء الاصطناعي AI في المؤسسات المصرفية يعزز من كفاءة عملية إدارة مخاطر الجرائم المالية وجهود مكافحة هذه الجرائم، إلا أنه في الوقت ذاته يطرح مجموعة من التحديات الجوهرية التي يجب معالجتها لضمان التطبيق الفعّال والمستدام لهذه التقنيات (Kok & Siripipatthanakul, 2023)، وفيما يلي نستعرض أهم هذه التحديات:

1. فقدان فرص العمل:

يُعد فقدان فرص العمل نتيجة لأتمتة المهام من أبرز المخاوف الناتجة عن تبني استخدام أنظمة الذكاء الاصطناعي AI في مؤسسات القطاع المصرفي، وفي هذا السياق تشير التقديرات إلى أن ما يزيد عن **50%** من الوظائف المصرفية بشكل عام، ومنها بالطبع تلك المتعلقة بإدارة المخاطر، معرضة للاستبدال بالأنظمة الذكية، خصوصًا الوظائف المرتبطة بإدخال البيانات والتحليل الأولي (Kovacevic et al., 2024).

2. التحيزوالتمييز:

تُظهر الأدلة والدراسات المحققة أن أنظمة الذكاء الاصطناعي AI قد تعكس التحيزات الكامنة في البيانات التي يتم تدريبها عليها، مما يؤدي إلى ممارسات تمييزية غير مقصودة، مثل رفض طلبات العملاء بناءً على خصائص اجتماعية أو ديموغرافية معينة، وهو ما يطلق عليه الظلم الخوارزمي Algorithmic Injustice (Mirishli, 2025).

3. الاعتماد المفرط على الذكاء الاصطناعي:

يمكن أن يؤدي الاعتماد المفرط على الذكاء الاصطناعي AI إلى تراجع مهارات التفكير النقدي التحليلي لدى الموظفين، مما قد يؤدي أحيانا إلى اتخاذ قرارات غير مدروسة دون تقييم بشري كافٍ (Kurshan et al., 2020) .

4. مخاطر الأمن السيبراني:

نظرًا لاعتماد أنظمة الذكاء الاصطناعي AI على البنية التحتية الرقمية، فإنها عرضة للهجمات السيبرانية، كما تم أيضا تسجيل حالات تم فيها استخدام الذكاء الاصطناعي في عمليات احتيال بمبالغ تصل إلى ملايين الدولارات (Aldasoro et al., 2024).

5. جودة البيانات وتو افرها:

تعتمد فاعلية أنظمة الذكاء الاصطناعي AI على جودة وتكامل البيانات المدخلة، ومن ثمَّ قد تؤدي البيانات الناقصة أو غير الدقيقة إلى تنبيهات كاذبة False Alerts وقرارات خاطئة (Kovacevic et al., 2024).

6. الامتثال التنظيمي:

تواجه المؤسسات المصرفية صعوبة في مواكبة التشريعات والتنظيمات المتغيرة والمتطورة باستمرار، خاصة تلك ذات الصلة باستخدام الذكاء الاصطناعي وأنظمته وتطبيقاته في العمليات والمعاملات المصرفية، وتفرض هذه الصعوبة تحديات إضافية في ضمان امتثال أنظمة الذكاء الاصطناعي للأطر القانونية والتنظيمية التي تحكم عمل هذه المؤسسات (Singh, 2024).

7. نقص المهارات:

هناك نقص ملحوظ في الكفاءات البشرية المتخصصة القادرة على تطوير وصيانة أنظمة الذكاء الاصطناعي AI في القطاع المصرفي، مما يستدعي المزيد من الاستثمارات في مجال التدريب والتطوير لهذه الكفاءات (Aldasoro et al., 2024).

8. التكامل مع الأنظمة القائمة:

تواجه المؤسسات المصرفية تحديات فنية وإدارية في دمج أنظمة وتطبيقات الذكاء الاصطناعي مع الأنظمة المصرفية القديمة، وهو ما قد يؤخر عملية التحول الرقمي ويزيد من تكاليف هذه العملية (Kovacevic et al., 2024).

9. التكاليف المرتفعة:

بصفة عامة، يمثل تبني أنظمة وتقنيات الذكاء الاصطناعي في القطاع المصرفي استثمارًا كبيرًا، لا يقتصر فقط على الجوانب التقنية، بل يشمل العديد من الجوانب، مثل التدريب وتطوير البنية التحتية وغيرها؛ ولذا قد تتجاوز التكاليف الأولية قدرة بعض المؤسسات المصرفية وإمكاناتها المالية (Singh, 2024) .

10. التنبيهات الكاذبة:

تُظهر عدة دراسات أن أنظمة الذكاء الاصطناعي قد تُصدر تنبيهات خاطئة False Alerts، سواء تنبيهات إيجابية كاذبة False Positives وهو ما يؤدي بدوره إلى إجراء المؤسسة لتحقيقات غير ضرورية تضيع الوقت والجهد، أو تنبيهات سلبية كاذبة False Negatives ينتج عنها الفشل في كشف أنشطة إجرامية فعلية، بكل ما يحمله ذلك من مخاطر وعواقب (Singh, 2024).

11. الشفافية والثقة:

يثير استخدام الذكاء الاصطناعي مخاوف تتعلق بالافتقار إلى الشفافية وقابلية تفسير قراراته، مما قد يُضعف ثقة العملاء إذا لم تكن المخرجات مفهومة أو مفسرة بشكل واضح (Mirishli, 2025).

وعليه، فإن فهم هذه التحديات والتخطيط المسبق للتعامل معها، يُعد خطوة جوهرية نحو الاستخدام الآمن والمستدام لتقنيات الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي، ورغم هذه القيود والتحديات يظل الذكاء الاصطناعي أداة إستراتيجية وفعّالة، ويمكن، من خلال سياسات حوكمة ملائمة واستثمارات مدروسة، تجاوز هذه التحديات بما يُمكّن المؤسسات المالية من تعظيم الفوائد وتقليل المخاطر المرتبطة بتطبيقه، وهذا ما سنتعرض له في السطور القادمة.

خامسًا: الآليات المقترحة لمعالجة التحديات المرتبطة بتبني الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي:

في ظل التحديات المتزايدة التي تواجه المؤسسات المصرفية في مجال مكافحة الجرائم المالية وإدارة مخاطرها، أصبح تبني تقنيات وتطبيقات الذكاء الاصطناعي (AI) ضرورة إستراتيجية لتعزيز فاعلية إدارة المخاطر والامتثال التنظيمي، ومع ذلك فهذا التبني يتطلب من المؤسسات المصرفية معالجة مجموعة من التحديات التقنية والتنظيمية والأخلاقية التي أوضحناها أعلاه لضمان الاستخدام الآمن والمستدام لهذه التقنيات، وتكمن أهم مقترحات هذه المعالجة فيما يلي (Shirvanporzour, 2025):

1. الحوكمة والامتثال التنظيمي:

تعد الحوكمة الصارمة للذكاء الاصطناعي وتطبيقاته ضرورية لضمان الامتثال للتشريعات المحلية والدولية، خاصة في مجالات مكافحة غسل الأموال وتمويل الإرهاب، وتشير الدراسات إلى أن غياب الأطر التنظيمية الواضحة قد يؤدي إلى استخدام غير مسؤول للتقنيات الذكية، مما يزيد من المخاطر القانونية والأخلاقية (Shirvanporzour, 2025).

2. جودة البيانات وإدارتها:

تعتمد فاعلية نماذج الذكاء الاصطناعي على جودة البيانات المستخدمة في تدريبها؛ لذا يجب على المؤسسات المالية الاستثمار في تحسين جودة البيانات وتحديثها بانتظام لضمان دقة التنبؤات وتقليل الإنذارات الكاذبة (Shirvanporzour, 2025).

3. الإشراف البشري والنهج الهجين:

على الرغم من القدرات التحليلية المتقدمة للذكاء الاصطناعي، يظل الإشراف البشري ضروريًا لضمان العدالة والشفافية وتقديم معلومات دقيقة وقابلة للاستخدام في اتخاذ القرارات، وفي هذا الصدد يوصى باعتماد نهج هجين يجمع بين الأتمتة والإشراف البشري، من خلال مشاركة الخبراء في التقييم والإشراف على الأنظمة، خاصة في المراحل الأولية لتبني واستخدام هذه الأنظمة والتقنيات الذكية (Al-Dosari et al., 2024).

4. الشفافية والمسؤولية:

يجب على المؤسسات المصرفية العمل على تعزيز الشفافية Transparency فيما يتعلق باستخدام الذكاء الاصطناعي من خلال توفير شروحات واضحة حول كيفية اتخاذ القرارات وتأثيرها على العملاء، مما يسهم في بناء الثقة وتعزيز المساءلة داخل المؤسسة (Shirvanporzour, 2025) .

5. قواعد لإدارة المخاوف الأخلاقية والخصوصية:

بينما يقدم الذكاء الاصطناعي العديد من المزايا، فإنه يثير أيضًا مخاوف تتعلق بالخصوصية Privacy واستخدام البيانات؛ ولذا يجب على المؤسسات المصرفية إرساء قواعد واضحة لاستخدام الذكاء الاصطناعي، مع التأكيد على حماية بيانات العملاء واحترام الخصوصية (Al-Dosari et al., 2024).

6. تطوير المهارات والتدريب:

يتطلب التبني الفعال للذكاء الاصطناعي توفير برامج تدريبية للموظفين لتعزيز فهمهم للتقنيات الجديدة وقدرتهم على التعامل معها بفاعلية، وتشير الدراسات إلى أن الاستثمار في تطوير المهارات يسهم في تحسين أداء المؤسسات وزيادة قدرتها على التكيف مع التغيرات التكنولوجية (Shirvanporzour, 2025).

سادسًا: الاتجاهات والتطورات المستقبلية لتوظيف الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي:

يُتوقَّع أن يشهد استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية تطورًا ملحوظًا في المستقبل، وذلك من خلال التحسين المستمر في أداء الخوارزميات، وتنامي الشراكات بين المؤسسات المصرفية والمالية من ناحية، ومزودي الحلول التقنية من ناحية أخرى، وتمثل هذه التطورات فرصة واعدة لتعزيز الكفاءة والفاعلية في عمليات إدارة مخاطر الجرائم المالية، بما ينعكس إيجابيًا على استقرار قطاع المؤسسات المصرفية والمالية وزيادة ثقة المتعاملين معها (Smit, 2024)، وفي هذا السياق نستعرض - فيما يلي - أبرز الاتجاهات والتطورات المستقبلية في توظيف الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية في القطاع المصرفي.

1. التطورات في خوارزميات تعلم الآلة والتعلم العميق:

أ. تحسين دقة التنبؤ:

تُعد خوارزميات تعلُّم الآلة Machine Learning والتعلُّم العميق Deep Learning من الأدوات الفعّالة في تحليل البيانات الضخمة Big Data، حيث تُمكِّن من الكشف عن الأنماط الدقيقة وفهم المعاملات المالية بشكل أكثر عمقًا، ومن المُتوقَّع أن تشهد هذه الخوارزميات تطورًا مستمرًا؛ الأمر الذي سينعكس إيجابًا على دقة نماذج التنبؤ بالمخاطر بمختلف أنواعها، سواء المخاطر الائتمانية Credit Risk أو المخاطر السوقية Market Risk أو مخاطر السيولة (Liquidity Risk Smit, 2023).

ب. التكيف والتعلم الذاتي:

تعد قدرة أنظمة الذكاء الاصطناعي على التكيف والتعلم المستمر بمرور الوقت من أبرز الاتجاهات المستقبلية في هذا المجال، ومن المتوقع أن تستثمر المؤسسات في تطوير خوارزميات ذكية قادرة على التعلم الديناميكي من البيانات التاريخية والتغيرات المستجدة في السوق، بما يعزز من مرونتها وكفاءتها في التفاعل مع التحولات المفاجئة في البيئة المالية Soori et al., (2023).

ج. التحليل الاستباقي:

سيسهم الذكاء الاصطناعي في تعزيز قدرة المؤسسات المصرفية على إجراء تحليلات استباقية تمكّن من اكتشاف المخاطر المحتملة قبل حدوثها، مما يوفّر لهذه المؤسسات فرصة اتخاذ تدابير وإجراءات احترازية فعّالة Precautionary Measures في الوقت المناسب (Smit, 2024).

2. دمج تقنيات الذكاء الاصطناعي مع التقنيات الأخرى (مثل تقنية البلوك تشين):

أ. تعزيز الشفافية والأمان:

يمكن أن يسهم دمج تقنيات الذكاء الاصطناعي مع تقنية البلوك تشين Block Chain في تعزيز الشفافية والأمان في المعاملات المالية، حيث تتيح تقنية البلوك تشين تتبع المعاملات بشكل فعال ومنع الاحتيال، في حين يوفر الذكاء الاصطناعي القدرة على تحليل البيانات المجمعة وتوجيهها نحو نماذج دقيقة لتقييم المخاطر (Kumar et al., 2023) .

ب. تحسين عمليات إدارة الهوية:

يمكن لتقنية البلوك تشين Block Chain دعم أنظمة الهوية الرقمية Digital Identity Systems بشكل فعّال، بينما يسهم الذكاء الاصطناعي في تحليل سلوك الأفراد واكتشاف الأنشطة غير الطبيعية، مما يعزز من إدارة المخاطر المرتبطة بالهوية (Kumar et al., 2023).

ج. تحليل البيانات الضخمة:

سيتيح دمج الذكاء الاصطناعي مع تقنية البلوك تشين Block Chain للمؤسسات المصرفية تحليل كميات ضخمة من البيانات بشكل آمن وسريع، مما يعزز قدرتها على اتخاذ القرارات المالية المدروسة والصائبة (Kumar et al., 2023).

3. التعاون بين المؤسسات المالية ومقدمي حلول الذكاء الاصطناعي:

أ. تطوير الحلول المخصصة:

تُسهم الشراكات بين المؤسسات المصرفية ومزودي حلول الذكاء الاصطناعي في تطوير أنظمة مخصصة Customized تتماشى مع احتياجات كل مؤسسة على حدة، مما يتيح تحسينًا أكثر فاعلية في إدارة المخاطر (Soori et al., 2023) .

ب. مشاركة المعرفة والخبرات:

تتيح هذه الشراكات بين المؤسسات المصرفية ومزودي حلول الذكاء الاصطناعي تبادل المعارف والخبرات بين الأطراف المعنية، مما يُسهم في تطوير تقنيات أكثر تقدمًا تمتاز بقدرة أعلى على التنبؤ والتحليل (Soori et al., 2023).

ج. تحسين لوائح الامتثال:

يُمكن للمؤسسات المصرفية، من خلال التعاون مع مزودي ومطوري حلول الذكاء الاصطناعي، تعزيز التزامها باللوائح التنظيمية؛ إذ يُسهم الذكاء الاصطناعي في مراقبة المعاملات وتحليل البيانات لضمان الامتثال للمعايير الدولية والأنظمة والقوانين الوطنية والقواعد الصادرة عن الهيئات التنظيمية المصرفية (Soori et al., 2023).

سابعًا: استعراض تطبيقات عملية للذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي:

يمثل الذكاء الاصطناعي أداة متقدمة تسهم بشكل متزايد في تعزيز كفاءة أنظمة إدارة المخاطر في القطاع المصرفي، وفي ظل تصاعد تهديدات الجرائم المالية وتعقيد أساليبها، بات من الضروري اعتماد حلول تقنية قادرة على التنبؤ والتصدي لهذه المخاطر بفاعلية، وفي هذا السياق يستعرض الباحث - فيما يلي - مجموعة من التطبيقات العملية التي توظف الذكاء الاصطناعي في مواجهة الجرائم المالية داخل المؤسسات المصرفية، وذلك من خلال استعراض التطبيقات المستخدمة في المجالات التالية:

1. برمجيات كشف الاحتيال.
2. أنظمة الكشف عن هجمات الاحتيال السيبراني واختراق الشبكة.
3. برامج إدارة هجمات الفدية والبرامج الضارة.

4. برمجيات حماية البيانات واكتشاف الاختراقات.
5. أنظمة إدارة المخاطر المرتبطة بالاحتيال الداخلي.
6. برمجيات إدارة الوصول والمصادقة.
7. برامج إدارة الامتثال والانتهاكات.
8. أنظمة تحليل المخاطر السيبرانية.

1. برمجيات كشف الاحتيال:

برمجيات كشف الاحتيال هي أدوات وتقنيات تستخدم لتحليل البيانات والكشف عن الأنشطة غير الطبيعية أو الخداع في المعاملات المالية أو المصرفية، وتعتمد هذه البرمجيات على خوارزميات متقدمة، مثل تعلم الآلة Machine Learning وتحليل البيانات Data Analysis، لتحديد الأنماط التي تشير إلى الاحتيال، وتسهم هذه البرمجيات في تقليل الخسائر المالية وزيادة الثقة لدى العملاء. ومن أمثلتها ما يلي (Al-Fatlawi et al., 2024):

أ. برمجيات ساس لإدارة مخاطر الاحتيال SAS Fraud Management (Hukla et al., 2024):

هو نظام متقدم طورته شركة **SAS**، ويُعدّ من الحلول المتكاملة التي تتيح للمنظمات رصد وتحليل الأنشطة المالية والنقدية لاكتشاف ومنع الاحتيال المالي في الوقت الفعلي Real Time خاصة في القطاع المصرفي ومجالات الخدمات المالية، وتعتمد هذه البرمجيات على تقنيات تحليل البيانات الضخمة وتعلم الآلة لتحليل أنماط المعاملات وتحديد الأنشطة المشبوهة فور حدوثها، ويتم استخدام هذه البرمجيات في مكافحة احتيال بطاقات الائتمان والخصم، ومراقبة عمليات التحويل المالي المشبوهة، والحماية من التلاعب في القروض أو الحسابات، وتتمتع هذه البرمجيات بالعديد من الخصائص المميزة، منها:

1. رصد المعاملات اللحظية:

مراقبة جميع المعاملات المالية في الوقت الفعلي وتحديد النشاطات المريبة والأنماط السلوكية غير الطبيعية بشكل فوري.

2. تقديم تحليلات متقدمة:

تستخدم **برمجيات ساس SAS** نماذج إحصائية وخوارزميات تعلم الآلة لاكتشاف الاحتيال المحتمل بدقة.

3. نظام إنذارات ذكي :

تقوم هذه البرمجيات بإصدار تنبيهات عند اكتشاف أنشطة مشبوهة، مما يتيح لفرق التحقيق اتخاذ الإجراءات بسرعة.

4. إمكانية التخصيص:

في هذه البرمجيات، يتم ضبط النماذج لتحليل البيانات وفقا لاحتياجات المؤسسة وبما يتناسب مع سياساتها وأنظمتها.

5. إدارة مركزية للقنوات المصرفية:

يمكن دمج جميع قنوات الدفع مثل بطاقات الائتمان، التحويلات المالية، أجهزة الصرافات الآلية، في منصة موحدة.

ب. نظام FICO Falcon المتقدم لإدارة مخاطر الاحتيال المالي (Oleiwi, 2024):

FICO® Falcon® Fraud Manager هو نظام متقدم لإدارة الاحتيال المالي، طورته شركة **FICO**، ويُعد من أكثر الحلول استخدامًا عالميًا في مجال كشف ومنع الاحتيال في المعاملات المالية .يستخدم هذا النظام على نطاق واسع من قبل المؤسسات المصرفية والمالية لتعزيز قدراتها في كشف ومنع الاحتيال المالي باستخدام تقنيات الذكاء الاصطناعي والتحليلات المتقدمة، ويمكن استخدام هذا النظام في كشف ومنع الاحتيال في بطاقات الائتمان والخصم، مراقبة التحويلات المالية والمدفوعات الرقمية، الحماية من الاستيلاء على الحسابات والاحتيال في الحسابات الجديدة، والامتثال لمتطلبات مكافحة غسل الأموال (AML) ومعرفة العميل (KYC)، ويتمتع هذا النظام بالعديد من الخصائص المميزة، منها:

1. تحليلات سلوكية متقدمة:

يعتمد النظام على تعلم الآلة لبناء ملفات سلوكية للعملاء والتجار والأجهزة، والتحليل العميق للسلوكيات المالية للمستخدمين لتحديد التغيرات المفاجئة في هذه السلوكيات؛ مما يساعد في الكشف عن الأنماط غير الاعتيادية والتصرفات المشبوهة في الوقت الحقيقي .

2. **شبكة استخبارات Falcon:**

يعتمد هذا النظام على منصة تستفيد من شبكة عالمية تضم أكثر من 9,000 مؤسسة مصرفية ومالية، حيث تُجمع بيانات معاملات مجهولة الهوية لتدريب النماذج وتحسين دقة الكشف عن الاحتيال .

3. **إدارة مركزية للحالات:**

يوفر النظام أدوات متقدمة لإدارة الحالات، مما يسهل على فرق التحقيق تتبع الحالات المشبوهة واتخاذ الإجراءات المناسبة بسرعة.

4. **مرونة في التخصيص:**

يمكن تكييف النظام ليتناسب مع احتياجات المؤسسات المختلفة، سواء كانت كبيرة أو صغيرة، مع إمكانية التوسع لتغطية قنوات ومنتجات جديدة .

2. **أنظمة الكشف عن هجمات الاحتيال السيبر اني واختراق الشبكة:**

تُعد أنظمة كشف هجمات الاحتيال السيبراني Cyber Fraud واختراق الشبكات من الحلول التقنية المتقدمة التي تعمل على المراقبة المستمرة للشبكات والأنظمة، وتعتمد هذه الأنظمة على خوارزميات متطورة لرصد السلوكيات غير الاعتيادية التي قد تدل على وجود محاولات اختراق أو هجمات احتيالية، ويكمن الهدف الأساسي من استخدامها في الكشف المبكر والاستباقي عن التهديدات، بما يسهم في تعزيز مستوى الأمن السيبراني Cyber Security داخل المؤسسات(Arjunan, 2024)، وتعد الأنظمة التالية من أهم الأنظمة المتخصصة في هذا المجال:

أ. **نظام Darktrace** (Dhiman et al., 2025):

Darktrace هو نظام أمني يعتمد على تقنيات الذكاء الاصطناعي وتعلم الآلة Machine Learning للكشف عن التهديدات الإلكترونية والاستجابة لها بشكل ذاتي وفي الوقت الفعلي، وتُستخدم حلول **Darktrace** على نطاق واسع في مختلف القطاعات، بما في ذلك **القطاع المصرفي**، حيث تلعب حلول **Darktrace** دورًا محوريًا في تعزيز الأمن السيبراني والتصدي للتهديدات المعقدة التي تستهدف المؤسسات المصرفية، ويتم ذلك من خلال الكشف المبكر عن الهجمات المعقدة والحماية الشاملة للقنوات المصرفية الرقمية، والاستجابة الذاتية للتهديدات، ومراقبة البنية التحتية المختلطة، بالإضافة إلى مساعدة هذا النظام للمؤسسات المصرفية على الامتثال لمتطلبات الحوكمة وحماية البيانات، من خلال توفير سجل دقيق للحوادث والاستجابات، ويتمتع هذا النظام بالعديد من الخصائص المميزة، منها:

1. **القدرة على التعلم الذاتي:**

وتُعرف هذه الميزة باسم "**نظام المناعة المؤسسي**"، وفيها يتعلم النظام سلوكيات المستخدمين والأجهزة داخل الشبكة لتحديد الأنماط الطبيعية، وتمكن هذه الميزة النظام من الكشف المبكر عن الانحرافات التي قد تشير إلى هجمات معقدة، مثل محاولات التسلل أو الاختراقات غير المعروفة مسبقًا، حتى تلك التي لا تُكتشف بسهولة عبر الأدوات التقليدية.

2. **الاستجابة الذاتية للهجمات:**

من خلال تقنية "**Antigena**" يمكن للنظام اتخاذ إجراءات تلقائية لاحتواء التهديدات، مثل إيقاف تحويلات مالية مشبوهة، أو فصل جهاز موظف مصاب ببرمجية خبيثة من الشبكة دون تعطيل العمليات المصرفية.

3. **رؤية شاملة للنظام:**

يوفر النظام مراقبة مستمرة لجميع مكونات البنية التحتية الرقمية المختلطة، التي تضم الشبكات المحلية، والأنظمة السحابية، وبيئات العمل عن بُعد، مما يوفر رؤية متكاملة حول المخاطر المحتملة داخل المؤسسة المصرفية وخارجها، ويُمكن من اكتشاف التهديدات عبر مختلف البيئات.

4. **الاستجابة في الوقت الحقيقي:**

يمكن للنظام اكتشاف الهجمات الإلكترونية، مثل برامج الفدية أو التصيد الاحتيالي، والتعامل معها فور حدوثها، مما يقلل من الأضرار المحتملة.

ب. نظام Splunk (Dhiman et al., 2025):

Splunk هو نظام برمجي متقدم يُستخدم لتحليل البيانات الضخمة ومراقبة الأنظمة الرقمية، ويُعد من الأدوات الرائدة في تحليل بيانات الآلة **Machine Data** في الوقت الحقيقي، ويُستخدم هذا النظام على نطاق واسع في المؤسسات الكبرى مثل المؤسسات المصرفية، وفي مجالات متعددة مثل الأمن السيبراني، وإدارة تكنولوجيا المعلومات، ومراقبة الأداء، والكشف عن الاحتيال، ومراقبة محاولات الدخول غير الطبيعية لحسابات العملاء، وتتبع نشاط العملاء والأنظمة، وتحليل أنماط التحويلات المالية لرصد محاولات الاحتيال، وضمان الجاهزية العالية للمنصات المصرفية، وتحليل الحوادث الأمنية والكشف عن البرمجيات الخبيثة من خلال تتبع حركة الشبكة.

ويتميز هذا النظام بقدرته على جمع البيانات من مصادر متعددة، مثل: سجلات الخوادم Logs، أجهزة الشبكة Routers، أنظمة التشغيل، قواعد البيانات، التطبيقات والواجهات البرمجية، ثم يقوم بتحليل هذه البيانات لحظيا وتصويرها على شكل لوحات بيانات Dashboards، ورسوم بيانية لمساعدة الفرق المتخصصة على:

أ. كشف الأعطال والمشكلات الفنية.

ب. رصد الأنشطة المشبوهة.

ج. تحليل الأداء وتحسينه.

د. ضمان الامتثال والمعايير الأمنية.

3. **برامج إدارة هجمات الفدية والبرامج الضارة:**

هي حلول تقنية متخصصة تهدف إلى التصدي لتلك التهديدات والتقليل من آثارها، وتتمثل أبرز وظائفها في الكشف السريع عن البرمجيات الخبيثة، وعزلها عن باقي النظام، واستعادة البيانات المتضررة بأمان، كما تتيح هذه البرامج تقارير دقيقة عن الأنشطة المشبوهة، وتدعم عملية التعافي بعد الهجوم (Arjunan, 2024)، ومن أبرز أمثلتها:

أ. منصة CrowdStrike (Alzboon et al., 2023):

منصة **CrowdStrike** هي منصة سحابية متقدمة للأمن السيبراني تُعرف بمنتجها الأساسي **CrowdStrike Falcon**، وتعتمد هذه المنصة على الذكاء الاصطناعي والتحليلات السلوكية، وقد صُممت لحماية الأنظمة الحساسة والأجهزة الطرفية Endpoints من التهديدات الحديثة والاختراقات المتقدمة، وتقوم المنصة بهذه المهمة بشكل رئيسي من خلال مراقبة التهديدات وسلوك المستخدمين في الوقت الفعلي Real Time Monitoring، والاستجابة للحوادث الأمنية مثل: البرمجيات الخبيثة Malware، وهجمات الفدية Ransomware وهجمات سلاسل التوريد، كما تُعدّ خيارًا قويًا لفرق الأمن السيبراني التي تحتاج إلى سرعة وكفاءة في اكتشاف والاستجابة لأي تهديد وإجراء التحقيقات الرقمية Forensics، وتمتع هذه المنصة بعدة خصائص متميزة، منها:

1. **الحماية السحابية الكاملة:**

لا تحتاج هذه المنصة إلى أجهزة مادية أو إعدادات محلية ثقيلة، حيث تعمل بالكامل من خلال واجهات سحابية.

2. **الكشف عن التهديدات بناءً على السلوك Behavioral Detection:**

تستخدم المنصة الذكاء الاصطناعي لتحليل سلوك المستخدمين والتطبيقات، واكتشاف أي نشاط غير طبيعي.

3. الاستجابة الفورية للحوادث Real-time Response:

توفر هذه المنصة أدوات تسمح بعزل الأجهزة، وإيقاف العمليات المشبوهة، وتقديم تقارير فورية عن مصدر الهجوم.

4. رصد التهديدات مدعومة بمعلومات استخباراتية Threat Intelligence:

تعتمد منصة **CrowdStrike** على قاعدة بيانات عالمية محدثة باستمرار لرصد التهديدات الجديدة والاستجابة لها بسرعة.

5. سهولة التكامل:

يمكن دمج هذه المنصة بسهولة مع أدوات أمنية أخرى وأنظمة إدارة الهوية.

ب. برمجيات Cylance (Alzboon et al., 2023):

Cylance هي إحدى الشركات المتخصصة في الأمن السيبراني Cyber Security، وتشتهر باستخدام تطبيقات الذكاء الاصطناعي وتقنيات تعلم الآلة Machine Learning لتقديم حلول حماية متقدمة ضد البرمجيات الخبيثة والتهديدات السيبرانية وحماية أجهزة الموظفين في المؤسسات والشركات وتأمين البيانات والمعلومات الحساسة؛ ولذلك تعد البرمجيات التي تنتجها هذه الشركة جزءًا مهمًا في إستراتيجيات الأمن السيبراني، خاصة في القطاعات الحساسة مثل القطاع المصرفي، وتمتلك الشركة مجموعة متنوعة من برمجيات وتطبيقات الذكاء الاصطناعي، من أهمها ما يلي:

1. CylancePROTECT:

أ. هو منتج مضاد للفيروسات (Antivirus) يعتمد بشكل رئيسي على تقنيات الذكاء الاصطناعي وتعلم الآلة لاكتشاف التهديدات، بدلاً من الطرق التقليدية.

ب. لا يعتمد هذا المنتج على توقيعات (بصمة رقمية محددة) الفيروسات التقليدية، بل يتنبأ بالتهديدات قبل حدوثها؛ ذلك أن هذا النظام يستخدم نماذج ذكاء اصطناعي مدرّبة على ملايين العينات من البرمجيات الضارة لتحديد سلوكيات التهديدات، ويستطيع التنبؤ بها ومنعها حتى قبل تنفيذها، دون الحاجة إلى تحديثات يومية للتوقيعات (signatures) .

ج. يعمل هذا النظام حتى دون اتصال بشبكة الإنترنت، أي يستطيع اكتشاف ومنع التهديدات محليًا على الجهاز، دون الحاجة إلى اتصال دائم بالإنترنت، ويعود ذلك إلى أن نموذج الذكاء الاصطناعي الخاص به مُخزن محليًا على النظام.

2. CylanceOPTICS:

أ. هي امتداد لحلول الحماية التي تقدمها أداة CylancePROTECT، وتعمل كأداة لرصد والاستجابة لتهديدات النقاط الطرفية (EDR - Endpoint Detection and Response)، وتتيح هذه الأداة جمع وتحليل البيانات المتعلقة بالنشاطات على أجهزة المستخدمين (Endpoints)، مما يساعد على الكشف عن الهجمات ومواجهتها بشكل استباقي.

ب. توفر هذه الأداة تحليلاً سلوكيًا عميقًا وتساعد في تتبع الهجمات المعقدة، حيث تعتمد على الذكاء الاصطناعي والتحليل السلوكي لفهم أنماط الأنشطة المشبوهة وتتبّع سلسلة الهجوم (Kill Chain)، ومن ثمَّ تساعد هذه الميزة في تحليل الحوادث بعد وقوعها (post-incident analysis)واكتشاف الهجمات المعقدة، كالتهديدات المستمرة المتقدمة .(Advanced Persistent Threats)

3. CylanceGUARD:

أ. هي خدمة مراقبة أمنية مدارة Managed Detection and Response تهدف إلى توفير مراقبة مستمرة وتحليلاً أمنيًا متخصصًا للشركات التي تحتاج إلى دعم خارجي محترف لتعزيز أمنها السيبراني دون الحاجة لبناء مركز عمليات أمنية داخلي.

ب. توفر هذه الخدمة مراقبة على مدار الساعة وتحليل تهديدات من قبل خبراء أمنيين، حيث يتم تحليل التنبيهات الصادرة من أدوات مثل: CylancePROTECT وCylanceOPTICS، ومن ثم اتخاذ إجراءات استجابة فورية أو توجيه فرق العملاء حول كيفية التعامل مع الحوادث.

وتتمتع برمجيات **Cylance** المختلفة عامة بالعديد من المميزات والخصائص، منها على سبيل المثال:

1. تعتمد هذه البرمجيات على الوقاية الاستباقية الفنية بدلاً من الاستجابة بعد حدوث الهجوم، حيث تحلل الملفات ونقاط النهاية بشكل استباقي باستخدام النماذج الرياضية.
2. يمكن لهذه البرمجيات تحسين الأداء بشكل كبير مقارنة بالأنظمة التقليدية، ومن ثمَّ تزداد فاعليتها ضد الهجمات المعقدة مثل هجمات الفدية Ransomware وZero-day.
3. تتمتع هذه البرمجيات باستهلاك منخفض لموارد النظام مقارنةً ببرمجيات الحماية التقليدية، حيث تعتمد على منهجيات التحليل السطحي الفعال مما يقلل من الحاجة إلى البنى التحتية الكبيرة بفضل تطويرها وسهولة استخدامها.

4. برمجيات حماية البيانات واكتشاف الاختراقات:

البرمجيات المخصصة لحماية البيانات واكتشاف الاختراقات Data Protection and Intrusion Detection Software هي أنظمة متكاملة تهدف إلى تأمين البيانات الحساسة وحمايتها من السرقة أو الوصول غير المصرح به، وتقدم هذه البرمجيات مجموعة من الخدمات تشمل: التشفير، والرصد المستمر، والتحليل المتقدم للبيانات، إضافة إلى كشف الثغرات ومحاولات الاستغلال (Srilatha & Thillaiarasu, 2023)، وفيما يلي نستعرض بعضا من نماذج هذه البرمجيات.

أ. نظام IBM Guardium (Shingornikar & Bhandari, 2023):

نظام **IBM Guardium** هو حل أمني متقدم طورته شركة IBM يُستخدم لمراقبة وتأمين قواعد البيانات Databases والبُنى التحتية للبيانات الحساسة في المؤسسات، ويندرج ضمن فئة إدارة أمان البيانات **Data Security & Protection**، ويُستخدم هذا النظام بشكل واسع في القطاعات الحساسة، ومنها القطاعات المصرفية للقيام بالعديد من الوظائف، منها:

1. **مراقبة النشاطات في قواعد البيانات Database Activity Monitoring - DAM:**
   أ. يتتبع النظام جميع العمليات التي تتم على قواعد البيانات، مثل: الاستعلامات، التعديلات، الوصول غير المشروع.
   ب. يُمكّن النظام من تتبع من قام بالوصول إلى أي نوع من البيانات، ومتى، ومن أي مكان.
2. **اكتشاف البيانات الحساسة Sensitive Data Discovery:**
   يقوم النظام بمسح قواعد البيانات وتحديد أماكن وجود البيانات الحساسة (كمعلومات العملاء أو أرقام البطاقات المصرفية).
3. **إدارة الامتثال Compliance Management:**
   أ. يوفر النظام تقارير جاهزة لتلبية متطلبات الامتثال.
   ب. يُسهل النظام عمليات التدقيق من خلال تتبع الامتثال بشكل مستمر.
4. **تحليل المخاطر Risk Analysis :**
   يستخدم النظام التحليلات للكشف عن الأنماط الغريبة أو المشبوهة في استخدام البيانات، وهو ما يساعد في منع تسربها.
5. **حماية البيانات في الوقت الحقيقي Real-Time Protection:**
   يمنع النظام بعض الأنشطة المشبوهة تلقائيًا عبر سياسات محددة مسبقًا.
6. **التكامل مع الذكاء الاصطناعي والأنظمة الأخرى:**
   يمكن دمج هذا النظام مع أنظمة أخرى مثل **IBM QRadar** لتعزيز قدرات اكتشاف التهديدات والاستجابة لها.

ب. برمجيات Varonis (Biliavskyi et al, 2024):

برمجيات **Varonis** هي مجموعة من الحلول الأمنية التي تركز على حماية البيانات الحساسة من التهديدات الداخلية والخارجية، ومراقبة النشاطات المتعلقة بالملفات والأنظمة، مع التركيز على تحليل سلوك المستخدمين داخل الشبكات المؤسسية، وتوفر برمجيات **Varonis** أدوات متقدمة لمساعدة المؤسسات المصرفية على القيام بعدة مهام، منها حماية البيانات الحساسة والمعلومات

المهمة، وحماية البيانات من التسريب غير المرغوب فيه داخل الشبكات، ومراقبة النشاطات التي تهم الامتثال وإدارة المخاطر، وتحليل التهديدات داخل الشبكات المؤسسية، واكتشاف الأنماط الغريبة في سلوك المستخدمين، وإدارة الوصول والتحكم في البيانات غير الهيكلية مثل المستندات والملفات بشكل دقيق وآمن، وتحقيق الشفافية والامتثال للوائح الأمنية.

5. أنظمة إدارة المخاطر المرتبطة بالاحتيال الداخلي:

تركز أنظمة إدارة المخاطر Risk Management Systems المرتبطة بالاحتيال الداخلي Internal Fraud على كشف الأنشطة المشبوهة التي قد تصدر عن الموظفين أو الأطراف الداخلية الأخرى ضمن المؤسسات المصرفية، وتتمثل أهداف هذه الأنظمة في تقييم مستويات المخاطر وتطوير إستراتيجيات فعالة للحد من هذا النوع من الاحتيال، وذلك من خلال مراقبة سلوكيات الأفراد وتحليل بيانات المعاملات (Putra et al., 2022)؛ وفيما يلي نستعرض بعضا من الأمثلة على هذه الأنظمة:

أ. منصة Palantir (Kuldova, 2022):

تُعدّ منصة **Palantir** واحدة من أكثر الحلول شمولية في مجال تحليل البيانات وإدارة المخاطر، وهي نظام برمجي متقدم لتحليل البيانات الضخمة Big Data Analytics، تُستخدم من قبل الحكومات والمؤسسات الكبرى لمعالجة كميات هائلة من البيانات من مصادر مختلفة، واستخلاص رؤى استخباراتية منها لدعم اتخاذ القرار، كما تساعد هذه المؤسسات في التعرف على الأنماط والاتجاهات غير العادية التي قد تشير إلى احتيال داخلي، وتتميز هذه المنصة بالعديد من الخصائص القوية، منها على سبيل المثال:

1. **تكامل البيانات Data Integration:**

تجمع المنصة بيانات من أنظمة مختلفة، مثل: قواعد البيانات، المستندات، الرسائل، الفيديوهات، ومن ثم توحدها في واجهة واحدة لتوفير رؤية شاملة.

2. **تحليل البيانات Data Analysis:**

تتيح المنصة أدوات قوية لتحليل الأنماط، والعلاقات، والسلوكيات في البيانات؛ مما يساعد على الكشف عن التهديدات أو الفرص.

3. **استخدام الذكاء الاصطناعي وتعلم الآلة:**

تدعم المنصة تطبيق نماذج الذكاء الاصطناعي وتعلم الآلة لتوقع النتائج وتحديد الأنشطة غير الطبيعية أو الاحتيالية.

4. **إجراءات الأمن والتحكم في الوصول:**

توفر المنصة حماية صارمة للبيانات من خلال إدارة دقيقة لصلاحيات المستخدمين ومراقبة الاستخدام في الوقت الفعلي.

5. **دعم اتخاذ القرار:**

تقدم المنصة تصورًا بصريًا وتحليليًا للبيانات يساعد في اتخاذ قرارات سريعة ودقيقة ورشيدة في المجالات المالية والمصرفية بناء على هذه البيانات.

ب. منصة MetricStream (Kuldova, 2022):

منصة MetricStream هي نظام برمجي متكامل يقدم مجموعة شاملة من الحلول لإدارة الحوكمة والمخاطر والامتثال (GRC)، ويُستخدم هذا النظام على نطاق واسع في المؤسسات المصرفية والمالية العالمية لإدارة مخاطر الاحتيال الداخلي وتوفير رؤية شاملة حول المخاطر وتعزيز القدرة على اتخاذ قرارات مستنيرة وتحقيق الامتثال التنظيمي، ولهذه المنصة مميزات متعددة ومتقدمة، منها:

1. **إدارة متكاملة للمخاطر والامتثال:**

توفر المنصة إطارا موحدًا لتحديد وتقييم ومراقبة المخاطر عبر المؤسسة، مما يعزز من القدرة على اتخاذ قرارات مستنيرة.

2. **تحليلات وتقارير متقدمة:**

تقدم المنصة أدوات تحليلية متطورة وتقارير تفاعلية تساعد في فهم أفضل للمخاطر والامتثال، مما يدعم اتخاذ قرارات إستراتيجية فعّالة.

3. **دعم الامتثال التنظيمي:**

تساعد المنصة المؤسسات في الامتثال لمجموعة واسعة من المتطلبات التنظيمية والمعايير الدولية، مثل: ISO 27001 .

4. **إدارة استمرارية الأعمال والتعافي من الكوارث:**

تدعم المنصة تخطيط استمرارية الأعمال والتعافي من الكوارث من خلال أدوات مرنة ومتكاملة لإدارة الأزمات والتواصل الجماعي في حالات الطوارئ.

5. **تكامل سلس مع الأنظمة الأخرى:**

توفر المنصة واجهات برمجة تطبيقات (APIs) تتيح التكامل مع أنظمة خارجية متعددة، مما يسهل تبادل البيانات وتحسين الكفاءة التشغيلية.

6. **برمجيات إدارة الوصول والمصادقة:**

تمثل برمجيات إدارة الوصول والمصادقة **Access and Authentication Management Software** أدوات تقنية متقدمة تُستخدم لتنظيم وضبط صلاحيات المستخدمين User Permissions في الوصول إلى الموارد الرقمية داخل الأنظمة المعلوماتية، وتعتمد هذه البرمجيات على آليات دقيقة للتحقق من هوية المستخدمين Identity Verification Mechanisms، بما في ذلك كلمات المرور، وتقنيات المصادقة متعددة العوامل MFA، وأنظمة التعرف البيومتري Biometric Recognition Systems، وذلك بهدف تعزيز مستوى أمان البيانات وتقليل مخاطر الوصول غير المصرح به (Ahmad, 2024)، وفي السطور التالية نستعرض بعضا من الأمثلة على هذه البرمجيات.

أ. برمجيات Okta (Singh & Aggarwal, 2023):

هي مجموعة من الحلول السحابية المتخصصة في إدارة الهوية والوصول Identity and Access Management – IAM، وتُستخدم لحماية والتحكم في وتأمين وصول المستخدمين إلى التطبيقات والأنظمة والبيانات الحساسة داخل المؤسسات، وتعتمد **Okta** على تقنيات حديثة للتحقق من الهوية وتقديم تجربة دخول آمنة وسلسة للمستخدمين، ويمكن تلخيص أهم القدرات التي تتمتع بها برمجيات **Okta** فيما يلي:

1. **الإدارة المركزية الموحدة لهويات المستخدمين Unified Identity Management:**

تسمح هذه البرمجيات للمؤسسات بإنشاء وإدارة هويات المستخدمين من مكان مركزي، مما يسهل التحكم في وصولهم إلى الأنظمة المختلفة.

2. **المصادقة متعددة العوامل MFA**:

توفر هذه البرمجيات أدوات تحقق متعددة مثل: الرسائل النصية، التطبيقات الأمنية، أو المقاييس الحيوية biometrics لزيادة أمان تسجيل الدخول.

3. **الدخول الموحد (الأحادي) Single Sign-On – SSO للتطبيقات:**

تتيح هذه البرمجيات للمستخدمين الدخول إلى جميع التطبيقات المرتبطة عبر تسجيل دخول واحد فقط، مما يسهل الاستخدام ويقلل من مخاطر كلمات المرور المتعددة.

4. **الامتثال والمعايير الأمنية:**

تساعد هذه البرمجيات المؤسسات في تلبية متطلبات الامتثال المختلفة من خلال تسجيل الأنشطة وإعداد تقارير أمنية مفصلة.

5. **التكامل مع مئات التطبيقات:**

توفر هذه البرمجيات مكتبة جاهزة للتكامل مع آلاف التطبيقات السحابية مثل: Microsoft 365، Google Workspace، Salesforce وغيرها.

6. **إدارة دورة حياة الهوية Identity Lifecycle Management:**

تقوم هذه البرمجيات بأتمتة عمليات إنشاء، تحديث، وتعطيل حسابات المستخدمين بناءً على وضعهم الوظيفي داخل المؤسسة.

7. **تحليل السلوك وإدارة المخاطر:**

تستخدم هذه البرمجيات تقنيات الذكاء الاصطناعي لتحليل سلوك المستخدمين واكتشاف الأنشطة غير العادية التي قد تشير إلى محاولات اختراق.

ب. برمجيات Ping Identity (Muhammad et al., 2024):

هي مجموعة من الحلول الأمنية المتقدمة المتخصصة في إدارة الهوية والوصول Identity and Access Management - IAM، وتُستخدم لحماية دخول المستخدمين إلى التطبيقات والأنظمة، سواء في بيئات العمل السحابية أو المحلية أو الهجينة، وتساعد هذه البرمجيات القطاعات الحساسة، ومنها المؤسسات المصرفية والتي تتطلب معايير مصادقة صارمة، على تحقيق الأمان الرقمي، وتقديم تجربة دخول سلسة وآمنة وموحدة للمستخدمين مع الالتزام بالامتثال التنظيمي، وتتمتع برمجيات Ping Identity بالعديد من القدرات المميزة التي تتشابه إلى حد مع تلك التي تتمتع بها برمجيات Okta، وفيما يلي استعراض لأهم هذه القدرات:

1. **الدخول الموحد (الأحادي) Single Sign-On – SSOللتطبيقات:**

تتيح هذه البرمجيات للمستخدمين الدخول إلى جميع التطبيقات المرتبطة عبر تسجيل دخول واحد فقط، مما يسهل الاستخدام ويقلل من مخاطر كلمات المرور المتعددة.

2. **المصادقة متعددة العوامل MFA:**

توفر البرمجيات أدوات تحقق متعددة كالرسائل النصية، البريد الإلكتروني، التطبيقات المخصصة لزيادة أمان تسجيل الدخول.

3. **الإدارة المركزية الموحدة لهويات المستخدمين Unified Identity Management:**

توفر هذه البرمجيات رؤية موحدة لهويات المستخدمين وإمكانية التحكم في صلاحياتهم من خلال واجهة مركزية موحدة، مما يسهل التحكم في وصولهم إلى الأنظمة المختلفة.

4. **تخصيص سياسات الوصول الديناميكية:**

تسمح هذه البرمجيات بوضع سياسات مرنة تعتمد على السياق (مثل الموقع الجغرافي، نوع الجهاز، مستوى الخطورة) لتحديد متى وكيف يُسمح بالوصول.

5. **إدارة دورة حياة الهوية Identity Lifecycle Management:**

تقوم هذه البرمجيات بأتمتة عمليات إنشاء، تحديث، وتعطيل حسابات المستخدمين بناءً على التغيرات في وضعهم الوظيفي داخل المؤسسة.

6. **دعم الامتثال والحوكمة:**

تساعد هذه البرمجيات المؤسسات في تلبية متطلبات الامتثال المختلفة من خلال تسجيل الأنشطة وإعداد تقارير وتحليلات أمنية مفصلة.

7. **تحليل ومر اقبة السلوك:**

توظف هذه البرمجيات تقنيات الذكاء الاصطناعي لمراقبة سلوك المستخدمين واكتشاف الأنشطة غير الطبيعية أو المشبوهة.

7. **برامج إدارة الامتثال والانتهاكات** (Aloumi et al., 2024):

تسهم برمجيات إدارة الامتثال Compliance Management Software والكشف عن الانتهاكات في مساعدة المؤسسات المصرفية على الالتزام بالمعايير القانونية والتنظيمية ذات الصلة بحماية البيانات وأمن المعلومات، وتوفر هذه البرمجيات أدوات فعالة

لمراقبة الأنشطة، واكتشاف المخالفات المحتملة، بالإضافة إلى إعداد تقارير دقيقة تسهم في تعزيز أنظمة الامتثال وتقليل المخاطر القانونية، وفيما يلي نستعرض بعضا من الأمثلة على هذه البرمجيات.

أ. برمجيات ComplyAdvantage (Aloumi et al., 2024):

ComplyAdvantage هي شركة تقنية مالية FinTech متخصصة في تقديم حلول متقدمة لإدارة مخاطر الجرائم المالية، مثل مكافحة غسل الأموال AML والتحقق من الهوية KYC باستخدام تقنيات الذكاء الاصطناعي وتعلم الآلة، وتستخدم برمجيات **ComplyAdvantage** من قبل أكثر من 1600 مؤسسة مالية حول العالم، بما في ذلك المؤسسات المصرفية، وشركات التأمين، وشركات التكنولوجيا المالية FinTech لتوفير بيئة مصرفية ومالية أكثر أمانًا وامتثالاً، ويمكن تلخيص المهام التي تقوم بها هذه البرمجيات فيما يلي:

1. **فحص العملاء Customer Screening:**

تُجري هذه البرمجيات عمليات فحص دقيقة للعملاء من الأفراد والشركات على قوائم العقوبات المختلفة، وقوائم الأشخاص ذوي المخاطر السياسية PEPs، ووسائل الإعلام السلبية، مما يساعد في تحديد المخاطر المحتملة قبل التعامل معهم.

2. **مراقبة المعاملات لحظيا Realtime Transaction Monitoring:**

تُراقب هذه البرمجيات المعاملات المالية في الوقت الحقيقي Real Time باستخدام قواعد محددة وخوارزميات تعلم الآلة Machine Learning، للكشف عن الأنشطة المشبوهة أو غير الاعتيادية.

3. **فحص المدفوعات Payment Screening:**

تُحلل هذه البرمجيات رسائل الدفع للكشف عن المخاطر المتعلقة بالعقوبات أو الأطراف المحظورة، مما يقلل من الإنذارات الكاذبة False Alerts ويحسن كفاءة العمليات.

4. **المراقبة والمتابعة المستمرة Ongoing Monitoring:**

تُراقب هذه البرمجيات وتتابع التغييرات في حالة العملاء من الأفراد والشركات بشكل مستمر، وتُصدر تنبيهات عند حدوث تغييرات قد تؤثر على تقييم المخاطر.

5. **تحليل المخاطر باستخدام الذكاء الاصطناعي AI-driven Risk Intelligence:**

تُقدم هذه البرمجيات رؤى تحليلية متقدمة حول المخاطر المالية باستخدام تقنيات الذكاء الاصطناعي، مما يساعد المؤسسات على اتخاذ قرارات مستنيرة.

ب. برمجيات وحلول LexisNexis Risk Solutions (Jofre et al., 2024):

LexisNexis Risk Solutions هي شركة عالمية متخصصة في تقديم حلول وبرمجيات تحليل البيانات وإدارة المخاطر، وتُستخدم حلولها على نطاق واسع في قطاعات مثل: الخدمات المصرفية والمالية، التأمين، الرعاية الصحية، والحكومات، وتُساعد هذه البرمجيات المؤسسات على اتخاذ قرارات مستنيرة بشأن التحقق من الهوية، منع الاحتيال، الامتثال التنظيمي، وتقييم المخاطر الائتمانية، ويمكن تلخيص الوظائف الرئيسية لبرمجيات **LexisNexis Risk Solutions** فيما يلي:

1. **التحقق من الهوية والمصادقة:**

تُوفر هذه البرمجيات أدوات متقدمة للتحقق من هويات العملاء من الأفراد والشركات، مما يُساعد في تقليل مخاطر الاحتيال وتحسين تجربة العملاء.

2. **مكافحة الاحتيال:**

تُستخدم تقنيات تحليل البيانات للكشف عن الأنشطة الاحتيالية في الوقت الحقيقي، مما يُمكّن المؤسسات من اتخاذ إجراءات سريعة وفعّالة.

3. **الامتثال التنظيمية:**

تُساعد هذه البرمجيات المؤسسات في الامتثال للمتطلبات التنظيمية من خلال أدوات فحص قوائم العقوبات، والأشخاص ذوي المخاطر السياسية PEPs، ووسائل الإعلام السلبية.

4. **تقييم المخاطر الائتمانية:**

تُوفر هذه البرمجيات للمؤسسات المصرفية تحليلات دقيقة لتقييم الجدارة الائتمانية للعملاء، مما يُساعد هذه المؤسسات في اتخاذ قرارات ائتمانية مستنيرة.

5. **إدارة البيانات والتحليلات المتقدمة:**

تُقدم هذه البرمجيات حلولاً لإدارة وتحليل كميات كبيرة من البيانات، مما يُمكّن المؤسسات المصرفية من استخراج رؤى قيمة لدعم اتخاذ القرار.

8. **أنظمة تحليل المخاطر السيبرانية:**

أنظمة تحليل المخاطر السيبرانية Cyber Risk Analysis Systems هي أدوات متخصصة تُستخدم لتقييم المخاطر المحتملة ضمن بيئات تكنولوجيا المعلومات، حيث تسهم في تقدير تأثير التهديدات السيبرانية وتحديد أولويات الاستجابة لها، وتُمكّن هذه الأنظمة المؤسسات من اتخاذ قرارات إستراتيجية تعزز من مستوى الأمن السيبراني Cyber Security، وتحُد من المخاطر المحتملة على الأصول والمعلومات الحساسة (Jofre et al., 2024)، ونستعرض فيما يلي نموذجًا من أهم نماذج هذه الأنظمة.

أ. **منصة وبرمجيات RiskLens** (Radanliev et al., 2024):

RiskLens هي منصة رائدة في مجال إدارة المخاطر السيبرانية، ومتخصصة في التحليل الكمي للمخاطر باستخدام **معيار تحليل عوامل مخاطر المعلومات Factor Analysis of Information Risk** أو ما يعرف اختصارًا باسم **FAIR** والذي يُعد المعيار الدولي لتحليل مخاطر المعلومات، وتُستخدم **RiskLens** من قبل مؤسسات كبرى في مختلف القطاعات، بما في ذلك الخدمات المالية والمصرفية والرعاية الصحية والقطاعات الحكومية، لتوفير بيئة أكثر أمانًا وامتثالاً، وتُساعد هذه المنصة المؤسسات المصرفية مثلا على تحويل التهديدات السيبرانية المعقدة إلى مقاييس مالية واضحة تمكّن الفرق الأمنية والإدارية من اتخاذ قرارات إستراتيجية قائمة على البيانات، وفيما يلي نلقي نظرة سريعة على الوظائف الرئيسية لبرمجيات **RiskLens:**

1. **التحليل الكمي للمخاطر السيبرانية:**

تُوفر هذه البرمجيات تقديرات مالية دقيقة للخسائر المحتملة الناتجة عن التهديدات السيبرانية، مما يُساعد المؤسسات المصرفية على تحديد أولوياتها فيما يتعلق بالاستثمارات الأمنية.

2. **المحاكاة:**

تمتلك هذه البرمجيات القدرة على محاكاة سيناريوهات المخاطر المختلفة لتحديد التأثير المحتمل للهجمات السيبرانية، وتقدير احتمالية وقوع خسائر مالية، مما يُعزز من دقة التقييمات.

3. **تحديد وتقييم السيناريوهات:**

تُتيح هذه البرمجيات إنشاء وتقييم سيناريوهات مخاطر مخصصة، مع تحديد الأصول والتهديدات ذات الصلة.

4. **التكامل مع الأنظمة:**

تتمتع هذه البرمجيات بالقدرة على التكامل والاندماج بسهولة مع أنظمة الحوكمة والمخاطر والامتثال (GRC)، مثل IBM OpenPagesوServiceNow، وهو ما يوفر لهذه المؤسسات رؤية شاملة للمخاطر.

5. **تحليل فاعلية الضوابط الأمنية:**

تُساعد هذه البرمجيات المؤسسات المصرفية على تقييم فاعلية الضوابط الأمنية المستخدمة فيها حاليا، وتحديد المجالات التي تحتاج إلى تحسين أو تطوير.

6. إعداد تقارير مخصصة:

تُوفر هذه البرمجيات للمؤسسات المصرفية تقارير قابلة للتخصيص تُساعد في توصيل نتائج تحليل المخاطر إلى أصحاب المصلحة بوضوح.

رابعًا: القطاع المصرفي القطري
وجهود التحول الرقمي وتبني التكنولوجيا المالية والذكاء الاصطناعي فيه

مقدمة:

يعد القطاع المصرفي القطري واحدا من أهم المكونات الحيوية لاقتصاد الدولة، وقد شهد هذا القطاع تطورًا ملحوظا منذ نشأته في مرحلته الأولى عام 1966، وصولا إلى عصرنا الحالي، وتميز هذا التطور بوجود نظام مصرفي مزدوج يشمل بنوكا تقليدية وأخرى إسلامية، حيث اكتسبت الأخيرة شهرة وقبولا واسعا بسبب الطلب المتزايد على المنتجات المالية المتوافقة مع الشريعة الإسلامية، وفي هذا القطاع برزت مؤسسات بارزة مثل **مصرف قطر الإسلامي (QIB)**، **وبنك قطر الوطني (QNB)** وغيرها كجهات فاعلة رئيسية، وهو ما يعكس قدرة هذا القطاع على التكيف والابتكار في ظل التغيرات الاقتصادية والأطر التنظيمية والرقابية المتغيرة (Fitch Report, 2024; Bait Al Mashura, 2025).

وفي العقد الحالي شهد القطاع المصرفي القطري - وما زال - تحولاً متسارعًا وغير مسبوق في ظل الثورة الرقمية العالمية، وتنامي التحديات والمخاطر المرتبطة بالجرائم المالية، ومع ازدياد حجم الأصول المصرفية لمؤسسات هذا القطاع واتساع نطاق عملياتها محليا وإقليميا وعالميا، بات اعتماد تطبيقات وتقنيات ونظم التكنولوجيا المالية Fintech خيارًا إستراتيجيًا لا غنى عنه وضرورة لا بد منها، وذلك بهدف تعزيز كفاءة إدارة المخاطر المالية، وضمان الامتثال للمتطلبات التنظيمية في بيئة مصرفية تتسم بتعقيد متزايد (IMF Report, 2023; Oxford Business Group, 2024).

وفي هذا الإطار يخصص الباحث هذا الجزء من الدراسة لاستعراض ميداني موجز لواقع القطاع المصرفي في دولة قطر، مسلطًا الضوء على أبرز المبادرات والجهود التي تبذلها المؤسسات المصرفية، تحت إشراف ومتابعة حثيثة ودقيقة وذات رؤية من **مصرف قطر المركزي (QCB)**، في سبيل تبنّي تقنيات وتطبيقات الذكاء الاصطناعي AI وتوظيفها في دعم الحوكمة Governance وتعزيز الأداء الرقابي والامتثال Compliance، وذلك من خلال دراسة العناصر التالية:

أولاً: نبذة مختصرة عن دولة قطر.

ثانيًا: تطور القطاع المصرفي القطري: الخلفية التاريخية والبنية المؤسسية.

ثالثًا: الإطار التنظيمي والإشرافي للقطاع المصرفي القطري.

رابعًا: هيكل القطاع المصرفي في دولة قطر.

خامسًا: إسهام القطاع المصرفي القطري في التنمية الوطنية وتحقيق **رؤية قطر 2030.**

سادسًا: الأداء المالي للقطاع المصرفي القطري.

سابعًا: الاتجاهات الحديثة في القطاع المصرفي القطري.

ثامنًا: التحول الرقمي والتكنولوجيا المالية في القطاع المصرفي القطري.

تاسعًا: دور مصرف قطر المركزي في تعزيز نمو التكنولوجيا المالية في القطاع المصرفي القطري.

أولاً: نبذة مختصرة عن دولة قطر:

تقع دولة قطر في قلب منطقة الخليج العربي، على شبه جزيرة تمتد بطول 160 كيلومترًا داخل مياه الخليج، وتبلغ مساحتها حوالي 11,581 كيلو مترًا مربعًا، ويحد قطر من الجنوب المملكة العربية السعودية، ومن باقي الجهات الخليج العربي، مما يمنحها موقعًا إستراتيجيًا مهمًا بين أهم طرق التجارة البحرية والطاقة في العالم، ويتمتع هذا الموقع بأهمية جيوسياسية بالغة؛ إذ يمكّن الدولة من لعب دور فاعل في الاقتصاد الإقليمي والدولي، ويُعزز من مكانتها كمركز للنقل والخدمات اللوجستية والطاقة، وقد أسهم هذا الموقع في جعل قطر نقطة عبور تجارية مهمة ومحورًا نشطا وفعالا للاستثمارات الأجنبية، وخصوصًا في مجالات الغاز الطبيعي المسال والنقل الجوي، من خلال كلا من مطار حمد الدولي وميناء حمد، اللذين يشكلان منصتين إستراتيجيتين لحركة البضائع والمسافرين إقليميًا وعالميًا (Kemp, 2025).

وتُعد دولة قطر من أبرز الاقتصادات الناشئة في منطقة الخليج العربي، حيث حققت خلال العقود الأخيرة نموًا اقتصاديًا لافتًا بفضل مواردها الطبيعية، وعلى رأسها الغاز الطبيعي، وتمتلك قطر ثالث أكبر احتياطي للغاز الطبيعي في العالم، ما مكّنها من تحقيق فوائض مالية متكررة، ورفع مستوى دخل الفرد، مما رسّخ مكانتها الاقتصادية إقليميًا ودوليًا (IMF Report, 2023).

وتمتاز دولة قطر بخصائص ديموغرافية واقتصادية تجعلها بيئة فريدة من نوعها، فهي دولة ذات دخل مرتفع، يبلغ عدد سكانها حوالي 3.08 مليون نسمة، حيث تتركز الغالبية في المناطق الحضرية (99.4%)، مع هيمنة واضحة للذكور (71%)، وغلبة للوافدين الذين يشكلون نحو (88%) من إجمالي السكان، ويعكس مؤشر التنمية البشرية المرتفع في قطر، والذي وضعها في المرتبة الأربعين عالميًا، واقعًا اجتماعيًا متقدمًا؛ إذ يبلغ متوسط العمر المتوقع فيها 81.6 عامًا، ويصل نصيب المواطن الفرد من الدخل القومي الإجمالي إلى نحو 95,944 دولارًا أمريكيًا سنويا (Kemp, 2025).

وفي السنوات الأخيرة، وخاصة بعد نجاح استضافة بطولة كأس العالم لكرة القدم **2022**، بدأت قطر في التحول التدريجي نحو تنويع اقتصادها، حيث بلغ معدل نمو الناتج المحلي الإجمالي 2.4% في عام **2024**، وتُظهر الخطط الحكومية أن الدولة تستثمر عائداتها من صادرات الغاز الطبيعي المسال في مجالات غير نفطية واعدة، مثل: القطاع المالي، والتعليم، والصحة، والسياحة، في انسجام تام مع أهداف **رؤية قطر الوطنية 2030**، وفي إطار سعيها لبناء اقتصاد قائم على المعرفة، تُعطي ميزانية الحكومة القطرية للعام **2025** أولوية واضحة لرأس المال البشري، من خلال تخصيص أكثر من 41 مليار ريال قطري لقطاعي الصحة والتعليم، كما تُشير تقديرات الموازنة إلى بلوغ الإيرادات غير النفطية نحو 43 مليار ريال، في خطوة تؤكد على تسارع مسار التنويع الاقتصادي وتقليل الاعتماد على الموارد الهيدروكربونية (Kemp, 2025).

ولتحقيق هذه الأهداف التنموية، تعتمد قطر على مجموعة من المزايا التنافسية، من بينها: الاستقرار السياسي، والسياسات الضريبية الجاذبة، والبنية التحتية المتطورة، والبيئة التشريعية المحفزة للأعمال والاستثمار، كما تركز **رؤية قطر الوطنية 2030** على دعم الابتكار، وتعزيز الاقتصاد القائم على المعرفة، وتنمية القطاعات الإنتاجية، بهدف بناء مستقبل مستدام اقتصاديًا ومؤسسيًا (World Bank, 2024).

ثانيًا: تطور القطاع المصرفي القطري: الخلفية التاريخية والبنية المؤسسية:

يُعد القطاع المصرفي أحد الركائز الأساسية في الهيكل الاقتصادي لدولة قطر، وتُظهر التجربة القطرية في مجال العمل المصرفي مسارًا تطوريًا متكاملاً، بدأ بهيمنة البنوك الأجنبية في خمسينيات القرن العشرين، وتطور تدريجيًا باتجاه تمكين المؤسسات الوطنية، وصولاً إلى بيئة مصرفية رقمية، مرنة، ومستدامة، مدعومة بسياسات تنظيمية رصينة، وتوجه إستراتيجي نحو الريادة في التمويل الإسلامي والتكنولوجيا المالية FinTech (PwC, 2024).

وقد ارتبط ظهور هذا القطاع ارتباطًا وثيقًا باكتشاف النفط في عام 1949، مما ولّد الحاجة إلى خدمات مالية رسمية تدعم الاقتصاد الناشئ، وفي عام 1950 تأسس أول بنك عامل في قطر، وهو "البنك الشرقي" (المعروف اليوم ببنك ستاندرد تشارترد/ Standard Chartered Bank)، وتبعته خلال عقدي الخمسينيات والستينيات مجموعة من البنوك الأجنبية، مثل البنك البريطاني للشرق الأوسط (HSBC)، والبنك العثماني والمعروف أيضا باسم (Grindlays Bank)، والبنك العربي، والبنك اللبناني (المشرق) وهو حاليا بنك لبنان والمهجر (BLOM BANK)، وهي البنوك التي كانت تخدم بصورة رئيسية احتياجات الحكومة وقطاع النفط (Abumughli et al., 2024).

ومع منتصف الستينيات بدأت ملامح القطاع المصرفي الوطني في التشكل بتأسيس أول بنك وطني، هو بنك قطر الوطني (**QNB**) عام **1964**، مما شكل نقطة تحول نحو تعزيز السيطرة الوطنية على القطاع، وقد أدى الازدهار الاقتصادي الناتج عن الطفرة النفطية في سبعينيات القرن الماضي إلى ترخيص بنوك وطنية إضافية مثل البنك التجاري القطري **CBQ** في عام **1975**، وبنك الدوحة Doha Bank في عام **1979**، بالإضافة إلى تأسيس أول بنك إسلامي، هو مصرف قطر الإسلامي **QIB** في عام **1982**،

ولاحقًا البنك الأهلي Ahli Bank عام **1983**، وهو ما أسهم في بروز هوية مصرفية وطنية مستقلة ومتنوعة (Abumughli et al., 2024).

أما على صعيد التنظيم والإشراف الرقابي والمؤسسي، فقد تأسست **مؤسسة النقد القطرية** في عام **1973** لتتولى إدارة السياسة النقدية والحفاظ على استقرار الريال القطري، ولاحقا تم تحويل **مؤسسة النقد** إلى **مصرف قطر المركزي QCB** بموجب المرسوم بقانون رقم (15) لسنة 1993، ليضطلع المصرف بدور الجهة الرقابية والتنظيمية العليا للقطاع، مع الاستمرار في تطبيق سياسة ربط الريال القطري بالدولار الأمريكي، بما يحقق الاستقرار النقدي والمالي للدولة (Abumughli et al., 2024).

وخلال العقدين الأخيرين من القرن العشرين شهد القطاع المصرفي القطري تطورًا نوعيًا، تميّز بإدخال المصرفية الإسلامية إلى السوق المحلية، وأسفر ذلك عن إنشاء مصارف وبنوك إسلامية رائدة، ومنها مصرف قطر الإسلامي QIB، وبنك الريان Rayan Bank، وبنك قطر الدولي الإسلامي QIIB، وبنك دخان Dukan Bank، وقدمت هذه البنوك والمصارف منتجات وخدمات مالية متوافقة مع الشريعة الإسلامية، مما رسّخ مكانة قطر كمركز إقليمي للتمويل الإسلامي (Gillet, 2022).

أما في المرحلة الممتدة من مطلع الألفية وحتى وقتنا الحاضر، فقد تمثلت أبرز ملامح التطور في التوسع المؤسسي والتحديث التشريعي، فبحلول عام 2024 كان عدد الفروع المصرفية في الدولة قد تجاوز 140 فرعًا، إضافة إلى المكاتب التمثيلية، وذلك في ظل زيادة الاندماج مع النظام المالي العالمي، ودور فاعل لمصرف قطر المركزي في الإشراف والتوجيه (Abumughli et al., 2024).

وفي العقد الأخير تبنى القطاع المصرفي منحى التحول الرقمي Digital Transformation والتكامل التكنولوجي، حيث اعتمدت البنية التحتية المصرفية في قطر تطبيقات التكنولوجيا المالية FinTech، ومعايير بازل 3 الخاصة برأس المال والسيولة، كما توسعت المؤسسات المصرفية في استخدام سلاسل الكتل Block Chain والمصرفية المفتوحة Open Banking والتمويل الأخضر Green Financing، وبدورها قدمت هذه التطورات دولة قطر بوصفها نموذجًا إقليميًا في الابتكار المصرفي والاستدامة (Abumughli et al., 2024)، وقد دعمت الدولة هذا التوجه من خلال تطوير أطر تنظيمية وإشرافية حديثة تستوعب المستجدات الرقمية، وأيضا من خلال مواءمة إستراتيجية التكنولوجيا المالية FinTech مع **رؤية قطر الوطنية 2030**، بما يرسّخ مفاهيم التنويع والابتكار (Qatar Central Bank, 2024) .

ثالثا: الإطار التنظيمي والإشرافي للقطاع المصرفي في دولة قطر:

في إطار السعي نحو بناء قطاع مصرفي قوي ومستدام، يتمتع النظام المصرفي في دولة قطر بإطار تنظيمي ورقابي متكامل يقوده مصرف قطر المركزي QCB، الذي يُعد الجهة التنظيمية والإشرافية العليا على المؤسسات المالية، ويضطلع مصرف قطر المركزي QCB بمهمة الحفاظ على الاستقرار النقدي Financial Stability، وضمان قيمة الريال القطري، وتعزيز سلامة النظام المالي في الدولة، كما يتمتع المصرف بصلاحيات واسعة في إصدار التراخيص، وتنظيم الأنشطة المصرفية، والإشراف عليها بما يتماشى مع أفضل المعايير الدولية (Qatar Central Bank, 2023).

وقد تم ترسيخ الأساس القانوني لهذا الدور من خلال القانون رقم (13) لسنة 2012 بشأن مصرف قطر المركزي وتنظيم المؤسسات المالية، وقد منح هذا القانون المصرف المركزي استقلالية مؤسسية وصلاحيات رقابية واسعة تشمل الترخيص والإشراف على البنوك التقليدية والإسلامية، والمؤسسات الأجنبية، وشركات التكنولوجيا المالية، وشركات التأمين، والمؤسسات المالية غير المصرفية، ويضم الهيكل التنظيمي لمصرف قطر المركزي ست (6) إدارات رقابية وإشرافية متخصصة، وهي: إدارة الإشراف على البنوك، وإدارة الإشراف على التأمين، وإدارة الإشراف على المؤسسات المالية الأخرى، وإدارة الإشراف على التكنولوجيا المالية، وإدارة مكافحة الجرائم المالية، وصولا إلى إدارة التراخيص، وهو ما يمثل إطارا تنظيميا يُعزز من الكفاءة والفاعلية الإشرافية التنظيمية والرقابية (Qatar Central Bank, 2023).

شكل رقم (13): الهيكل التنظيمي لمصرف قطر المركزي QCB

المصدر: مصرف قطر المركزي

وفيما يتعلق بالتنسيق الرقابي، يتعاون مصرف قطر المركزي QCB تعاونا فعالا مع كلا من هيئة تنظيم مركز قطر للمال QFCRA وهي جهة الإشراف والرقابة على المؤسسات المالية المنشأة وفق قانون الاستثمار تحت مظلة مركز قطر للمال QFC، وهيئة قطر للأسواق المالية QFMA، وهي الجهة المختصة بالإشراف والرقابة على الأسواق المالية في دولة قطر والمؤسسات العاملة بها، ومن خلال هذا التعاون يتم توحيد الجهود التنظيمية وتطوير الأطر الرقابية بشكل متكامل وشامل (Qatar Central Bank, 2023).

وبذلك يُعد الإطار التنظيمي والرقابي في قطر نموذجًا متقدمًا على مستوى المنطقة، يعكس التزام الدولة بالامتثال للمعايير الدولية، وحماية النظام المالي من المخاطر النظامية، ودعم مسار الابتكار والتحول الرقمي في القطاع المصرفي، مع المحافظة على أعلى درجات الشفافية والحوكمة (Qatar Central Bank, 2023).

رابعًا: هيكل القطاع المصرفي في دولة قطر:

مع استمرار دولة قطر في تنويع اقتصادها بعيدًا عن الهيدروكربونات والاستثمار في تطوير البنية التحتية، أصبح القطاع المصرفي أحد الركائز الأساسية للاقتصاد القطري لما يتمتع به من مستوى عالٍ من التنظيم، وبيئة تشغيلية مستقرة، ومؤشرات

أداء قوية، ويتميز هذا القطاع بتنوعه، وتطوره، واندماجه في المنظومة المالية العالمية، وهو ما جعله من بين أكثر القطاعات المصرفية تطورًا في منطقة الخليج العربي (PwC, 2024).

ويتبنى القطاع المصرفي القطري **نظاما مزدوجا** يشمل المؤسسات المصرفية أو البنوك **التقليدية والإسلامية**، حيث تعمل كل فئة ضمن إطار تنظيمي محدد وتقدم مجموعة متنوعة من الخدمات المصرفية لتلبية احتياجات قاعدة عملاء متباينة؛ فالبنوك التقليدية Traditional Banks تقدم أنشطة التمويل والإقراض والودائع والخدمات المصرفية للأفراد والشركات، بينما تلتزم البنوك أو المصارف الإسلامية Islamic Banks بمبادئ الشريعة الإسلامية في معاملاتها، وتلعب دورًا متناميًا في تمويل المشاريع الكبرى والتمويل العقاري والتجزئة المصرفية، مما عزز من مكانة قطر كمركز إقليمي للتمويل الإسلامي (S&P Global, 2025).

ويتألف القطاع المصرفي الخاضع لإشراف **مصرف قطر المركزي** من **تسعة بنوك وطنية**، و**سبعة بنوك أجنبية** مرخصة، إضافة إلى **مكتب تمثيلي واحد** لأحد البنوك الأجنبية، وتشمل البنوك الوطنية مؤسسات تقليدية كبرى مثل: **بنك قطر الوطني QNB**، و**البنك التجاري القطري CBQ**، و**بنك الدوحة Doha Bank**، و**البنك الأهلي Ahli Bank**، ومن جانب آخر تشمل البنوك والمصارف الإسلامية الوطنية الرائدة كلا من: **مصرف قطر الإسلامي QIB**، و**بنك الريان Rayan Bank**، و**بنك دخان Dukhan Bank**، بالإضافة إلى **بنك قطر الدولي الإسلامي QIIB** (QNB Group, 2025; QIB, 2015)، ويُلاحظ تزايد أهمية البنوك والمصارف الإسلامية في النظام المصرفي والمالي القطري، لا سيما في تمويل المشاريع الكبرى، والتوسع في التمويل العقاري، وتعزيز أدوات التمويل المستدام، وتُسهم هذه البنوك والمصارف بدور رئيسي في ترسيخ موقع قطر كمركز مالي إقليمي متوافق مع الشريعة الإسلامية، كما يعكس هذا التنوع المصرفي انفتاح السوق المصرفية القطرية على المنافسة الإقليمية والدولية، ويُسهم هذا التنوع أيضا في تعزيز اتصال القطاع المصرفي القطري بالأسواق العالمية، وهو ما يؤدي بدوره إلى تعزيز الابتكار وتبادل الخبرات العالمية (S&P Global, 2025).

أما من حيث **هياكل الملكية**، فتتنوع البنوك العاملة في دولة قطر بين بنوك مملوكة للدولة وأخرى مملوكة للقطاع الخاص وثالثة ذات ملكية مشتركة، ذلك إلى جانب فروع لبنوك أجنبية أو دولية، وتشير الدراسات إلى أن نوع الملكية يلعب دورًا محوريًا في تشكيل إستراتيجيات البنوك وسلوكها في تحمل المخاطر، حيث تميل البنوك ذات الملكية الحكومية إلى سلوك نهج أكثر تحفظًا مقارنة بالمؤسسات المصرفية المملوكة للقطاع الخاص؛ الأمر الذي يُسهم في تحقيق توازن في سوق التمويل المحلي (PwC, 2024).

وفي إطار تحليل البنية المؤسسية للقطاع المصرفي في دولة قطر، يبرز تصنيف البنوك العاملة كأداة تنظيمية أساسية يعتمدها مصرف قطر المركزي لتنظيم السوق وضمان الاستقرار المالي، وقد طوّر المصرف منظومة رقابية متكاملة تقوم على تصنيف البنوك وفقًا لطبيعة أنشطتها ونموذج أعمالها، بما يتيح تطبيق رقابة متمايزة تعزز من كفاءة الامتثال، وتحفز التنوع المؤسسي في النظام المالي (Qatar Central Bank, 2024)، وفي هذا الصدد يمكن تقسيم البنوك العاملة في السوق القطرية إلى ست فئات رئيسة، تُجسّد كل منها دورًا وظيفيًا وإستراتيجيًا محددًا في الاقتصاد الوطني القطري، وذلك كما يلي:

1- البنوك التقليدية Traditional Banks:

تمثل البنوك التقليدية Traditional Banks العمود الفقري للنظام المصرفي القطري، وتعمل هذه البنوك وفق نموذج قائم على الفائدة، يشمل قبول الودائع، وتقديم القروض، وتوفير التسهيلات الائتمانية، وخدمات الدفع، وتخضع هذه المؤسسات لإشراف مباشر من مصرف قطر المركزي ضمن إطار تنظيمي واضح (PwC, 2024).

ويُعد **بنك قطر الوطني QNB** أبرز هذه المؤسسات؛ إذ يُعدّ أكبر بنك في الدولة من حيث الأصول والانتشار الإقليمي، كما يضطلع بدور رائد في التمويل الاستثماري من خلال ذراعه QNB كابيتال والحائز على جائزة أفضل بنك استثماري لعام 2025، وتشمل هذه الفئة أيضًا **البنك التجاري القطري CBQ** والذي يُعد أكبر بنك خاص في الدولة، وله إسهامات واضحة في دعم

الشمول المالي وتمويل المؤسسات، إلى جانب ذلك نجد بنوكًا أخرى **كبنك الدوحة Doha Bank والبنك الأهلي Ahli Bank**، واللذين يقدمان خدمات مصرفية متكاملة للأفراد والشركات (Global Finance, 2025).

2- البنوك والمصارف الإسلامية Islamic Banks :

تُشكل البنوك أو المصارف الإسلامية Islamic Banks ركيزة أساسية في هيكل القطاع المصرفي القطري، وتعمل هذه المؤسسات وفقًا لمبادئ الشريعة الإسلامية التي تقوم على تحريم الفائدة، وتطبق صيغ تمويلية شرعية مثل: المضاربة، والمرابحة، والإجارة، والصكوك، وتخضع هذه البنوك أو المصارف الإسلامية لإشراف مزدوج من مصرف قطر المركزي QCB وهيئات الرقابة الشرعية الداخلية لضمان الامتثال الشرعي والتنظيمي (S&P Global, 2025).

ويتصدر **مصرف قطر الإسلامي QIB** هذه الفئة بفضل ريادته في تطوير المنتجات الإسلامية والتحول الرقمي، كما يتميز **بنك الريان Rayan Bank** بقاعدة رأسمالية قوية وتركيز كبير على الابتكار وتبني ممارسات تمويل أخلاقية تتماشى مع الشريعة الإسلامية، ومن جانب آخر يواصل **بنك دخان Dukhan Bank** –المعروف سابقًا **ببنك بروة** – التوسع بفضل شراكاته الإستراتيجية وهيكل ملكيته الفعّال، وتكتمل هذه الفئة بوجود **بنك قطرالدولي الإسلامي QIIB**، والذي يُعد من الفاعلين المؤثرين في سوق الصيرفة الإسلامية (Moody's Investors Service, 2025).

3- البنوك الأجنبية والدولية Foreign and International Banks :

تشمل هذه الفئة فروعًا لبنوك دولية International Banks أو بنوك أجنبية Foreign Banks مرخصة للعمل في السوق القطرية، وتتركّز أنشطتها غالبا في تقديم الخدمات المصرفية للشركات وتمويل التجارة، مع وجود بعض القيود على تقديم بعض الخدمات المصرفية للأفراد في بعض الحالات، وتُعد **بنوك HSBC**، **وستاندرد تشارترد Standard Chartered البريطانية**، **وبنك BNP Paribas الفرنسي** من أبرز البنوك الدولية العاملة في دولة قطر، وفي جانب آخر يعد **بنك المشرق الإماراتي Mashreq Bank**، **والبنك المتحد المحدود United Bank Limited (UBL) الباكستاني**، وكذا **البنك العربي المحدود ذو الملكية الأردنية**، من أبرز البنوك الأجنبية العاملة في قطر، حيث تسهم كلا الفئتين من خلال شبكاتها الدولية وخبراتها المتراكمة في تعزيز الطابع العالمي للنظام المالي القطري (Global Finance, 2025).

4- البنوك الرقمية Digital Banks:

يمثل دخول البنوك الرقمية Digital Banks تحولاً نوعيًا في النظام المالي والمصرفي القطري، حيث تُدار هذه المؤسسات بالكامل عبر الإنترنت دون الحاجة إلى وجود فروع مادية تقليدية، ويتبع مصرف قطر المركزي QCB نهجًا تدريجيًا في منح الترخيص لهذه البنوك، وهو النهج الذي يشتمل على مرحلتين: الترخيص المبدئي، ثم التشغيل الكامل بعد استيفاء المعايير التنظيمية والتقنية، ومن الأمثلة الرائدة في هذا المجال **QNB Digital**، والذي يمثل الذراع الرقمية **لمجموعة QNB**، كما تعمل جهات أخرى حاليا على استكمال متطلبات الترخيص لتقديم خدمات مصرفية رقمية متكاملة (Global Finance, 2025).

5- البنوك المتخصصة Specialized Banks :

تُعنى هذه البنوك بتقديم أدوار وظيفية محددة تخدم الأهداف الإنمائية للدولة، مثل تمويل المشاريع الصغيرة، والإسكان، والزراعة، ويتم ترخيص هذه المؤسسات لتقديم حلول مالية موجهة إلى قطاعات أعمال إستراتيجية، ويُعد **بنك قطر للتنمية QDB** أبرز مثال على هذه الفئة، حيث يبرز دوره الحيوي في دعم ريادة الأعمال وتوفير التمويل الميسر بما يخدم أهداف ومشروعات التنمية الوطنية (PwC, 2024).

6- مكاتب التمثيل Representation Offices:

يسمح الإطار التنظيمي للبنوك الأجنبية بإنشاء مكاتب تمثيلية داخل قطر لأغراض تنسيقية دون ممارسة أي أنشطة تشغيلية كالإقراض أو إدارة الحسابات، ومن الأمثلة على ذلك **مكتب البنك الشعبي المغربي** في الدوحة، والذي يلعب دور الوسيط بين

المغاربة المقيمين في قطر وفروع البنك المتواجدة بمناطق منشئهم؛ لتقريبهم من الخدمات المالية والمصرفية التي تحقق مصالحهم ومصالح عائلاتهم، كما يوفر هذا المكتب أيضا استشارات للمستثمرين القطريين الراغبين في دخول السوق المغربي، ويسهم في تعزيز العلاقات التجارية والمالية بين البلدين (PwC, 2024).

جدول رقم (3) هيكل ومؤسسات القطاع المصرفي في دولة قطر

م	المصرف / البنك	الجنسية	فئة البنك	هيكل الملكية
-1	بنك قطر الوطني - QNB	قطري	تقليدي	مملوك بشكل رئيسي للدولة القطرية بنسبة (50% - 52%) عبر جهاز قطر للاستثمار بالإضافة إلى مساهمين قطريين آخرين
-2	البنك التجاري - CBQ	قطري	تقليدي	ملكية مشتركة تشمل مستثمرين قطريين وأجانب، أفرادًا ومؤسسات.
-3	بنك الدوحة – Doha Bank	قطري	تقليدي	ملكية مشتركة بين الدولة عبر جهاز قطر للاستثمار بنسبة 17.1% وصندوق التقاعد العام بنسبة 6.7% من ناحية، وبين مؤسسات استثمارية ومساهمون محليون من الأفراد والمؤسسات من ناحية أخرى
-4	البنك الأهلي – Ahli Bank	قطري	تقليدي	ملكية مشتركة بين الدولة عبر جهاز قطر للاستثمار بنسبة 47.71% بينما يمتلك المساهمون من الشركات والأفراد القطريين مجتمعين 52.29% من الأسهم .
-5	بنك قطر للتنمية - QDB	قطري	متخصص	مملوك بالكامل للحكومة القطرية (بنك تنموي غير ربحي)
-6	مصرف قطر الإسلامي - QIB	قطري	إسلامي	ملكية مشتركة بين الدولة عبر شركة قطر القابضة التابعة لجهاز قطر للاستثمار وتمتلك 17%، ومؤسسات استثمارية عالمية بنسبة 8%، ومستثمرون قطريون آخرون من الأفراد والمؤسسات
-7	بنك قطر الدولي الإسلامي - QIIB	قطري	إسلامي	ملكية مشتركة بين الدولة عبر جهاز قطر للاستثمار بنسبة 16.62%، بينما تتاح بقيّة الأسهم (تقريبًا 83.4%) للتداول الحر من قبل مستثمرين قطريين وأجانب، خاصة بعد رفع الحد الأقصى للملكية الأجنبية إلى 100%.
-8	بنك دخان – Dukhan Bank	قطري	إسلامي	تحول البنك إلى شركة مساهمة عامة تعود مليكتها بنسبة 36% لصناديق تقاعد حكومية مختلفة، وحوالي 7% لجهاز قطر للاستثمار، و23.5 لمؤسسات استثمار خاصة محلية مثل مؤسستي بروق وسند، مع نسبة بيع وتداول حر تبلغ 33%.
-9	بنك الريان – Rayan Bank	قطري	إسلامي	ملكية مشتركة بين الدولة عبر جهاز قطر للاستثمار بنسبة20.6%،و حوالي 13.5% لصناديق تقاعد حكومية واستثمارية مختلفة، و5% لمؤسسات قطرية خاصة، وحوالي 66% للمساهمين العامين.
-10	البنك العربي المحدود	أردني	أجنبي	ملكية أردنية خاصة
-11	بنك المشرق	إماراتي	أجنبي	ملكية إماراتية خاصة
-12	بنك ستاندرد تشارترد	بريطاني	أجنبي	ملكية بريطانية عامة
-13	بنك HSBC الشرق الاوسط	بريطاني	أجنبي	ملكية بريطانية عامة
-14	بنك يونايتد المحدود	باكستاني	أجنبي	ملكية باكستانية حكومية
-15	بنك صادرات إيران	إيراني	أجنبي	ملكية إيرانية حكومية
-16	بنك بي أن بي باريبا	فرنسي	أجنبي	ملكية فرنسية عامة
-17	البنك الشعبي المركزي المغربي	مغربي	مكتب تمثيل	ملكية مغربية حكومية

المصدر: من إعداد الباحث بناء على مصادر الدراسة

خامسًا: إسهام القطاع المصرفي القطري في التنمية الوطنية وتحقيق رؤية قطر 2030:

يعد القطاع المصرفي في دولة قطر دعامة أساسية للاقتصاد الوطني، ويؤدي دورًا حيويًا في دفع عجلة التنمية، خاصة في سياق تحقيق أهداف **رؤية قطر الوطنية 2030**، فمع بلوغ أصول هذا القطاع نحو 2.2 **تريليون ريال قطري** بحلول العام الحالي **2025**، وهو ما يعادل حوالي **198%** من الناتج المحلي الإجمالي، يتضح جليا مدى أهمية هذا القطاع ضمن الهيكل الاقتصادي للدولة، وعلى الرغم من أن وتيرة نمو الأصول قد جاءت أبطأ قليلاً من التوسع الاقتصادي العام، فإن القطاع يظل محوريًا في دعم الأنشطة الاقتصادية، سواء النفطية أو غير النفطية، وفي إطار الإسهام في الناتج المحلي الإجمالي غير النفطي، تلعب المؤسسات المصرفية القطرية دورًا مؤثرًا في تمويل توسع إنتاج الغاز الطبيعي المسال (LNG)، وهو ما يسهم في تعزيز النمو غير النفطي، ويدعم

توجهات الدولة نحو تنويع الاقتصاد، وتشير نسبة الودائع إلى الناتج المحلي، التي تجاوزت 91% في السنوات الأخيرة، إلى عمق هذا القطاع ودرجة ارتباطه العضوي بالتنمية الاقتصادية (Moody's Investors Service, 2025).

كما تُعَدّ المؤسسات المصرفية القطرية شريكًا فاعلاً في تمويل أولويات التنمية الوطنية، لا سيما في مجالات المشروعات الصغيرة والمتوسطة (SMEs)، وقطاع الإسكان، والبنية التحتية؛ فقد وسّعت المؤسسات المصرفية القطرية نطاق تمويلها الموجّه إلى المشاريع الصغيرة والمتوسطة عبر أدوات ومنتجات مالية مدعومة بضمانات حكومية، دعمًا لريادة الأعمال وتعزيزًا لدور القطاع الخاص، وفي قطاع الإسكان تشكل القروض العقارية أكثر من 30% من محافظ التجزئة في بعض المؤسسات المصرفية القطرية، مما يعزز مبادرات تملك المساكن التي تتبناها الدولة، أما على صعيد البنية التحتية، فقد اضطلع القطاع المصرفي بدور أساسي في تمويل المشاريع الكبرى في مجالات مختلفة كمجالات النقل، والتعليم، والرعاية الصحية، بما يتسق مع الركائز الإستراتيجية **لرؤية قطر 2030** (QNB Financial Services, 2025).

وفي سياق تنويع الاقتصاد يوجّه القطاع المصرفي تمويلاته بشكل متزايد إلى القطاعات غير النفطية، مثل العقارات والخدمات والصناعة؛ إذ يذهب نحو 40% من الائتمان المحلي إلى تلك القطاعات، مما يعزز جهود التحول الاقتصادي، كما تعمل المؤسسات المصرفية القطرية على دعم جهود الشمول المالي Financial Inclusion من خلال الاستثمار في التكنولوجيا المصرفية وتوسيع شبكة الخدمات، بما في ذلك الوصول إلى الشرائح غير المخدومة مصرفيا، مثل الشباب والسيدات وذوي الهمم والعمال ذوي الدخل المحدود والمجتمعات خارج المدن وغيرها من الفئات الهشة، ويأتي ذلك انسجامًا مع المبادئ التوجيهية للنمو الشامل في **رؤية قطر 2030** (QNB Financial Services, 2025).

ويتقاطع هذا التوجه مع **الإستراتيجية الوطنية للتكنولوجيا المالية (2023-2027)**، التي تهدف إلى ترسيخ مكانة قطر كمركز إقليمي للتمويل الرقمي Digital Financing، وتُسهم المؤسسات المصرفية القطرية في هذا الإطار عبر تسريع جهود التحول الرقمي Digital Transformation، واعتماد تقنيات الذكاء الاصطناعي AI والحوسبة السحابية Cloud Computing، إضافة إلى تعزيز الشراكات مع شركات التكنولوجيا المالية FinTech الناشئة ضمن بيئات تنظيمية مرنة، كما أن الالتزام الصارم بالمعايير التنظيمية في مجالات الأمن السيبراني Cyber Security والتكنولوجيا التنظيمية RegTech يوفر إطارا حيويًا لتبني الابتكار Innovation وتحقيق الاستدامة المالية Financial Sustainability (Moody's Investors Service, 2025).

سادسًا: الأداء المالي للقطاع المصرفي في قطر:

شهد القطاع المصرفي القطري خلال السنوات الأخيرة أداء ماليًا لافتًا، وجاء ذلك مدعومًا بإطار تنظيمي قوي، وبيئة اقتصادية مستقرة، وقدرة عالية على امتصاص الصدمات. وقد أظهرت **الأزمة المالية العالمية في 2008** مرونة المؤسسات المصرفية القطرية، خاصة الإسلامية منها، في الحفاظ على مستويات مستقرة من السيولة Liquidity والربحية Profitability. وكان ذلك ما عزز الثقة في الصيرفة الإسلامية وأسهم في توسعها داخل دولة قطر بشكل خاص، وكذا في دول مجلس التعاون الخليجي بشكل عام (QNB Financial Services, 2025).

وفي السنوات التالية أسهمت عوامل متعددة، مثل الدعم الحكومي وزيادة الإنفاق العام والاستثمار في البنية التحتية، إلى جانب الإصلاحات التي تبناها مصرف قطر المركزي QCB، في تعزيز صلابة هذا القطاع، فقد تم تطبيق **معايير بازل 3**، مما ساعد على رفع مستويات كفاية رأس المال Capital Adequacy، والتي بلغت في بعض الفترات 18.2%، ورأسمال الفئة الأولى 17.0%، وهي نسب تعكس متانة الوضع المالي للمؤسسات المصرفية القطرية، كما سجّل القطاع أداء متقدمًا من حيث الكفاءة التشغيلية Operational Efficiency، مستفيدًا من التحول الرقمي Digital Transformation وتوظيف التكنولوجيا المالية FinTech في تقليص التكاليف التشغيلية Operational Costs وتعزيز الإنتاجية، فخلال الربع الثالث من عام 2023 سجلت

المؤسسات المصرفية القطرية أعلى نمو ربع سنوي في صافي دخل الفوائد بين المؤسسات المصرفية الخليجية بنسبة 10.8%، تزامنًا مع أدنى مستويات التكاليف التشغيلية Operational Costs في المنطقة (QNB Financial Services, 2025).

ورغم التحديات المرتبطة بتقلبات بعض القطاعات، مثل العقارات، حافظ القطاع المصرفي القطري على مستويات معتدلة من القروض المتعثرة، حيث بلغت نحو 2.3% في عام 2023، وفقًا لبيانات مصرف قطر المركزي، وتشير التقديرات الأولية إلى تحسن طفيف في جودة الأصول خلال عام 2024، بدعم من سياسات إدارة المخاطر الفعالة.

كما تؤكد وكالات التصنيف الائتماني، مثل **Moody's**، أن المؤسسات المصرفية القطرية تحافظ على تصنيفات ائتمانية قوية A1 أو A2 تعكس قوة رأسمالها، وتوافر السيولة Liquidity، وانخفاض نسب التعثر Default Rates، وهو ما يعزز ثقة المستثمرين المحليين والدوليين (Moody's Investors Service, 2025).

وفيما يتعلق بالإسهام الاقتصادي، فقد سجلت الأنشطة المالية، التي يُعد القطاع المصرفي ركيزتها الأساسية، نموًا سنويًا بنسبة 11.1% خلال الربع الرابع من عام 2024، بقيمة 14.8 مليار ريال قطري، من أصل الناتج المحلي غير النفطي البالغ 181 مليار ريال، ما يُبرز أهمية القطاع في تحقيق أهداف التنويع الاقتصادي، وبلغت أصول المؤسسات المصرفية القطرية حوالي 2 تريليون ريال بنهاية 2024، مع سيولة نسبتها 31.3% من إجمالي الأصول، وكفاية رأس مال عند 19.9%، في حين استقرت القروض المتعثرة عند 4.% (QNB Financial Services, 2025).

وبحسب تقرير شركة بنك قطر الوطني للخدمات المالية QNB Financial Services لعام 2025 فقد واصلت أصول المؤسسات المصرفية القطرية نموها لتبلغ 2.074 تريليون ريال بنهاية الربع الأول من 2025، وهو أعلى مستوى تاريخي، بزيادة سنوية قدرها 4.4%، مدعومة بارتفاع حجم الائتمان إلى 1.39 تريليون ريال، كما شهدت الودائع المصرفية نموًا بنسبة 2.7% على أساس سنوي، لتصل إلى 1.06 تريليون ريال، مدفوعة بشكل رئيس بزيادة ودائع غير المقيمين بنسبة 6.6.% (QNB Financial Services, 2025).

سابعًا: الاتجاهات الحديثة في القطاع المصرفي القطري:

يشهد القطاع المصرفي القطري تحولاً نوعيًا مدفوعًا بعدد من الاتجاهات الحديثة التي تعكس استجابته الفعّالة للمتغيرات الاقتصادية العالمية والتطورات التكنولوجية وتنامي المتطلبات المرتبطة بالتنمية المستدامة، وقد أسهم هذا التفاعل في تعزيز القدرة التنافسية للقطاع إقليميًا ودوليًا، ورسّخ توجه القطاع ومؤسساته نحو نموذج أكثر شمولية ومسؤولية، يجمع بين الكفاءة المالية والإسهام المجتمعي والالتزام البيئي، بما يتسق مع أهداف **رؤية قطر الوطنية 2030** و**إستراتيجية التنمية الوطنية الثالثة (2024 – 2030).**

ويسترشد القطاع المصرفي في قطر **بالخطة الإستراتيجية الثالثة للقطاع المالي (2024–2030)** التي أطلقها **مصرف قطر المركزي**، وتسعى هذه الخطى إلى تطوير منظومة مالية متقدمة ومتنوعة، من خلال تبني أولويات إستراتيجية تشمل التحول الرقمي Digital Transformation، وتطوير البنية التحتية للمدفوعات Payment Infrastructure، وتحفيز الابتكار، وتعزيز الشمول المالي Financial Inclusion، وتوسيع نطاق التمويل المستدام Sustainable Finance، وتطبيق مبادئ الحوكمة البيئية والاجتماعية والمؤسسية ESG (QCB, 2023). وتشمل الاتجاهات والأولويات الإستراتيجية في القطاع المصرفي القطري ما يلي:

1. تنامي دور التمويل الإسلامي:

يواصل التمويل الإسلامي Islamic Finance ترسيخ موقعه داخل النظام المصرفي القطري، حيث تمثل البنوك والمصارف الإسلامية منافسًا رئيسيًا لنظيرتها التقليدية، ويرجع هذا إلى قدرة البنوك والمصارف الإسلامية على تقديم منتجات مالية متوافقة مع أحكام الشريعة الإسلامية تلبي تطلعات شريحة واسعة من العملاء، لا سيما في مجالات تمويل المشاريع الكبرى، والتجزئة المصرفية Retail Banking، وخدمات إدارة الثروات Wealth Management، وقد أدى هذا النمو إلى تعزيز إسهام هذه المؤسسات في دعم التنمية الاقتصادية، وتنويع هيكل السوق المصرفي المحلي (Hadchity, 2025).

2. **التحول الرقمي والابتكار التكنولوجي:**

يُعد التحول الرقمي Digital Transformation أحد أهم المحاور الإستراتيجية للمؤسسات المصرفية القطرية، مدفوعًا في ذلك بالتطور في مجالات الذكاء الاصطناعي AI، وتعلم الآلة Machine Learning، وتحليل البيانات الضخمة Big Data Analysis، وتُولي **إستراتيجية التنمية الوطنية الثالثة (2024 – 2030)** اهتمامًا خاصًا بالبنية التحتية الرقمية، حيث تستثمر المؤسسات المصرفية في الحوسبة السحابية Cloud Computing، وتطبيقات الذكاء الاصطناعي AI Applications، وتحليلات البيانات Data Analysis، بهدف تحسين الكفاءة التشغيلية Operational Efficiency، وتعزيز تجربة العملاء Customer Experience، ورفع مستوى الأمان السيبراني Cyber Security، كما تبنّى **مصرف قطر المركزي QCB** مبادرات متعددة لتطوير أنظمة الدفع الرقمية Digital Payment Systems وتعزيز إدارة البيانات Data Management، بما يرسّخ مكانة دولة قطر كمركز مالي رقمي متقدم (QCB, 2023).

3. **تعزيز إدارة المخاطر وتبني نماذج أعمال مرنة:**

في ظل التحديات العالمية، من تقلبات أسعار الطاقة، والتغيرات الجيوسياسية، والضغوط التنظيمية، يتجه القطاع المصرفي القطري إلى اعتماد نماذج تشغيلية مرنة تتكيف مع الديناميكيات السوقية المتغيرة، ويشمل ذلك تطوير أدوات تحليل متقدمة لإدارة المخاطر الائتمانية Credit Risks، والتشغيلية Operational Risks، والتقنية Technical Risks، مما يُعزز من قدرتها على الصمود وتحقيق الاستقرار المالي طويل الأمد (PwC, 2024).

4. **الشمول المالي والابتكار لخدمة الفئات غير المخدومة مصرفيا:**

يُعدّ تعزيز الشمول المالي Financial Inclusiuon من الأهداف الأساسية للمؤسسات المصرفية في قطر، وذلك عبر تطوير منتجات وخدمات موجهة للفئات غير المخدومة مصرفيًا، مثل الشباب والسيدات وذوي الهمم والعمال ذوي الدخل المحدود والمجتمعات خارج المدن وغيرها من الفئات الهشة، وتتعاون المؤسسات المصرفية مع شركات التكنولوجيا المالية لتوفير حلول مبتكرة تشمل المحافظ الرقمية Digital Wallets، والخدمات المصرفية عبر الهاتف المحمول Mobile Banking، والتصنيف الائتماني البديل Alternative Credit Scoring، مما يُسهم في توسيع قاعدة العملاء وتعزيز الاستقرار الاجتماعي والاقتصادي (Bi et al., 2025).

5. **تبني مبادئ الحوكمة كقيمة مؤسسية:**

تشهد مؤسسات القطاع المصرفي توجهًا متزايدًا نحو دمج مبادئ الحوكمة البيئية والاجتماعية والحوكمة المؤسسية ESG ضمن عملياتها الأساسية، ويشمل ذلك إدراج معايير الاستدامة Sustainabilityفي قرارات التمويل، وابتكار أدوات مالية خضراء Green Financial Instruments، مثل القروض المستدامة Sustainable Loans، والصكوك البيئية Green Sukuk، بالإضافة إلى إصدار تقارير الأداء غير المالي وفقًا للمعايير العالمية، ويُعزز هذا التوجه من ثقة المستثمرين، ويؤكد التزام المؤسسات المصرفية القطرية بتحقيق قيمة طويلة الأجل تتجاوز المؤشرات المالية التقليدية (PwC, 2024).

6. **التوسع الإقليمي وتنويع الأسواق:**

تستثمر المؤسسات المصرفية القطرية فائضها الرأسمالي لتوسيع نطاق عملياتها إقليميًا ودوليًا، سواء من خلال فتح فروع جديدة لها في الأسواق المجاورة، أو عبر شراكات إستراتيجية مع مديري الأصول الدوليين، وتهدف هذه الخطوة إلى تنويع مصادر الدخل وتقليل الاعتماد على السوق المحلي، بالإضافة إلى تعزيز نفوذ المؤسسات المصرفية القطرية على مستوى العالم (Oxford Business Group, 2024) .

ثامنًا: التحول الرقمي والتكنولوجيا المالية في القطاع المصرفي القطري:

يشهد القطاع المصرفي القطري في السنوات الأخيرة تحولاً رقميًا عميقًا، يُجسد الرؤية الإستراتيجية للدولة نحو بناء اقتصاد معرفي متنوع، ويتسق مع أهداف **رؤية قطر الوطنية 2030**، وقد جاء هذا التحول نتيجة تفاعل عدة عوامل، من أبرزها الإصلاحات التنظيمية التي يقودها مصرف قطر المركزي، والتطورات المتسارعة في تقنيات التكنولوجيا المالية (FinTech)، إلى جانب تغيّر سلوكيات العملاء، والدفع نحو تعزيز الاستدامة والاقتصاد الرقمي (QCB, 2024)، وفيما يلي نستعرض أهم ملامح هذا التحول:

1. الإطار التنظيمي الوطني للتحول الرقمي:

أطلقت وزارة الاتصالات وتكنولوجيا المعلومات "**أجندة قطر الرقمية الوطنية 2030**"، التي تمثل خارطة طريق إستراتيجية لتحديث البنية الرقمية في مختلف القطاعات، وفي مقدمتها القطاع المالي، وتركّز هذه الأجندة على تبني الحوسبة السحابية Cloud Computing، والأتمتة الذكية Intelligent Automation، وتقنيات الاتصال المتقدمة، بغرض تحقيق كفاءة تشغيلية أعلى، وفي هذا السياق أعلن **مصرف قطر المركزي QCB** عن "**الخطة الإستراتيجية الثالثة للقطاع المالي (2024–2030)**"، التي تهدف إلى ترسيخ مكانة دولة قطر كمركز مالي إقليمي بحلول عام 2030، من خلال تعزيز بيئة الابتكار، وتطوير أطر تنظيمية مرنة للبنوك الرقمية، وتفعيل **الإستراتيجية الوطنية للتكنولوجيا المالية (2023-2027)** (QCB, 2024).

2. التكنولوجيا المالية كمحرك للنمو الاقتصادي:

أصبحت التكنولوجيا المالية FinTech أحد المحاور الرئيسية لدفع عجلة النمو الاقتصادي، بفضل ما توفره من حلول مرنة ومخصصة، لا سيما في تمويل المشاريع الصغيرة والمتوسطة SMEs، والمدفوعات الرقمية Digital Payments، وإدارة الثروات Wealth Management، وقد عزّز التعاون بين المؤسسات المصرفية القطرية وشركات التكنولوجيا المالية من كفاءة المنظومة المصرفية، من خلال تبني تقديم حلول ذكية تشمل كلا من المدفوعات الرقمية Digital Payments، والتمويل الصغير Small Lending، والخدمات المصرفية الذاتية Self-service banking، والمحافظ الرقمية Digital Wallets، وخيارات "اشترِ الآن وادفع لاحقًا (BNPL)"، وأنظمة الدفع المدمجة (Bi et al., 2025).

كما أسهمت مبادرات مثل "مسرّعات قطر للتكنولوجيا المالية Qatar FinTech Accelerators"، بالتوازي مع تنظيم فعاليات دولية مثل قمة الويب Web Summit قطر 2025، في جذب رواد الأعمال العالميين، وتعزيز التعاون بين المؤسسات المصرفية والشركات الناشئة والهيئات التنظيمية، مما أسهم في ترسيخ بيئة مصرفية تنافسية وابتكارية (QNB, 2025).

3. التحول الرقمي وتكامل الخدمات الذكية:

أتاح الإطار التنظيمي لمصرف قطر المركزي QCB دمج تقنيات رقمية متقدمة ضمن العمليات المصرفية، مما عزز من التحول الرقمي Digital Transformation ورفع مستوى جودة الخدمات، واعتمدت المؤسسات المصرفية القطرية على أدوات متقدمة تشمل تقنيات التحقق البيومتري Biometric Verification، وتحليلات البيانات الضخمة Big Data Analysis، والذكاء الاصطناعي AI، والمحافظ الرقمية Digital Wallets، وقد أدى انتشار جائحة كورونا (كوفيد-19) إلى تسريع هذا التحول، عبر تبني تقنيات مثل سلسلة الكتل Block Chain وأنظمة الذكاء الاصطناعي للكشف عن الاحتيال AI Fraud Detection Systems، بما عزز من المرونة التشغيلية لهذه المؤسسات (Bi et al., 2025).

وفي هذا الإطار، برزت نماذج بارزة منها **منصة مصرف قطر الإسلامي QIB المصرفية** الحائزة على عدة جوائز دولية، والتي توفر أكثر من 300 خدمة، منها إمكانية فتح حساب عن بُعد (QIB, 2025)، وكذلك مبادرة "ALRAYAN GO" من **بنك الريان**، وهي مناطق خدمة رقمية ذاتية تعتمد الذكاء الاصطناعي لتقديم خدمات مرنة خارج الفروع التقليدية (Rayan Bank, 2025).

4. الابتكار المؤسسي والمختبرات التجريبية:

دعمًا للابتكار، أطلق مصرف قطر المركزي QCB مبادرة مختبر التكنولوجيا المالية Regulatory Sandboxes، والمبادرة هي منصة خاضعة للرقابة تتيح اختبار حلول مالية مبتكرة في بيئة منظمة وآمنة، وتُسهم في تمكين الشركات الناشئة من تطوير نماذج أعمال متقدمة ضمن إطار يوازن بين الابتكار والاستقرار المالي (Al-Sharq,2025)، وقد مثّلت بطولة كأس العالم FIFA 2022 التي نظمتها قطر بنجاح نقطة تحول حاسمة في مجال الابتكارات المصرفية، حيث ساعدت في تسريع البنية الرقمية وتعزيز التفاعل الفوري بين المؤسسات المصرفية والعملاء، مما عزز مكانة قطر إقليميًا كمركز مالي ذكي (Bi et al., 2025).

5. الخدمات المصرفية المفتوحة وواجهات التطبيقات (APIs) :

برزت الخدمات المصرفية المفتوحة Open Banking Platform كأداة رئيسية في تطوير القطاع المصرفي في قطر، وتسمح واجهات برمجة التطبيقات API بمشاركة البيانات المالية بشكل آمن بين المؤسسات المصرفية وشركات التكنولوجيا المالية، مما يتيح تطوير خدمات مالية أكثر تخصيصًا وفاعلية، ويعزز من الشفافية وسرعة الابتكار (Bi et al., 2025).

6. الذكاء الاصطناعي والتقنيات المتقدمة في العمليات المصرفية:

يشكل الذكاء الاصطناعي AI والحوسبة السحابية Cloud Computing والتحليلات البيانية التنبؤية Predictive Analytics ركيزة جوهرية في التحول الرقمي Digital Transformation للمؤسسات المصرفية القطرية، ويُوظّف الذكاء الاصطناعي AI في أتمتة العمليات Process Automation، وإدارة المخاطر Risk Management، وتقديم توصيات مالية مخصصة، كما اعتمدت المؤسسات المصرفية القطرية على الذكاء الاصطناعي لتعزيز الأمان، حيث طُبّقت أنظمة المصادقة البيومترية Biometric Verification وخوارزميات كشف الاحتيال في الوقت الحقيقي Real Time Fraud Detection Algorithms، إضافة إلى دمج تقنيات سلسلة الكتل Block Chain مع أنظمة الذكاء الاصطناعي لتأمين المعاملات (Bi et al., 2025).

ومن النماذج البارزة في هذا الإطار، نجد تبني **بنك قطر الوطني QNB** لتقنيات الذكاء الاصطناعي لتقليل خسائر الاحتيال بنسبة تقارب 40% (QNB, 2025)، بينما يعتمد **مصرف قطر الإسلامي QIB** نظام مراقبة مدعومًا بالذكاء الاصطناعي لحماية قنواته الرقمية، كما أطلق **مصرف قطر الإسلامي QIB** مساعدًا رقميًا متعدد اللغات يدعى **"زكي"** (QIB, 2025)، في حين يوفر **بنك الريان** روبوتات محادثة ذكية على مدار الساعة (Rayan Bank, 2025).

ومن جانب آخر، يُعتمد الذكاء الاصطناعي أيضًا في بناء نماذج ائتمانية آلية قائمة على تعلم الآلة Machine Learning، ومثال ذلك ما يقدمه بنك **قطر للتنمية QDB** في تمويل المشاريع الناشئة، كما تُستخدم تقنيات أتمتة العمليات الروبوتية (RPA) في **بنك قطر الوطني QNB** لتقليل الاعتماد على العامل البشري وتحسين دقة التقارير التنظيمية (QDB & QNB, 2025).

7. التمويل الرقمي المستدام والابتكاري:

يشهد القطاع المصرفي القطري حاليا تبني نماذج تمويل مبتكرة، مثل التمويل الجماعي Crowdfunding والخدمات المصرفية الافتراضية Virtual Banking Services، وهو ما يتيح فرصًا تمويلية غير تقليدية لأصحاب المشاريع الناشئة، كما تدرس قطر إمكانية إصدار عملة رقمية قطرية بواسطة مصرف قطر المركزي (CBDC) في ظل التوسع في استخدام المحافظ الإلكترونية، وهو ما يعزز من الشمول المالي (GoGlobe, 2024).

وفي سياق الاستدامة تبنّت المؤسسات المصرفية القطرية أنظمة دفع خضراء Green Payment Systems تسعى إلى تقليل البصمة الكربونية، إلى جانب إصدار الصكوك والسندات الخضراء Green Sukuk لتمويل مشاريع الطاقة النظيفة والبنية البيئية، بما يتماشى مع توجهات الاقتصاد منخفض الكربون (GoGlobe, 2024).

8. الأمن السيبراني وإدارة المخاطر التقنية:

تزايدت أهمية الأمن السيبراني Cyber Security في ظل الاعتماد المتنامي على التكنولوجيا، حيث استثمرت المؤسسات المصرفية في أنظمة حماية متقدمة، وخطط استمرارية الأعمال Business Continuity، وتحليل التهديدات السيبرانية، ويشير تقرير مصرف قطر المركزي QCB إلى أن غالبية المؤسسات المصرفية تصنف مخاطر الفضاء السيبراني بأنها "**عالية إلى عالية جدًا**"، وهو ما يبرز الحاجة إلى أطر صارمة لحماية البيانات وتحقيق المرونة التشغيلية (QCB, 2023) .

تاسعًا: دور مصرف قطر المركزي في تعزيز نمو التكنولوجيا المالية في القطاع المصرفي القطري:

يشهد القطاع المصرفي في دولة قطر تحولاً متسارعًا في بنيته الرقمية والوظيفية نتيجة التوسع في تطبيقات التكنولوجيا المالية(FinTech) ، وذلك ضمن رؤية إستراتيجية يقودها مصرف قطر المركزي QCB بالتنسيق مع الجهات التشريعية والمؤسسات المالية، وتكمن أهمية هذا التحول في أنه لا يستند فقط إلى الابتكار التكنولوجي، بل إلى بيئة تنظيمية داعمة ومترابطة تسعى إلى تحقيق التوازن بين تمكين الابتكار وضمان الاستقرار المالي، وفي هذا السياق تمثل الأطر التنظيمية أداة فاعلة لدعم نمو التكنولوجيا المالية، وتعزيز تنافسية النظام المصرفي القطري إقليميًا وعالميًا، بما يتماشى مع ركائز **رؤية قطر الوطنية 2030**، وفيما يلي نستعرض باختصار دور **مصرف قطر المركزي QCB** وجهوده في تعزيز **نمو التكنولوجيا المالية FinTech** في **القطاع المصرفي القطري.**

1. الإطار الإستراتيجي الشامل للتكنولوجيا المالية:

أ. **تعزيز الابتكار من خلال السياسات الوطنية:**

أطلق مصرف قطر المركزي QCB **الخطة الإستراتيجية الثالثة للقطاع المالي (2024-2030)** التي ترتكز على دعم النمو والابتكار في القطاع المالي، وتشمل هذه الخطة الإستراتيجية إنشاء وحدة متخصصة بالتكنولوجيا المالية **FinTech**، وتوفير بيئات اختبار تنظيمية (Regulatory Sandboxes) تتيح لشركات التكنولوجيا المالية FinTech اختبار منتجاتها في بيئة رقابية مرنة وآمنة قبل اعتمادها الكامل (Al-Sharq, 2025).

ب. **تطوير البنية التحتية الرقمية:**

تشمل **الخطة الإستراتيجية الثالثة** أيضًا عدة مبادرات لتحسين البنية التحتية للسوق المالي والمصرفي، وتوسيع نطاق استخدام حلول الدفع الرقمية Digital Payments، وتنمية الكفاءات الوطنية في المجال الرقمي، بما يُعزز من القدرة التنافسية للقطاع المالي على المدى الطويل (QCB, 2024).

2. تنظيم عمل البنوك الرقمية:

أ. **إطار تنظيمي مرن لتحفيز الابتكار:**

اعتمد مصرف قطر المركزي QCB في ديسمبر 2024 إطارا تنظيميًا خاصًا بالبنوك الرقمية Digital Banks، يهدف إلى تمكين هذه المؤسسات المصرفية من تقديم خدماتها بالكامل عبر الإنترنت، وتعزز هذه الخطوة جهود الشمول المالي Financial Inclusion وتفتح المجال أمام دخول منافسين جدد للسوق (Jawan Partners, 2024).

ب. **ضمان الحماية الرقمية والرقابة المرحلية:**

يتكوّن هذا الإطار التنظيمي الخاص للبنوك الرقمية من مرحلتين تضمنان التدرج في استيفاء المعايير التنظيمية، مع فرض ضوابط صارمة في مجالات الأمن السيبراني Cyber Security وحماية البيانات، وتهدف هذه المراحل إلى ضمان تحقيق الابتكار دون تعريض النظام المالي للمخاطر (Jawan Partners, 2024).

3. بيئات الاختبار التنظيمية كأداة لتمكين الشركات الناشئة:

أ. بيئات الاختبار التنظيمية كمساحة تجريبية للابتكار:

تُعدّ بيئات الاختبار التنظيمية Regulatory Sandboxes التي أنشأها مصرف قطر المركزي QCB أداة حيوية لتسريع اعتماد التكنولوجيا المالية FinTech، فهذه البيئات تتيح للشركات والمؤسسات اختبار المنتجات الجديدة، مثل المحافظ الرقمية Digital Wallets ومنصات الذكاء الاصطناعي في بيئة خاضعة للرقابة (Al-Sharq,2025).

ب. خفض الحواجز أمام دخول السوق:

ومن جانب آخر تقلل هذه البيئة أيضا من التكلفة التنظيمية، وتمنح الشركات الناشئة فرصًا لتطوير منتجات قابلة للتوسع بسرعة، مع الالتزام بالمعايير الرقابية ذات الصلة، مما يعزز من ديناميكية النظام المصرفي القطري (Al-Sharq,2025).

4. الدمج بين التكنولوجيا المالية والتمويل الإسلامي والمستدام:

أ. حلول مبتكرة متوافقة مع الشريعة الإسلامية:

تدعم الأطر التنظيمية استخدام التكنولوجيا المالية FinTech في تطوير منتجات مالية متوافقة مع أحكام الشريعة الإسلامية، بما يشمل حلول التمويل الجماعي Crowdfunding، والمحافظ الاستثمارية الرقمية (MENA Fintech Association, 2024).

ب. دعم التمويل الأخضر والاستدامة:

تشجع السياسات التنظيمية لمصرف قطر المركزي QCB أيضًا الابتكار في مجالات التمويل الأخضر Green Financing، والإقراض المستدام Sustainable lending، من خلال توفير حوافز للمنتجات التي تراعي الاعتبارات البيئية والاجتماعية (GoGlobe, 2024).

5. مواءمة الابتكار مع المعايير الدولية:

أ. تطبيق معايير بازل 3:

تسعى الجهات التنظيمية في قطر، وعلى رأسها مصرف قطر المركزي QCB، إلى تعزيز الأطر الرقابية عبر تطبيق معايير بازل 3، لضمان كفاية رأس المال، وتقليل المخاطر التشغيلية، ومكافحة غسل الأموال، ما يضمن سلامة القطاع مع تمكين الابتكار (PwC, 2024).

6.الإشراف على استخدامات الذكاء الاصطناعي في القطاع المصرفي:

أ. إطار تنظيمي لاستخدام مسؤول وآمن:

أصدر مصرف قطر المركزي QCB تعليمات تنظم استخدام الذكاء الاصطناعي AI في العمليات المصرفية وتُلزم المؤسسات بإجراء تقييم للمخاطر، وضمان وجود إشراف بشري في القرارات الحساسة مثل تقييم الجدارة الائتمانية وكشف الاحتيال (QCB, 2024).

ب. حماية البيانات والامتثال التنظيمي:

تؤكد اللوائح التنظيمية لمصرف قطر المركزي على حماية البيانات، من خلال تشفيرها، وضمان الخصوصية، وربط أدوات الذكاء الاصطناعي بأنظمة الامتثال مثل KYC وAML، بهدف رفع كفاءة القطاع دون الإخلال بالأمان القانوني والرقابي (QCB, 2024).

7.التطورات التنظيمية والتوجهات المستقبلية:

يواصل مصرف قطر المركزي QCB تطوير منهجيته الرقابية لمواكبة التحولات المتسارعة في التكنولوجيا المالية، وخاصة الذكاء الاصطناعي، ويشمل هذا النهج ثلاث ركائز أساسية كالتالي (QCB, 2024):

أ. المشاورات العامة:

يعمل المصرف على إشراك الأطراف المعنية في عملية تطوير السياسات التنظيمية من خلال جلسات استماع ومشاورات مفتوحة، وذلك بهدف ضمان توافق اللوائح مع احتياجات السوق وتشجيع الابتكار المسؤول.

ب. بناء القدرات:

يتم الاستثمار في تأهيل الكوادر الرقابية والتقنية داخل الجهات التنظيمية والمؤسسات المالية، من خلال التدريب المستمر وبرامج التوعية الخاصة بالتقنيات الناشئة.

ج. التعاون الدولي:

يسعى مصرف قطر المركزي إلى مواءمة الأطر التنظيمية مع أفضل الممارسات والمعايير الدولية، مما يعزز من فرص التعاون مع الجهات المصرفية وشركات التكنولوجيا على المستوى الإقليمي والعالمي.

8.ضوابط صارمة لحماية البنية الرقمية:

تفرض لوائح مصرف قطر المركزي معايير متقدمة في الأمن السيبراني، تشمل حوكمة البيانات، وإجراء تقييمات دورية للمخاطر، والاستجابة للحوادث، بما يعزز من ثقة العملاء واستقرار المنظومة المالية (QCB, 2023).

ويلخص الجدول رقم (4) أدناه المفاهيم المختلفة التي تم مناقشتها في هذا الفصل من الدراسة، وينقسم هذا الجدول إلى قسمين كالتالي:

1. المفاهيم ذات الصلة بالمتغير المستقل (الذكاء الاصطناعي).
2. المفاهيم ذات الصلة بالمتغير **التابع** (إدارة مخاطر الجريمة المالية) والمتغيرات الفرعية منه.

جدول رقم (4) ملخص المفاهيم ذات الصلة بمتغيرات الدراسة

1.المفاهيم ذات الصلة بالمتغير المستقل (الذكاء الاصطناعي):

المصطلح	التعريف
الذكاء Intelligence	عرف Dearbom **الذكاء** بأنه: **القدرة على اكتساب الخبرة والإفادة منها** (إلياس، 2009)، كما عرف أيضا بأنه: **القدرة على حل المشكلات المألوفة وغير المألوفة من خلال توظيف المعارف والخبرات لمعالجة المواقف المختلفة التي يواجهها الأفراد** (العيتي، 2008)، كما عرف بكونه **قدرة الفرد وخبراته وتجاربه التراكمية، بالإضافة إلى معرفته ومعلوماته التي تقدم له المساعدة في حل المشكلات التي تواجهه** (المجاهد وآخرين، 2021)
الذكاء الاصطناعي Artificial Intelligence – AI	عرف Ming-Hwa Wang **الذكاء الاصطناعي (AI)** بأنه: **مجال الدراسة الذي يشمل التقنيات الحسابية لأداء المهام التي يقوم بها الإنسان وتتطلب الذكاء** (بوبعابة، وآخرون، 2021)، كما عرف **الذكاء الاصطناعي** بأنه: **التقنية التي تسهم في إدارة العمليات والمهام بآليات الأكثر تطورًا وذكاءً من الإنسان الذي صنعها ومنحها المعرفة والمقومات الحسية، بما يساعدها على التعلم التلقائي والتطور الذاتي** (الجابر، 2020)، كما يعرف بأنه: **قدرة حاسب أوروبوت مدعم بحاسب على معالجة المعلومات، والوصول إلى نتائج بطريقة مماثلة لعملية التفكير لدى البشر في التعلم، و اتخاذ القرارات وحل المشكلات، ومن ثمَّ فإن هدف أنظمة الذكاء الاصطناعي هو تطوير أنظمة قادرة على معالجة المشكلات المعقدة بطرق مشابهة للعمليات المنطقية والاستدلالية عند البشر** (سالمي وكمال، 2020).
النظم الخبيرة Expert Systems	عرف (الخوالدة 2020) **النظم الخبيرة (Expert Systems)** بأنها: **أنظمة متقدمة جدًا تستخدم أساليب الإنسان الخبير وتدمجها مع خصائص الآلة الذكية باستخدام المنطق والتحليل الرياضي لحل مشكلة أو أداء مهمة، ويتم ذلك كما لو أن النظام المستعمل لذلك الغرض خبير في المجال**، كما عرفت بكونها **برامج حاسوبية متطورة تحتوي المعرفة المرتبطة بحقل معين صممت خصيصًا لتقوم بعمل الخبراء البشريين في هذا الحقل، وتستخدم لأداء عدد كبير من الأعمال المعقدة والتي يمكن أن تؤدى بواسطة عدد من الخبراء المتخصصين، ويتم أداء هذه الأعمال عن طريق محاكاة عمل الخبير البشري الذي يستخدم المعرفة المرتبطة بمجال معين والقواعد العلمية المطلوبة للوصول إلى التوصية أو الاقتراح ومن ثمَّ اتخاذ القرار** (إسماعيل والمطيري، 2022).

المصطلح	التعريف
تعلم الآلة Machine Learning	يعرف تعلم الآلة **(Machine Learning)** بأنه: فرع من فروع الذكاء الاصطناعي يتضمن بناء نماذج حاسوبية قادرة على التعلم والقيام بتنبؤات أو اتخاذ قرارات مستقلة بناءً على البيانات المقدمة لها، وتعمل هذه النماذج على تحسين دقتها باستمرار من خلال البيانات المكتسبة (Kufel et al, 2023)، كما عرف بكونه دراسة الخوارزميات الحاسوبية التي تسمح لبرامج الحاسب الآلي بالتعلم تلقائيًا وتحسين أدائها من خلال الخبرة، كما أنه يعد مجالاً فرعيًا للذكاء الاصطناعي يوفر للأنظمة القدرة على التعلم تلقائيًا وتحسين الأداء من خلال الخبرة دون أن يتم برمجتها صراحةً (Shyam & Chakraborty, 2021).
التعلم العميق Deep Learning	عرف التعلم العميق **(Deep Learning)** بكونه التقنية التي تحاول تقليد ومحاكاة الطريقة التي يعمل بها العقل البشري في جميع قدراته، مثل الرؤية، وفهم الحديث وتكوينه، والسمع، وغيرها من القدرات القوية للعقل البشري، وذلك من خلال خوارزميات وبرامج مستوحاة من الدراسات الطبية والعصبية الخاصة بالإنسان وتحاول قدر الإمكان أن تقلدها ولكن بطرق حاسوبية لا بيولوجية، حيث يتم استبدال الخلايا العصبية في العقل البشري بالخلايا العصبية الاصطناعية (حسن، 2025)، كما عرف أيضًا بأنه: فرع من فروع تعلم الآلة يهدف لتطوير نموذج يطابق مستوى الدماغ البشري في حل المشكلات المعقدة في العالم الحقيقي من خلال الاستفادة من الشبكات العصبية الاصطناعية والتعلم المحاكي (Aggarwal et al, 2022).
معالجة اللغة الطبيعية Natural Language Processing (NLP)	تعرف (Xu et al, 2024) **معالجة اللغة الطبيعية (NLP)** على أنها التقنية التي تمكن أجهزة الحاسب الآلي من فهم وتفسير وتوليد اللغة البشرية، ومن ثم تعمل على سد الفجوة بين التواصل البشري وفهم الحاسب الآلي، مما يسهل من ثمَّ التفاعلات الأكثر طبيعية فيما بين البشر والآلات، كما عرفها كلا من (Jerfy, Selden & Balkrishnan , 2024) بأنها: فرع الذكاء الاصطناعي الذي يركز على التفاعل بين أجهزة الحاسب الآلي والبشر من خلال اللغة الطبيعية، وتنطوي على قدرة أجهزة الحاسب على فهم وتفسير وتوليد اللغة البشرية بطريقة ذات معنى ومفيدة، وتشمل مهام مختلفة مثل الترجمة الآلية وتحليل المشاعر واستخراج المعلومات من بين أمور أخرى، ويتمثل هدفها في تمكين الآلات من معالجة وتحليل كميات كبيرة من بيانات اللغة الطبيعية بشكل فعال، ومن ثمَّ تسهيل التواصل والتفاهم بشكل أفضل بين البشر وأجهزة الحاسب.
رؤية الحاسب Computer Vision	تعرف رؤية الحاسب **(Computer Vision)** بأنها: فرع الذكاء الاصطناعي الذي يسمح لأجهزة الحاسب باستخراج معلومات مفيدة من الصور الرقمية ومقاطع الفيديو وغيرها من المدخلات المرئية والتصرف أو تقديم توصيات بناءً على تلك المعلومات، ومن وجهة نظر هندسية، تهدف رؤية الحاسب إلى فهم و أتمتة العمليات التي يكون النظام البصري البشري قادرًا على القيام بها، ونتيجة لذلك يتعلق الأمر بالاستخراج الآلي وتحليل وفهم المعلومات ذات الصلة من صورة واحدة أو سلسلة من الصور (Krizhevsky, Sutskever & Hinton, 2023)، وعرفها (Che et al, 2024) بأنها: عملية محاكاة الملاحظة البصرية البشرية واستخدام أجهزة الحاسب لتحليل الصور، والتي تتطلب من الحاسب أن يكون لديه القدرة على إدراك البيئة المحيطة من خلال الصور ومحاكاة عملية الرؤية البشرية المحددة لتحقيق المعالجة الذكية للصور ذات الصلة.
الذكاء الاصطناعي التوليدي Generative AI	يشير مصطلح الذكاء الاصطناعي التوليدي **(Generative AI)** إلى تقنيات الحاسب الآلي القادرة على توليد محتوى جديد وذي مغزى، مثل النصوص أو الصور أو الأصوات، اعتماد على بيانات التدريب التي تدربت عليها مسبقا (Feuerriegel et al., 2024)، بالإضافة إلى ذلك تتيح الأنماط والأشكال المتنوعة للمحتوى الذي تم إنشاؤه من الذكاء الاصطناعي التوليدي **(Generative AI)** مجموعة واسعة من التطبيقات، مثل القصائد والبيانات السياسية والأوراق الأكاديمية (Hu، 2023)، والتي يكون من الصعب التمييز بينها وبين المحتوى الذي ينشئه البشر عادة (Nah et al, 2023).

المصطلح	التعريف
أتمتة العمليات الروبوتية Robots Process Automation	وفقا لـ (Hsiung & Wang, 2022) تعرف أتمتة العمليات الآلية **(Robots Process Automation)** بأنها: تقنية قائمة على البرمجيات تحاكي الإجراءات البشرية لتنفيذ عمليات و أنشطة الأعمال المتكررة القائمة على القواعد بواسطة التفاعل مع الأنظمة الرقمية من خلال واجهات المستخدم الخاصة بهم، تمامًا كما يفعل المستخدم البشر. كما عرفت أتمتة العمليات الآلية **(RPA)** أيضا بكونها التقنية التي تتيح للمؤسسات أتمتة المهام الرتيبة المتكررة والقائمة على القواعد من خلال محاكاة تصرفات المستخدم البشري، ومن ثمَّ تحرير وتفريغ الموارد البشرية للقيام بالأنشطة الإستراتيجية والأعلى قيمة. (Bhardwaj, 2023).

2.المفاهيم ذات الصلة بالمتغير التابع (إدارة مخاطر الجريمة المالية) والمتغيرات الفرعية:

المصطلح	التعريف
الخطر / المخاطر Risk / Risks	الخطر **(Risk)** هو النتيجة غير المتوقعة وغير المرغوب فيها التي تحدث بسبب عوامل مختلفة، ودائما ما يكون اتجاه الخطر معاكسا لاتجاه الهدف الذي يجب تحقيقه، أما "المخاطر"، فهي تُشير إلى احتمالية وقوع ذلك الخطر أو الحدث غير المرغوب فيه، وما يترتب عليه من عواقب سلبية، بمعنى آخر: المخاطر هي تقدير لمدى احتمالية وقوع الخطر وحجم الضرر الذي قد يسببه (Sleimi, 2020)، وبالنسبة للمنظمات **تعرف المخاطر (Risks)**على أنها: تأثير أي حالة من عدم اليقين على أهداف المنظمة أو عواقب بعض الأحداث سواء من داخل المنظمة أو خارجها (Azuma-Kotei & Ibrahim, 2024).
إدارة المخاطر Risk Management	عرف (المغربي، 2020) إدارة المخاطر **(Risk Management)** بكونها نظام متكامل وشامل لتهيئة البيئة المناسبة، والأدوات اللازمة لتوقع ودراسة المخاطر المحتملة وتحديدها وقياسها وتحديد مقدار آثارها المحتملة على أعمال المنظمة، وأصولها و إيراداتها ووضع الخطط المناسبة لما يلزم وما يمكن القيام به لتجنب هذه المخاطر أو لكبحها والسيطرة عليها وضبطها للتخفيف من آثارها إن لم يكن القضاء على مصادرها، كما عرف (النسور وبقيلة،2022) إدارة المخاطر **(Risk Management)** في المؤسسات المصرفية بأنها: عملية تقييم للمخاطر التي تواجه المؤسسات المصرفية والعمل على تطوير إستراتيجيات معاصرة لأجل إدارتها، تحتوي على تجنب هذه المخاطر والحد منها قدر الإمكان.
تحديد المخاطر Risk Identification	يقصد بتحديد المخاطر **(Risk Identification)** عملية بدء الإجراءات وخلق الوعي ووجهة النظر المشتركة والالتزامات، وكذلك توضيح التوقعات فيما يتعلق بالمخاطر، ويمكن تحقيق ذلك من خلال وضع قواعد لتحديد المخاطر، أو التي تحاول تحديد مخاطر محددة من خلال عوامل الخطر (Sleimi, 2020)، كما عرفها (Kountar & Sari, 2023) بأنها: عملية اكتشاف المخاطر التي قد تؤثر على أهداف أو أغراض المنظمة، وهي خطوة أولى بالغة الأهمية في عملية إدارة المخاطر، حيث إنها تسمح للمنظمات بالتعرف على التهديدات المحتملة قبل أن تؤثر على العمليات، وتتضمن تحديد المخاطر وتوثيقها بشكل منهجي لضمان إمكانية إدارتها والتخفيف منها بشكل فعال.
تحليل و تقييم مستوى المخاطر Risk Analysis & Evaluation	يقصد بتحليل وتقييم مستوى المخاطر **(Risk Analysis and Evaluation)** عملية تحليل المخاطر التي تم تحديدها؛ وذلك من أجل فهم تأثيرها المحتمل على المنظمة واحتمالية حدوثها، ويتضمن ذلك تقييمات كمية ونوعية لقياس مدى تأثير هذه المخاطر على أداء المنظمة، ثم مقارنة هذه المخاطر المقدرة بمعايير المخاطر لتحديد أهميتها، ومن ثم تحديد أولويات المخاطر بناءً على تأثيرها المحتمل على أهداف المنظمة Bao et al (2024).

المصطلح	التعريف
معالجة وتخفيف المخاطر Risk Mitigation	يقصد بمعالجة وتخفيف المخاطر **(Risk Mitigation)** مرحلة ممارسة السيطرة على المخاطر؛ وهذه هي المرحلة التي يتم فيها وضع إستراتيجيات الحد من المخاطر ومعالجتها موضع التنفيذ بهدف تقليل شدة المخاطر وتأثيراتها وعواقبها إلى مستوى مقبول (Khinvasara & Tzenios, 2023).
مراقبة ومراجعة المخاطر Risk Monitoring & Review	ويطلق عليها أحيانا متابعة ومراجعة المخاطر **(Risk Monitoring & Review)**، ويقصد بها التتبع والتقييم المستمر للمخاطر، فضلاً عن ضمان فاعلية إجراءات وتدابير معالجة المخاطر، لضمان أن تظل إستراتيجية إدارة المخاطر في المنظمة ذات صلة وحديثة وتحديد مجالات التحسين (Efe, 2023).
الجريمة المالية Financial Crime	عرف (Brici, 2022) الجريمة المالية **(Financial Crime)** بأنها: كل أشكال الجرائم غير العنيفة التي تسبب خسارة مالية، بينما عرفتها الشرطة الدولية (الإنتربول - **Interpol**) بكونها كل فعل مجرم قانونًا ينطوي على أو يترتب عليه الاستلاء على مال الغير، أو ينطوي على التصرف في الأموال أو تحريكها على نحو مخالف للقانون (Interpol, 2020).

المصدر: من إعداد الباحث بناء على مصادر الدراسة

الفصل الثالث

منهجية و نتائج الدراسة الميدانية

- مقدمة
- منهجية الدراسة و إجراءاتها:
  - الهدف من الدراسة الميدانية
  - منهج الدراسة
  - مصادر بيانات الدراسة
  - مجتمع وعينة الدراسة وأداة القياس
  - قياس صلاحية أداة جمع البيانات
- عرض البيانات و تحليلها:
  - عرض نتائج البيانات لعينة الدراسة و تحليلها
  - عرض و تحليل نتائج متغيرات الدراسة
- اختبار فروض الدراسة:
  - التوزيع الطبيعي لمتغيرات الدراسة
  - اختبار فروض الدراسة

الفصل الثالث
منهجية ونتائج الدراسة الميدانية

مقدمة:

يقدّم هذا الفصل **الإطار المنهجي والتطبيقي للدراسة** بوصفه **ركيزة أساسية لفهم بنيتها العلمية ونتائجها الميدانية**؛ إذ يبدأ بعرض **المنهجية العلمية** التي اعتمد عليها الباحث، من خلال تحديد **نوع المنهج المستخدم وأسباب اختياره**، إضافة إلى تحديد **مصادر البيانات ومجتمع الدراسة** بدقة، ووصف **الخصائص الديموغرافية لعينة الدراسة**. كما يستعرض الفصل **إجراءات بناء أداة الدراسة (الاستبانة)** وخطوات التحقق من **صدقها وثباتها** باستخدام **الأساليب العلمية الملائمة**. وفي سياق متصل، يُشكّل هذا الفصل **الجانب التطبيقي للدراسة** عبر عرض **البيانات الميدانية** التي جُمعت وتحليلها بغرض الإجابة عن **تساؤلات الدراسة واختبار فروضها**، بما ينسجم مع **الإطار النظري والمنهجي المعتمد**. وقد استند التحليل إلى **المنهج التحليلي**، وذلك بعد توظيف **المنهج الوصفي** في تناول **الجوانب النظرية** وتحديد **المتغيرات الرئيسة للعلاقة بين الذكاء الاصطناعي وإدارة مخاطر الجرائم المالية في القطاع المصرفي**. ويتضمن هذا الفصل - لاحقا - عرضًا منهجيًا شاملاً **للنتائج** المستخلصة من **الاستبانة** التي وُزّعت على **عينة الدراسة**، مع **تحليل البيانات** باستخدام **برنامج SPSS** وتطبيق أدوات التحليل الإحصائي المناسبة، مثل: **التكرارات**، و**النسب المئوية**، و**المتوسطات الحسابية**، و**الانحرافات المعيارية**. ويلي ذلك عرض **البيانات الشخصية للمستجيبين** باعتبارها **مدخلًا لفهم خصائص العينة**، و ينتقل هذا الفصل بعدها إلى مناقشة **استجاباتهم** حول **متغيرات الدراسة** الرئيسة، وهي **الذكاء الاصطناعي كمتغير مستقل**، و**إدارة مخاطر الجريمة المالية كمتغير تابع بأبعاده الفرعية**. ويعتمد **التحليل الوصفي** لاستكشاف **الاتجاهات العامة** وتحديد **مستويات تقييم أفراد العينة** لهذه الأبعاد، تمهيدًا لاشتقاق **مؤشرات كمية** تفسّر **العلاقة** بين **الذكاء الاصطناعي** و**كفاءة إدارة مخاطر الجريمة المالية**. وفي ضوء ذلك، يسعى الفصل إلى الوصول إلى **استنتاجات مدعومة بالأدلة الإحصائية** تُعزّز فهم **أدوار** و**تطبيقات الذكاء الاصطناعي** في **تحسين إدارة مخاطر الجريمة المالية** في **مؤسسات القطاع المصرفي**، وذلك من خلال مناقشة العناصر التي يتضمنها هذا الفصل بصورة مترابطة ومتسلسلة. وسيقوم الباحث بتحقيق أهداف هذا الفصل من خلال مناقشة العناصر التالية:

أولاً: منهجية الدراسة و إجراءاتها:

- الهدف من الدراسة
- منهج الدراسة
- مصادر بيانات الدراسة
- مجتمع وعينة البحث و أداة الدراسة
- قياس صلاحية أداة جمع البيانات

ثانيا: عرض البيانات و تحليلها:

- عرض نتائج البيانات لعينة الدراسة و تحليلها
- عرض و تحليل نتائج متغيرات الدراسة

ثالثا: اختبار فروض الدراسة:

- التوزيع الطبيعي لمتغيرات الدراسة
- اختبار فروض الدراسة

أولا: منهجية الدراسة وإجراءاتها:

1.الهدف من الدراسة الميدانية:

تهدف الدراسة الميدانية إلى **تحديد دور تأثير المتغير المستقل**، والمتمثل في **الذكاء الاصطناعي**، على **المتغير التابع** وهو **إدارة مخاطر الجرائم المالية**، وذلك من خلال **تحليل و اقع توظيف تقنيات الذكاء الاصطناعي في الكشف المبكر عن الأنماط غير الاعتيادية في المعاملات والعمليات المالية والمصرفية في مؤسسات القطاع المصرفي القطري**، **وو اقع استخدامها في تعزيز قدرات التنبؤ بالمخاطر المالية المحتملة**، وإضافة إلى ذلك تهدف الدراسة الميدانية أيضا إلى **تقديم مجموعة من المقترحات العملية** التي **تسهم في تطوير إستراتيجيات أكثر كفاءة لإدارة مخاطر الجرائم المالية بمؤسسات القطاع المصرفي القطري**، بما **ينسجم مع التوجهات الوطنية نحو التحول الرقمي**، وتحقيق **متطلبات الامتثال للمعايير الدولية في مكافحة الجرائم المالية**.

2. منهج الدراسة:

بالنظر الى طبيعة موضوع الدراسة، ومن أجل الإجابة عن مشكلتها الرئيسية والتساؤلات الفرعية المنبثقة عنها، ولتحقيق أهدافها واختبار فروضها، ونظرا للجوانب العديدة التي تحتويها، فقد اعتمد الباحث في هذه الدراسة بشكل أساسي على **منهجين متكاملين**، هما: **المنهج الوصفي والمنهج التحليلي**؛ ففي **شقها النظري**، ومن أجل بلورة الإطار الفكري والسياق النظري لموضوع الدراسة، وتوصيف متغيراتها (**الذكاء الاصطناعي**، و**إدارة مخاطر الجرائم المالية**)، وتوضيح علاقاتها وخصائصها، اعتمدت الدراسة على **المنهج الوصفي**؛ **لكونه المنهج المناسب لوصف واستعراض الإطار النظري لها**، وقد تمثل ذلك في الدراسة المكتبية من خلال مسح المصادر الرئيسية من الأدبيات النظرية الحديثة ذات الصلة بموضوع الدراسة ومتغيراتها المختلفة، كما تضمن ذلك أيضا الاطلاع على بحوث تطبيقية ودراسات ميدانية سابقة لجمع الحقائق والبيانات عن الذكاء الاصطناعي وتطبيقاته المختلفة، وروابط الصلة بينه وبين إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي، مع محاولة تفسير تأثير هذه الروابط تفسيرا وافيًا.

أما في **الجانب العملي التطبيقي** للدراسة، فقد تم الاعتماد على **المنهج التحليلي**؛ من أجل **تحليل المعلومات والبيانات التي تم جمعها باعتماد أسلوب الدراسة الميدانية**، من خلال **توزيع أداة الاستبانة** كأداة لجمع العينة المستهدفة، وتحليلها باستخدام الأدوات الاحصائية بالاستعانة **ببرنامج** (**SPSS**).

3.مصادر بيانات الدراسة:

فيما يتعلق **بمصادر البيانات**، فقد تم الحصول عليها من **مصدرين**، هما:

أ. البيانات الثانوية:

اتجه الباحث في معالجة الإطار النظري للدراسة إلى مصادر البيانات الثانوية ذات الصلة بأبعاد الذكاء الاصطناعي وإدارة مخاطر الجريمة المالية، وتتمثل هذه المصادر في الكتب والمراجع العربية والأجنبية ذات العلاقة، والدوريات والمقالات والتقارير، والأبحاث والدراسات السابقة التي تناولت موضوع الدارسة، والبحث والمطالعة في مواقع الإنترنت المختلفة، بالإضافة إلى ذلك تشمل هذه المصادر أيضا البيانات والمعلومات ذات الصلة بموضوع الدراسة التي تم الحصول عليها من خلال النشرات والإحصائيات والتقارير الصادرة عن الجهات المختصة الدولية والإقليمية والمحلية.

ب. البيانات الأولية:

اعتمد الباحث عند جمع البيانات الأولية اللازمة للدراسة على تصميم استمارة استبانة وزعت على عينة عشوائية من العاملين في مؤسسات القطاع المصرفي القطري، وتحوي هذه الاستمارة العناصر الأساسية والفرعية المطلوب تغطيتها لاختبار فروض الدراسة وتحقيق أهدافها، وقد روعي فيها عدم ذكر اسم المستقصى منه بهدف توفير الاطمئنان للإجابة عن الأسئلة بمصداقية، كما روعي

أيضا ترتيب الأسئلة ترتيبًا منطقيًا مترابطا، في محاولة لمعرفة آراء عينة الدراسة حول تأثير استخدام تطبيقات الذكاء الاصطناعي على إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

4. مجتمع وعينة الدراسة وأداة القياس:

أ. مجتمع وعينة الدراسة:

يقصد بمجتمع الدراسة المجموعة الكلية من العناصر التي تسعى الدراسة إلى أن يعمم عليها النتائج ذات العلاقة بالمشكلة المدروسة، ويتمثل مجتمع الدراسة في العاملين بمؤسسات القطاع المصرفي القطري الخاضعة لإشراف مصرف قطر المركزي في مختلف الإدارات والأقسام ذات الصلة بموضوع الدراسة، وهي: (**إدارة الامتثال / الالتزام، إدارة المخاطر، إدارة مكافحة الجرائم المالية، إدارة التدقيق الداخلي، إدارة الأمن السيبراني**)، وقد اعتمد الباحث على أسلوب العينة العشوائية في دراسة مفردات مجتمع الدراسة؛ نظرا لكبر عدد العاملين في هذا القطاع محل الدراسة والذي يقدر بحوالي **1017** موظفًا تقريبًا، وفقا لما هو مبين في **الجدول رقم (5)**:

جدول رقم (5) عدد العاملين في الإدارات ذات الصلة بموضوع الدراسة في كل بنك / مصرف في القطاع المصرفي القطري

م	المصرف / البنك	عدد الفروع	عدد العاملين في جميع الإدارات ذات الصلة
-1	بنك قطر الوطني	35	188
-2	البنك التجاري	28	143
-3	بنك الدوحة	14	176
-4	البنك الأهلي	12	79
-5	بنك قطر للتنمية	3	33
-6	مصرف قطر الإسلامي	21	110
-7	بنك قطر الدولي الإسلامي	17	71
-8	بنك دخان	9	76
-9	مصرف الريان	13	104
-10	البنك العربي المحدود	2	8
-11	بنك المشرق	1	5
-12	بنك ستاندرد تشارترد	1	5
-13	بنك اتش اس بى سى الشرق الاوسط	2	6
-14	بنك يونايتد المحدود	1	5
-15	بنك صادرات إيران	2	3
-16	بنك بي أن بي باريبا	1	5
	الإجمالي		1017

المصدر: من إعداد الباحث بالاعتماد على بيانات البنك / المصرف محل الدراسة

أما عينة البحث فقد تم اختيارها بطريقة عشوائية من العاملين بالإدارات والوظائف ذات الصلة بموضوع الدراسة في مؤسسات القطاع المصرفي القطري، وتم تحديد حجم العينة عند **معامل ثقة 95%**، **وحدود خطأ 5%**، بـ **278** مفردة من الجداول الإحصائية، حيث كان **حجم المجتمع 1017مفردة تقريبًا** كما تم توضيحه مسبقا، وقد تم الحصول علي **270 استمارة صالحة للتحليل**، أي **بنسبة استجابة 97%**، ويمكن توزيع عينة البحث كما هو موضح في **الجدول رقم (6)** على النحو التالي:

جدول رقم (6) توزيع حجم عينة العاملين بمؤسسات القطاع المصرفي محل الدراسة

م	المصرف / البنك	حجم عينة العاملين في الإدارات ذات الصلة	النسبة المئوية
-1	بنك قطر الوطني	52	18.705
-2	البنك التجاري	38	14.029
-3	بنك الدوحة	46	17.266
-4	البنك الأهلي	22	7.914
-5	بنك قطر للتنمية	9	3.237
-6	مصرف قطر الإسلامي	28	10.791
-7	بنك قطر الدولي الإسلامي	18	6.835
-8	بنك دخان	22	7.554
-9	مصرف الريان	26	9.712
-10	البنك العربي المحدود	2	0.719
-11	بنك المشرق	1	0.360
-12	بنك ستاندرد تشارترد	1	0.360
-13	بنك اتش اس بى سى الشرق الاوسط	2	0.719
-14	بنك يونايتد المحدود	1	0.360
-15	بنك صادرات إيران	1	0.360
-16	بنك بي أن بي باريبا	1	0.360
	الإجمالي	270	%100

المصدر: من إعداد الباحث

وبناء علي ذلك سوف يتم التعامل مع هذه القائمة كما لو كان الباحث قد اعتمد علي أسلوب العينات لجمع البيانات الأولية لهذا البحث، ومن ثمَّ سوف يتم الاعتماد على الأساليب الإحصائية المناسبة لهذا الأسلوب.

ب. تصميم استمارة الاستبانة:

تم تصميم استمارة استبانة لجمع البيانات الأولية من مفردات مجتمع البحث وذلك بعد مراجعة الدراسات السابقة؛ من أجل الوصول إلى مقاييس أبعاد البحث، وقد تضمنت استمارة الاستبانة **(43) عبارة**، منها **(15) عبارة لقياس المتغير المستقل**، و**(28) عبارة لقياس المتغير التابع**، وكانت الأسئلة الواردة باستمارة الاستبانة والعبارات على النحو التالي:

1. لقياس المتغير المستقل (**الذكاء الاصطناعي**) تم وضع الجزء الثاني والذي يحتوي على **15 عبارة** استخدمت لقياس (**الذكاء الاصطناعي**).

2. لقياس المتغير التابع (**إدارة مخاطر الجريمة المالية**) تم وضع الجزء الثالث والذي يحتوي على **28 عبارة** استخدمت لقياس (**إدارة مخاطر الجريمة المالية**).

وبصورة أكثر تفصيلاً يوضح الجدول رقم (7) متغيرات البحث وعناصر قياسها ورموز أسئلتها التي تعكسها قائمة الاستقصاء.

جدول رقم (7) متغيرات البحث وعناصر قياسها ورموز أسئلتها

المتغيرات	الأبعاد	الرمز	عدد الأسئلة
(المتغير المستقل) الذكاء الاصطناعي		**X**	**من)1-10)**
(المتغير التابع) إدارة مخاطر الجريمة المالية	تحديد مخاطر الجريمة المالية	**Y1**	**من) 1-7)**
	تحليل وتقييم مخاطر الجريمة المالية	**Y2**	**من) 8-14)**
	معالجة مخاطر الجريمة المالية	**Y3**	**من) 15-21)**
	مراقبة ومراجعة مخاطر الجريمة المالية	**Y4**	**من) 22-28)**

المصدر: من إعداد الباحث

وقد تم **قياس استجابات أفراد العينة لفقرات المقياس**، طبقا **لمقياس ليكرت الخماسي** كما هو موضح في **الجدول رقم (8)**:

جدول رقم (8) درجات مقياس ليكرت

أو افق تماما	أو افق	محايد	غير مو افق	غير مو افق تماما
5	**4**	**3**	**2**	**1**

المصدر: من إعداد الباحث بناء على مصادر الدراسة

وقد تم حساب مستوى الأهمية وفقًا للمعادلة التالية:

- **مستوى الأهمية** = (الحد الأعلى للإجابة – الحد الأدنى للإجابة) ÷ الحد الأعلى للإجابة.
- **مستوى الأهمية = (5 -1) ÷ 5 = 0.80**، كما هو موضح في **الجدول رقم (9)**.

جدول رقم (9) مستوى الأهمية لأبعاد الدراسة

المتوسط المرجح	مستوى الأهمية
أقل من 1.80	**ضعيفة جدا**
من 1.80 إلى أقل 2.60	**ضعيفة**
من 2.60 إلى أقل 3.40	**متوسطة**
من 3.40 إلى أقل 4.20	**مرتفعة**
من 4.20 إلى 5	**مرتفعة جدا**

المصدر: من إعداد الباحث بناء على مصادر الدراسة

5. قياس صلاحية أداة جمع البيانات:

تُعدّ أداة جمع البيانات (استمارة الاستبانة) ضرورية لأي دراسة، وتحتاج هذه الأداة لكي تؤدي الغرض منها إلى عاملين أساسيين لا بد من توافرهما في أداة جمع البيانات، ألا وهما: (**الصدق والثبات**)، وكلاهما يكتسب أهمية خاصة في البحوث الإنسانية؛ لأن القياس في هذه المجالات قياس غير مباشر؛ لذا يجب التأكد من أن ما تقيسه أدوات البحث يمكن الوثوق به والاعتماد عليه (بو علام، 2001)؛ ولذلك، يتعين التأكد أولاً من أن هذه الأداة صالحة للقياس، وشاملة لغرض جمع البيانات المطلوبة، وثانيًا التأكد من صلاحيتها لقياس ما أعدت بغرض قياسه بحيث يمكن الاعتماد على النتائج التي يتم التوصل إليها من خلال جمع تلك البيانات، وهذا يتضمن صدق وثبات فقرات الاستبانة.

أ. **قياس صدق وثبات استمارة الاستبانة:**

قبل إجراء عملية توزيع الاستبانة على المبحوثين قام الباحث بتوزيعها على عينة استطلاعية مكونة من **(20)** مفردة، وذلك من أجل قياس صدق وثبات استمارة الاستبانة، والتأكد من صلاحيتها في قياس ما أعدت لقياسه بصورة نهائية، وكذلك التمهيد لعملية توزيعها وجمعها من عينة الدراسة، وكانت النتائج كما يلي:

1. **قياس ثبات فقرات استمارة الاستبانة:**

يقصد بثبات الاستبانة أن تعطي هذا الاستبانة النتيجة نفسها لو تم إعادة توزيعها أكثر من مرة تحت الظروف نفسها والشروط نفسها، أو بعبارة أخرى أن ثبات الاستبانة يعني الاستقرار في نتائج الاستبانة وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

يقيس اختبار كرونباخ ألفا مدى ثبات أبعاد العناصر الداخلة في الاستبانة، ويقدم تقديرًا لقوة العلاقة بين هذه العناصر، وتتراوح قيمة كرونباخ ألفا بين 0 و1، حيث تشير قيمة أعلى من **0.6** إلى ثبات الاستبانة، ويمكن تقييم مدى جودة الاستبانة من خلال تفسير قيم معامل ألفا كرونباخ كما يلي:

- إذا كانت القيمة أعلى من **0.90**: فإن ذلك يُشير إلى **موثوقية عالية جدًا**.
- إذا كانت القيمة بين **0.80** و**0.90**: فإن ذلك يُشير إلى **موثوقية عالية**.
- إذا كانت القيمة بين **0.70** و**0.80**: فإن ذلك يُشير إلى **موثوقية جيدة**.
- إذا كانت القيمة بين **0.60** و**0.70**: فإن ذلك يُشير إلى **موثوقية مقبولة**.

جدول رقم (10) قيم معامل الثبات (طريقة ألفا كرونباخ) لأبعاد الدراسة

م	محاور و أبعاد الدراسة	عدد الفقرات	معامل ألفا كرونباخ	درجة الموثوقية
أ	**المتغير المستقل الأول (الذكاء الاصطناعي)**	**15**	**.967**	**موثوقية عالية**
ب	**المحور الثاني: المتغير التابع (إدارة مخاطر الجرائم المالية)**	**28**	**.845**	**موثوقية عالية**
1	تحديد مخاطر الجريمة المالية	7	.885	موثوقية عالية
2	تحليل وتقييم مخاطر الجريمة المالية	7	.878	موثوقية عالية
3	معالجة مخاطر الجريمة المالية	7	.945	موثوقية عالية
4	مراقبة ومراجعة مخاطر الجريمة المالية	7	.942	موثوقية عالية
	جميع الفقرات	**28**	**.956**	**موثوقية عالية**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

ويتضح من الجدول رقم (10):

- أن قيمة معامل ألفا كرونباخ (معامل الثبات لأبعاد المتغير المستقل الذكاء الاصطناعي) هي: (.967)
- وأن معامل ألفا كرونباخ (معامل الثبات لأبعاد المتغير التابع إدارة مخاطر الجرائم المالية) هو: (.845).
- وأن قيمة معامل ألفا كرونباخ (معامل الثبات الكلي لجميع فقرات أداة الدراسة) هو: (.956)
- وأن جميع قيم معامل الثبات على مستوى المتغيرات والأبعاد والفقرات، وكذا على المستوى الكلي موجبة، وتحديدًا قيمة معامل الثبات الكلي على مستوى الأداة ككل قوية، وتشير إلى درجة موثوقية عالية، وهذا يدل على أن **الاستبانة تتمتع بدرجة عالية من الثبات، تطمئن الباحث إلى تطبيقها على عينة الدراسة.**

2. قياس صدق استمارة الاستبانة:

ويقصد بصدق الأداة أن المقياس يقيس ما وضع لقياسه، أي يقيس الظاهرة ذاتها التي وضع من أجل قياسها، ولا يقيس غيرها، أو يقيس ظاهرة أو سمة أخرى معها (الضحيان، 2002)، ويعني صدق الاستبانة التأكد من أنها تقيس ما أُعدت لقياسه، كما يقصد به شمول الاستبانة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها، ومفرداتها من ناحية أخرى، بحيث تكون مفهومة لكل من يستخدمها، وقد قام الباحث بالتأكد من صدق أداة الدراسة، وذلك على النحو التالي:

أولاً: الصدق الظاهري:

يقصد **بالصدق الظاهري (Face Validity)** مدى صلاحية أداة جمع البيانات في الظاهر لقياس ما يفترض بها قياسه، بمعنى آخر: هو تقييم سطحي وسهل لأداة جمع البيانات لتحديد ما إذا كانت تبدو ذات صلة بالمفهوم الذي تحاول قياسه، وفي هذا الصدد قام الباحث بالإجراءات التالية:

1. بعد أن تم الانتهاء من إعداد الاستبانة بصورتها الأولية تم عرضها على الأستاذ الدكتور/ محمد شريف، المشرف على الرسالة، والذي أبدى بعض الملاحظات والمقترحات حولها، ثم قام الباحث بالتعديل بناء على تلك الملاحظات والمقترحات.
2. بعد الموافقة على الاستبانة بصورتها النهائية الأولية من قبل **الأستاذ الدكتور/ محمد شريف**، المشرف على الرسالة، تم عرضها على عدد من الخبراء والمختصين في الإحصاء ومناهج البحث، والمتخصصين في مجال الإدارة (المحكمين)، وتم أخذ آراءهم وملاحظاتهم، ومن ثم تم تعديل الاستبانة وفقًا لتلك الآراء والملاحظات.
3. بعد إجراء التعديلات اللازمة على الاستبانة وفقًا لآراء وملاحظات ومقترحات المحكمين، أصبحت الاستبانة بالصورة النهائية وفقًا لأبعادها التي اشتملت على (43) فقرة.

ثانيًا: الصدق الداخلي:

يعني الصدق الداخلي (Internal Validity): مقياس مدى قدرة أداة جمع البيانات على إثبات أن النتائج التي حصلت عليها تعود إلى المتغيرات المستقلة التي تمت دراستها، وليس إلى عوامل خارجية أو متغيرات أخرى غير مدروسة، بعبارة أخرى: يشير الصدق الداخلي إلى قدرة الأداة على إثبات العلاقة السببية بين المتغيرات.

وفي هذا الصدد قام الباحث بإجراء اختبار معامل الصدق الداخلي **Internal Validity Factor**، وهو أحد مقاييس صدق الأداة، والذي يستخدم للتحقق من درجة ارتباط كل بُعد من أبعاد الدراسة بالدرجة الكلية لعبارات الأبعاد، وجاءت النتائج كما هو موضح في **الجدول رقم (11)**:

جدول رقم (11) قيم معامل الصدق الداخلي بين فقرات أبعاد الدراسة

م	متغيرات الدراسة	العنوان	عدد الفقرات	قيمة الارتباط	مستوى المعنوية
أ	المتغير المستقل الأول	المتغير المستقل (الذكاء الاصطناعي)	15	.983	0.01
ب	المتغير التابع	المتغير التابع (إدارة مخاطر الجرائم المالية)	28	.919	0.01
1	البُعد الأول	تحديد مخاطر الجريمة المالية	7	.941	0.01
2	البُعد الثاني	تحليل وتقييم مخاطر الجريمة المالية	7	.937	0.01
3	البُعد الثالث	معالجة مخاطر الجريمة المالية	7	.972	0.01
4	البُعد الرابع	مراقبة ومراجعة مخاطر الجريمة المالية	7	.963	0.01

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

من **الجدول رقم (11)** يتضح أن **قيم معامل الصدق الداخلي** بين فقرات أبعاد **المتغير المستقل (الذكاء الاصطناعي)**، **والمعدل الكلي** لفقرات هذا المتغير **دالة عند مستوى دلالة (0.01)**، حيث إن **جميع فقرات الاستبانة الخاصة بهذا المتغير** قد جاءت **مرتبطة بأبعادها بدرجة ارتباط موجبة وقوية، وذات دلالة إحصائية** تتراوح بين **(**937.)** و**(**972.)**، وهي دالة عند مستوى دلالة **(0.01)** بشكل عام؛ مما يشير إلى أن **الاستبانة صادقة لما وضعت لقياسه**، كما يتضح أن **قيم معامل الصدق الداخلي** بين فقرات أبعاد **المتغير التابع (إدارة مخاطر الجرائم المالية)** ذات **دلالة إحصائية** بقيمة **(**919.)**، وهي دالة عند مستوى دلالة **(0.01)** بشكل عام؛ مما يشير إلى أن **الاستبانة صادقة لما وضعت لقياسه.**

ثانيا: عرض البيانات وتحليلها:

1. عرض نتائج البيانات لعينة الدراسة وتحليلها:

يتضمن هذا الجزء عرض نتائج الدراسة الميدانية وتحليلها ومناقشتها وفقًا لمتغيرات الدراسة وتسلسل محاور أداة الاستبانة المقدمة لأفراد عينة الدراسة، وقد تمثلت البيانات الشخصية لعينة الدراسة في: (**العمر، النوع، العلاقة بالخدمة، العلاقة بالعينة**)، ولمعرفة وصف أو خصائص أفراد العينة، فقد تم استخدام التكرارات والنسب المئوية لكل متغير، ونتائج الجداول التالية توضح ذلك كما يلي:

أ. **النوع:**

لمعرفة النوع لأفراد عينة الدراسة فقد تم سؤالهم عن النوع، وتم إعطاؤهم الخيارات أدناه، وجاءت إجاباتهم موزعة كما هو مبين في **الجدول رقم (12)** أدناه.

جدول رقم (12) توزيع أفراد عينة الدراسة وفق متغير النوع

النوع	التكرار	النسبة
ذكر	186	68.89
أنثى	84	31.11
الإجمالي	270	%100

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (12)** أن أعلى نسبة من أفراد العينة هم أصحاب النوع (**ذكر**) بنسبة (**68.89%**)، ويأتي أصحاب النوع (**أنثى**) بنسبة (**31.11%**) في المرتبة الأخيرة، **وتتفق هذه النتيجة** مع الإحصاءات الرسمية المنشورة بواسطة جهاز التخطيط والإحصاء القطري، والتي تشير إلى أن عدد العاملين من الذكور في مؤسسات القطاع المصرفي القطري يبلغ ضعف عدد العاملين من الإناث (National Planning Committee, 2025).

ب. العمر:

لمعرفة مستوى العمر لأفراد عينة الدراسة فقد تم سؤالهم عن أعمارهم، وتم إعطاؤهم الخيارات أدناه، وجاءت إجاباتهم موزعة كما في هو مبين في **الجدول رقم (13):**

جدول رقم (13) توزيع أفراد عينة الدراسة وفق متغير العمر

العمر	التكرار	النسبة
35- 26	**35**	**12.96**
45-36	**151**	**55.93**
55-46	**77**	**28.52**
55 فأكثر	**7**	**2.59**
الإجمالي	**270**	**%100**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (13)** أعلاه أن أعلى نسبة من أفراد العينة هم فئة العمر **36-45 عاما** بنسبة **(55.93%)**، بينما جاءت فئة العمر **55 فأكثر** بنسبة (**2.59%**) في المرتبة الأخيرة. **ويرى الباحث** أن هذه النتيجة تتفق مع الواقع العملي في مؤسسات القطاع المصرفي القطري والذي يشهد زيادة عدد العاملين فيه من هذه الفئة السنية عن باقي الفئات السنية، حيث يتم استهداف الأفراد فئة العمر **36-45 عاما** في القطاع المصرفي القطري لعدة أسباب، منها: خبرتهم وكفاءتهم العالية، حيث يتمتع الأفراد في هذه الفئة بقدرة على تحقيق الإنتاجية العالية والاستقرار الوظيفي، كما تعكس هذه النسبة التوجهات الاقتصادية التي تفضل استقطاب الكفاءات المؤهلة، بالإضافة إلى استثمار المؤسسات في تدريب وتطوير هذه الفئة، بالمقابل تعد نسبة العاملين في الفئات الأكبر سنًا (**عاما 55 فأكثر**) منخفضة؛ بسبب التوجه نحو التقاعد وقلة الحاجة للأيدي العاملة الأكبر سنًا في ظل التطورات التكنولوجية.

ج. المؤهل الدراسي:

لمعرفة مستوى المؤهل الدراسي لأفراد عينة الدراسة فقد تم سؤالهم عن المؤهل الدراسي الحاصلين عليه، وتم إعطاؤهم الخيارات أدناه، وجاءت إجاباتهم موزعة كما هو مبين في **الجدول رقم (14):**

جدول رقم (14) توزيع أفراد عينة الدراسة وفق متغير المؤهل الدراسي

المؤهل الدراسي	التكرار	النسبة
بكالوريوس / ما يعادله	160	59.26
دبلوم دراسات عليا / ما يعادله	7	2.59
ماجستير/ ما يعادله	96	35.56
دكتوراه / ما يعادلها	7	2.59
الإجمالي	270	%100

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (14)** أن أعلى نسبة من أفراد العينة هم فئة المؤهل الدراسي (**بكالوريوس / ما يعادله**) بنسبة (**59.26%**)، بينما جاء الذين مؤهلهم (**دكتوراه/ ما يعادلها**) بنسبة (**2.59%**) في المرتبة الأخيرة، **ويرى الباحث** أن هذه النتيجة تعود إلى أن مؤسسات القطاع المصرفي تفضل توظيف الأفراد ذوي المؤهلات الجامعية؛ نظرًا لقدرتهم على تلبية متطلبات الوظائف المتوسطة إلى العليا بشكل فعال، مما يعكس التوجه نحو استقطاب الكفاءات القادرة على التكيف مع بيئة العمل الديناميكية، كما أن الحاصلين على الدرجات العليا قد يُعدّون أقل ملاءمة للوظائف المتاحة، أو يميلون إلى البحث عن فرص أكاديمية أو بحثية بدلاً من العمل في القطاع المصرفي.

د. سنوات الخبرة:

لمعرفة عدد سنوات الخبرة لأفراد عينة الدراسة فقد تم سؤالهم عن سنوات الخبرة لديهم، وتم إعطاؤهم الخيارات أدناه، وجاءت إجاباتهم موزعة كما هو مبين في **الجدول رقم (15)**:

جدول رقم (15) توزيع أفراد عينة الدراسة وفق متغير سنوات الخبرة

عدد سنوات الخبرة	التكرار	النسبة
5 سنوات أو أقل	28	10.37
6 – 10 سنوات	38	14.07
11 – 15 سنة	45	16.67
16 – 20 سنة	82	30.37
21 سنة أو أكثر	77	28.52
الإجمالي	270	%100

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (15)** أن أعلى نسبة من أفراد العينة هم الفئة التي تتمتع بسنوات خبرة من (**16-20 سنة**) بنسبة (**30.37%**)، بينما جاءت الفئة ذات سنوات الخبرة (**5 سنوات أو أقل**) بنسبة (**10.37%**) ، وكذا الفئة ذات سنوات الخبرة (**6 – 10 سنوات**) بنسبة (**14.07%**) في المرتبة الأخيرة، **ويرى الباحث** أن السبب في ذلك يعود إلى أن المؤسسات المصرفية تفضل توظيف الأفراد ذوي الخبرة الطويلة، الذين يمتلكون معرفة عميقة بالعمليات والإجراءات المصرفية؛ مما يعزز من كفاءة الأداء ويدعم استقرار المؤسسات. كما أن وجود نسبة أقل من الموظفين ذوي الخبرة المحدودة يشير إلى أن القطاع يميل إلى استقطاب الكفاءات التي يمكنها الإسهام الفعال في تحقيق أهداف العمل.

2.عرض وتحليل نتائج متغيرات الدراسة:

بعد أن تم عرض وتحليل ومناقشة البيانات الشخصية لعينة الدراسة فإن الباحث سيقوم هنا بعرض وتحليل ومناقشة استجابات أفراد عينة الدراسة حول متغيرات الدراسة الرئيسة، وهذه المتغيرات هي على النحو التالي:

أ. نتائج التحليل الوصفي للمتغير المستقل (الذكاء الاصطناعي):

يتناول **الجدول رقم (16)** نتائج التحليل الوصفي **للمتغير المستقل (الذكاء الاصطناعي)** لتوضيح مدى تأثير الذكاء الاصطناعي وتطبيقاته على إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي القطري.

جدول رقم (16) المتوسطات والانحرافات المعيارية واستجابات الدراسة نحو بُعد (الذكاء الاصطناعي) ن = 270

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية
1	تعزز أنظمة الذكاء الاصطناعي القدرة على التنبؤ بحدوث المخاطر المالية قبل وقوعها .	3.73	74.67	0.879	9	مرتفعة
2	يسهم استخدام النظم الخبيرة في تحسين قدرة المؤسسات على كشف عمليات الاحتيال المالي بشكل أسرع وأكثر دقة .	3.43	68.66	0.816	12	مرتفعة
3	تساعد النظم الخبيرة في وضع قواعد وإستراتيجيات مخصصة للكشف عن الأنشطة المشبوهة .	4.19	83.70	0.948	2	مرتفعة
4	تسهم النظم الخبيرة في تحسين إدارة البيانات وتحليلها بشكل أكثر كفاءة .	3.97	79.41	0.819	5	مرتفعة
5	يعزز تعلم الآلة من قدرة أنظمة إدارة المخاطر على التعرف على أنماط الجرائم المالية المستجدة .	4.00	80.00	0.810	4	مرتفعة
6	يعزز تعلم الآلة من قدرة أنظمة المراقبة على التكيف مع تغير أساليب الجرائم المالية .	3.44	68.89	0.863	11	مرتفعة
7	يرفع تعلم الآلة من مستوى الأمان في أنظمة المؤسسات المالية ضد عمليات الاحتيال والجرائم المالية .	3.73	74.67	0.879	10	مرتفعة
8	يسهم التعلم العميق في التعرف على عمليات غسيل الأموال بشكل أكثر دقة وفعالية .	3.41	68.22	0.824	14	مرتفعة
9	يساعد التعلم العميق في اكتشاف أنماط غير تقليدية في البيانات المالية قد تشير إلى عمليات غسيل أموال .	3.42	68.40	0.814	13	مرتفعة
10	يسهم التعلم العميق في تحسين تصنيف المعاملات المشبوهة وتقليل الإنذارات الكاذبة .	3.89	77.78	0.835	7	مرتفعة
11	يتيح الذكاء الاصطناعي التوليدي إنشاء تقارير وتحليلات دقيقة بشكل تلقائي لمساعدة فرق إدارة مخاطر الجريمة المالية .	4.16	83.11	0.753	3	مرتفعة

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية

12	يتيح الذكاء الاصطناعي التوليدي توليد سيناريوهات محتملة لحدوث الجرائم المالية لمزيد من الاستعداد .	3.85	77.04	0.833	8	مرتفعة
13	يتيح الذكاء الاصطناعي التوليدي تصميم نماذج وتوقعات دقيقة لمخاطر الجرائم المالية.	4.29	85.78	0.645	1	مرتفعة جدا
14	تسهم الأتمتة الروبوتية في تقليل الأخطاء البشرية وتحسين سرعة استجابة المؤسسات لمخاطر الجرائم المالية .	3.40	68	0.813	15	مرتفعة
15	تسهم العمليات الروبوتية في أتمتة إجراءات التحقيق وتقليل الوقت المستغرق فيها.	3.93	78.52	0.886	6	مرتفعة
إجمالي بُعد الذكاء الاصطناعي		**3.73**	**74.69**	**0.379**	**مرتفعة**	

*** تم وضع أرقام العبارات بترتيب وجودها بقائمة الاستبانة في جميع جداول الدراسة.**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يظهر **الجدول رقم (16) المتوسطات الحسابية والانحرافات المعيارية** لاستجابات عينة الدراسة تجاه عبارات **بُعد الذكاء الاصطناعي**، وتشير الدرجة الكلية الواردة في الجدول أن درجة **بُعد الذكاء الاصطناعي** لعينة الدراسة **(مرتفعة)**، حيث بلغ **المتوسط الحسابي** للدرجة الكلية **لبُعد الذكاء الاصطناعي (3.73) وبانحراف معياري** بلغ **(0.379)** ونسبة **مئوية** بلغت **(74.69%)**؛ مما يدل على **انخفاض التشتت** في آراء عينة الدراسة **وتقارب الآراء**، ويعد ذلك مؤشرًا مهمًا من الناحية الإحصائية والتفسيرية، حيث إن مفهوم **التشتت** يُشير إلى **مدى تنوع أو تباين الآراء داخل العينة**، ويُقاس غالبًا بمؤشرات مثل الانحراف المعياري أو التباين، حيث يُعبر انخفاض هذه القيم عن تقارب في آراء المبحوثين وتجانس في تقييماتهم، وتكمن أهمية هذا التقارب في كونه يُعزز من **موثوقية النتائج وقابليتها للتعميم**؛ إذ إن محدودية التباين تعكس حالة من **الاتساق الداخلي في الإجابات**، ما يُدلل على وضوح المفاهيم محل القياس وسلامة تصميم أداة الاستبانة.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Mytnyk et al.,2023) بعنوان: "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition" من أن **تطبيقات الذكاء الاصطناعي** قد أثبتت فاعليتها في **تحسين دقة اكتشاف جرائم الاحتيال**، ومن **منظور الباحث** فإن **انخفاض التشتت** يُسهم في **تدعيم استنتاج** أن **عينة الدراسة تُعبر بدرجة جيدة عن الظاهرة المدروسة**، ويُضيف قوة تفسيرية للنتائج، حيث يُمكن فهمها على أنها **انعكاس حقيقي للاتجاه العام ووعي جيد لدى مجتمع الدراسة إزاء تبني تطبيقات الذكاء الاصطناعي في المؤسسات المصرفية**، وأن **مستوى تطبيق الذكاء الاصطناعي في المؤسسات المصرفية مرتفع.**

ويلاحظ في **الجدول رقم (16)** أن **العبارة رقم (13)** قد حصلت على **أعلى المتوسطات الحسابية**، حيث بلغ **(4.29) وبانحراف معياري** بلغ **(645.0)**، ونسبة **مئوية** بلغت **(85.78%)** وجاءت بدرجة **(مرتفعة جدا)**، في حين حصلت **العبارة رقم (14)** على **أدنى المتوسطات الحسابية**، حيث بلغ **(3.40)**، **وبانحراف معياري** بلغ **(0.813)**، ونسبة **مئوية** بلغت **(68.00%)** وجاءت بدرجة **(مرتفعة)**.

وكما يتضح من **ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح**، نجد تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: **"يتيح الذكاء الاصطناعي التوليدي تصميم نماذج وتوقعات دقيقة لمخاطر الجرائم المالية"** بنسبة **(85.78%)** وصولاً إلى عبارة: **"تسهم الأتمتة الروبوتية في تقليل الأخطاء البشرية وتحسين سرعة استجابة المؤسسات لمخاطر الجرائم المالية"** بنسبة **(68.00%).**

ويُعد تحليل المتوسطات الحسابية والانحرافات المعيارية من الأدوات الإحصائية المهمة التي تسهم في الكشف عن مدى قبول ورضا أفراد العينة تجاه العبارات المتعلقة **بالمتغير المستقل "الذكاء الاصطناعي"**؛ إذ يُمكن من خلال هذا التحليل استقراء اتجاهات الاستجابة وتحديد مجالات القوة والقصور، مما يزود الباحثين بمؤشرات دقيقة لتوجيه جهود التطوير المستقبلية.

ومن ثمَّ فإن حصول **العبارة رقم (13): "يتيح الذكاء الاصطناعي التوليدي تصميم نماذج وتوقعات دقيقة لمخاطر الجرائم المالية"** على **أعلى متوسط حسابي ونسبة مئوية مرتفعة، مع انحراف معياري منخفض، يعكس درجة عالية من التوافق والقبول بين أفراد العينة**، وتُشير هذه النتيجة إلى قناعة قوية **بفاعلية الذكاء الاصطناعي التوليدي في تحسين دقة التحليل والتنبؤ بالمخاطر المالية المحتملة**، وهو ما **يُعزز من مكانته كأداة متقدمة في دعم القرار الوقائي في المؤسسات المصرفية**.

في المقابل، فإن حصول **العبارة رقم (14): "تسهم الأتمتة الروبوتية في تقليل الأخطاء البشرية وتحسين سرعة استجابة المؤسسات لمخاطر الجرائم المالية"** في المرتبة الأخيرة من حيث المتوسطات الحسابية، يدل على **انخفاض نسبي في مستوى الاتفاق أو الرضا عنها مقارنة ببقية العبارات**، وقد يُعزى ذلك **إلى تفاوت في تطبيق الأتمتة الروبوتية داخل المؤسسات** أو إلى **ضعف المعرفة لدى بعض المشاركين بآليات عملها وتأثيرها العملي المباشر**؛ مما يُبرز الحاجة **لمزيد من التوعية أو التطوير في هذا المجال.**

ويرى الباحث أنه يمكن **استخلاص عدد من الدلالات من هذه النتائج** كالتالي:

1. **تمييز جوانب القوة في تبني الذكاء الاصطناعي:** تعكس النتائج الإيجابية المرتبطة بالعبارة (13) نجاح تطبيقات الذكاء الاصطناعي التوليدي في مجال تحديد مخاطر الجرائم المالية، وهو ما يدعو إلى تعزيزه وتوسيع نطاقه ليشمل مزيدًا من أنشطة الكشف المبكر وإدارة المخاطر.
2. **تحديد مجالات القصور أو ضعف الفاعلية:** يشير التراجع النسبي في تقييم العبارة (14) إلى احتمالات وجود تحديات في تفعيل الأتمتة الروبوتية كمكوّن من مكونات الذكاء الاصطناعي في المؤسسات المصرفية، ما يُحتم إجراء مراجعات تطبيقية وفنية لتعزيز هذا الجانب.
3. **توجيه السياسات والتوجهات المستقبلية:** تمكّن هذه المؤشرات الباحثين وصناع القرار من بناء إستراتيجيات أكثر استهدافًا، تستند إلى بيانات واقعية تعكس مواقف العاملين حيال استخدام الذكاء الاصطناعي في التصدي لمخاطر الجريمة المالية.

وعليه، فإن نتائج هذا التحليل لا تقتصر على الوصف الكمي، بل تُعد مدخلاً تفسيريًا وإستراتيجيًا فاعلاً لفهم ديناميكيات تبني الذكاء الاصطناعي في القطاع المصرفي، وتُسهم في توجيه الجهود نحو تعزيز التطبيقات الناجحة، ومعالجة مكامن الضعف، لضمان بيئة مصرفية أكثر أمنًا وكفاءة.

ب. نتائج التحليل الوصفي للمتغير التابع (إدارة مخاطر الجريمة المالية):

سوف يقوم الباحث بقياس نتائج التحليل الوصفي للمتغير التابع **(إدارة مخاطر الجريمة المالية)** الخاصة بالأبعاد التالية:

1. تحديد مخاطر الجريمة المالية.
2. تحليل وتقييم مخاطر الجريمة المالية.
3. معالجة مخاطر الجريمة المالية.
4. مراقبة ومراجعة مخاطر الجريمة المالية.

1. نتائج التحليل الوصفي لبُعد المتغير التابع (تحديد مخاطر الجريمة المالية):

يتناول **الجدول رقم (17)** نتائج التحليل الوصفي **لبُعد المتغير التابع (تحديد مخاطر الجريمة المالية)** لتوضيح مدى **تأثير الذكاء الاصطناعي وتطبيقاته** على بُعد **تحديد مخاطر الجرائم المالية** في مؤسسات القطاع المصرفي القطري.

جدول رقم (17) المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (تحديد مخاطر الجريمة المالية) ن = 270

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية
1	تساعد أتمتة عمليات الكشف عن مخاطر الجريمة المالية على تحديد الجرائم المالية بشكل أدق.	3.89	77.78	0.735	5	مرتفعة
2	تسهم نظم الذكاء الاصطناعي في التعرف المبكر على مؤشرات الجرائم المالية.	4.21	84.15	0.703	1	مرتفعة جدا
3	يسهل تعلم الآلة عملية من تحديد أنماط الجرائم المالية غير الاعتيادية.	3.97	79.41	0.719	3	مرتفعة
4	تسهم تقنيات الذكاء الاصطناعي في توسيع نطاق الكشف عن مصادر الجرائم المالية.	4.04	80.74	0.709	2	مرتفعة
5	يُحسن الاعتماد على النظم الخبيرة من عملية تحديد مخاطر الجرائم المالية المحتملة.	3.84	76.89	0.792	7	مرتفعة
6	تساعد أدوات الذكاء الاصطناعي في تحديد مخاطر الجرائم المالية قبل وقوعها.	3.90	78.07	0.705	4	مرتفعة
7	تقلل تكنولوجيا الذكاء الاصطناعي من احتمالية التغاضي عن مخاطر الجرائم المالية.	3.86	77.19	0.748	6	مرتفعة
	إجمالي بُعد تحديد مخاطر الجريمة المالية	3.96	79.18	0.669	مرتفعة	

*** تم وضع أرقام العبارات بترتيب وجودها بقائمة الاستبانة في جميع جداول الدراسة.**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يُظهر **الجدول رقم (17) المتوسطات الحسابية والانحرافات المعيارية** لاستجابات عينة الدراسة تجاه عبارات **بُعد تحديد مخاطر الجريمة المالية**، وتشير الدرجة الكلية الواردة في الجدول أن درجة **بُعد تحديد مخاطر الجريمة المالية** لعينة الدراسة **(مرتفعة)**، حيث بلغ **المتوسط الحسابي** للدرجة الكلية **لبُعد تحديد مخاطر الجريمة المالية (3.96)** و**بانحراف معياري (0.669)** و**نسبة مئوية** بلغت **(79.18%)**؛ مما يدل على **انخفاض التشتت** في آراء عينة الدراسة **وتقارب الآراء**، ويُعد هذا المؤشر ذا دلالة إحصائية مهمة، حيث إنه يعكس **تجانسًا وتقاربًا في إدراك المشاركين لتأثير تقنيات الذكاء الاصطناعي على عمليات تحديد مخاطر الجريمة المالية داخل المؤسسات المصرفية**، ويُشير هذا التجانس إلى وجود **اتفاق نسبي بين آراء المبحوثين حول فاعلية الذكاء الاصطناعي في دعم آليات التعرف المبكر على أنماط و أنشطة قد تنطوي على مخاطر مالية غير مشروعة**.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Zhu et al., 2021) بعنوان: "Intelligent Financial Fraud Detection Practices in Post-Pandemic Era." والتي توصلت إلى أن **تقنيات الذكاء الاصطناعي** لديها **قدرات كبيرة على أتمتة الكشف عن الاحتيال وتحديد الأنماط المشبوهة**، ومن منظور الباحث فإن **انخفاض مستوى التباين في الاستجابات يُعزز** من **موثوقية النتائج ودقتها التفسيرية**، حيث يدل ذلك على **وعي مشترك بأهمية توظيف أدوات الذكاء الاصطناعي**، مثل تعلم الآلة والنظم الخبيرة، **في تحسين قدرات المؤسسات المصرفية على تحديد المخاطر في مراحلها الأولى**، كما يُسهم هذا الاتساق في تأكيد أن **بُعد تحديد المخاطر يعد من الأبعاد الأساسية في إدارة مخاطر الجريمة المالية**، وأن مستوى الوعي به مرتفع، وأن **الذكاء الاصطناعي يُمثل**

عاملاً مؤثرًا ومُعززًا في عملية تحديد مخاطر الجريمة المالية، ويُضفي على نتائج الدراسة مزيدًا من **القوة والقدرة على التعميم في سياق المؤسسات المصرفية محل الدراسة**.

ويلاحظ في **الجدول رقم (17)** أن **العبارة رقم (2): "تسهم نظم الذكاء الاصطناعي في التعرف المبكر على مؤشرات الجرائم المالية"** قد حصلت على **أعلى المتوسطات الحسابية**، حيث بلغ **(4.21)** **وبانحراف معياري (0.703)**، **ونسبة مئوية** بلغت **(84.15%)** وجاءت بدرجة (**مرتفعة جدا**)، في حين حصلت **العبارة رقم (5): "يُحسن الاعتماد على النظم الخبيرة من عملية تحديد المخاطر المحتملة"** على **أدنى المتوسطات الحسابية**، حيث بلغ **(3.84)**، **وبانحراف معياري** بلغ **(0.792)**، **ونسبة مئوية** بلغت **(76.89%)** وجاءت بدرجة (**مرتفعة**).

وكما يتضح من **ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح**، نجد تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "**تسهم نظم الذكاء الاصطناعي في التعرف المبكر على مؤشرات الجرائم المالية**" بنسبة **(84.15%)**، وصولاً إلى عبارة: **يُحسن الاعتماد على النظم الخبيرة من عملية تحديد المخاطر المحتملة"** بنسبة **(76.89%)**.

ويُعد تحليل المتوسطات الحسابية والانحرافات المعيارية وسيلة فعالة لفهم اتجاهات استجابات المشاركين بشأن **تأثير الذكاء الاصطناعي على بُعد "تحديد مخاطر الجريمة المالية" في المؤسسات المصرفية**، حيث تتيح هذه المؤشرات رصد مستويات القبول ومدى التوافق أو التباين في الرؤى حول دور تقنيات الذكاء الاصطناعي في هذا الجانب الحيوي، ومن ثمَّ فإن حصول **العبارة رقم (2)** على **أعلى متوسط حسابي ونسبة مئوية عالية، مع انحراف معياري منخفض** يعني وجود **درجة مرتفعة للغاية من المو افقة** من قبل أفراد العينة، وتُعبر هذه النتيجة عن **إدراك قوي** لدى المشاركين **بأهمية نظم الذكاء الاصطناعي في تعزيز القدرة الاستباقية للمؤسسات المصرفية على رصد الإشارات الأولية التي قد تنذر بوقوع جرائم مالية**؛ الأمر الذي يعزز من كفاءة نظم الإنذار المبكر، ويُعد أحد أهم جوانب الوقاية المؤسسية، وفي المقابل يعكس حصول **العبارة رقم (5)** على **أدنى متوسط حسابي مستوى أقل نسبيًا من المو افقة أو القناعة مقارنة بالعبارات الأخرى**، وقد يشير ذلك إلى **تفاوت في درجة الثقة أو الانتشار الفعلي لاستخدام النظم الخبيرة في القطاع المصرفي أو محدودية فهم بعض المشاركين لطبيعة هذه النظم وآلية عملها**.

ويرى الباحث أنه يمكن **استخلاص عدد من الدلالات من هذه النتائج** كالتالي:

1. **أن تركيز المشاركين على التأثير العملي والتطبيقي المباشر للذكاء الاصطناعي**، كما في **العبارة رقم (2)**، يُبرز **الجوانب الأكثر وضوحًا وتأثيرًا في الممارسات اليومية**.
2. **وجود تباين نسبي في المو اقف تجاه النظم المتخصصة**، مثل "**النظم الخبيرة**"، والتي قد لا تكون منتشرة أو مفهومة بالدرجة نفسها، **ما يستدعي المزيد من التدريب أو التوعية**.
3. **تعزيز ثقة الباحث بنتائج الدراسة**؛ إذ تؤكد هذه المؤشرات أن للذكاء الاصطناعي دورًا فعّالاً وملموسًا في دعم عمليات تحديد مخاطر الجرائم المالية، سواء من خلال قدراته التحليلية أو من خلال أدواته التخصصية.

ومن ثمَّ تؤكد هذه النتائج أن **الذكاء الاصطناعي يُمثل أداة إستراتيجية في تحديد مخاطر الجريمة المالية** داخل القطاع المصرفي، مع وجود تفاوت نسبي في مدى الاستفادة من تطبيقاته المختلفة، ما يُبرز الحاجة إلى مواصلة التطوير المؤسسي والتقني في هذا المجال.

2. نتائج التحليل الوصفي لبُعد المتغير التابع (تحليل وتقييم مخاطر الجريمة المالية):

يتناول **الجدول رقم (18)** نتائج التحليل الوصفي **لبُعد المتغير التابع (تحليل وتقييم مخاطر الجريمة المالية)** لتوضيح مدى **تأثير الذكاء الاصطناعي وتطبيقاته** على بُعد **تحليل وتقييم مخاطر الجرائم المالية** في مؤسسات القطاع المصرفي القطري.

جدول رقم (18) المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (تحليل وتقييم مخاطر الجريمة المالية) ن = 270

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية
1	تتيح تقنيات التعلم العميق تحليل أكثر دقة لبيانات الجرائم المالية.	4.00	80.00	0.638	2	مرتفعة
2	تسهل نظم الذكاء الاصطناعي تقييم درجة خطورة كل خطر جريمة مالية.	3.61	72.19	0.708	7	مرتفعة
3	تساعد أدوات الذكاء الاصطناعي في تصنيف مخاطر الجرائم المالية حسب مستوى احتمالية حدوثها.	3.80	77.10	0.621	3	مرتفعة
4	تعلم تحليل البيانات باستخدام الآلة يسرع من عملية تقييم مخاطر الجريمة المالية.	3.68	73.63	0.669	6	مرتفعة
5	يسهم الذكاء الاصطناعي في تطوير نماذج تقييم مخاطر جريمة مالية أكثر موضوعية وفعالية.	3.78	75.59	0.652	4	مرتفعة
6	يتم التقييم المستمر لمخاطر الجرائم المالية بشكل أكثر دقة باستخدام التقنيات الذكية.	3.73	74.60	0.779	5	مرتفعة
7	تقلل أدوات الذكاء الاصطناعي من الاعتماد على التقديرات الشخصية في تقييم مخاطر الجرائم المالية.	4.13	82.60	0.609	1	مرتفعة
إجمالي بُعد تحليل وتقييم مخاطر الجريمة المالية		**3.825**	**76.50**	**0.683**	**مرتفعة**	

*** تم وضع أرقام العبارات بترتيب وجودها بقائمة الاستبانة في جميع جداول الدراسة.**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يُظهر **الجدول رقم (18) المتوسطات الحسابية والانحرافات المعيارية** لاستجابات عينة الدراسة تجاه **عبارات بُعد تحليل وتقييم مخاطر الجريمة المالية**، وتشير الدرجة الكلية الواردة في الجدول أن **درجة بُعد تحليل وتقييم مخاطر الجريمة المالية** لعينة الدراسة **(مرتفعة)**، حيث بلغ **المتوسط الحسابي** للدرجة الكلية **لبُعد تحليل وتقييم مخاطر الجريمة المالية (3.825)** وبانحراف **معياري (0.683)** ونسبة **مئوية** بلغت **(76.50%)**؛ مما يدل على **انخفاض التشتت** في آراء عينة الدراسة **وتقارب الآراء**، ويُعد هذا المؤشر ذا دلالة إحصائية مهمة، حيث إنه يدل على وجود **اتفاق واسع بين المشاركين بشأن الدور الإيجابي والفعّال لتقنيات الذكاء الاصطناعي في تعزيز عمليات التحليل والتقييم** داخل المؤسسات المصرفية، ويُشير هذا التجانس إلى أن أفراد العينة يُدركون بصورة متقاربة **أهمية الذكاء الاصطناعي في دعم اتخاذ القرار في مجال تحليل وتقييم مخاطر الجريمة المالية** من خلال استخدام خوارزميات متقدمة لتحليل البيانات المالية المعقدة، ورصد الأنماط غير الاعتيادية التي قد تدل على وجود نشاط إجرامي.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Piao and Xiao, 2022) بعنوان: "Risk Management Analysis of Modern Commercial Banks Using Behavioral Finance Theory and Artificial Neural Networks" والتي توصلت إلى أن **تقنيات الذكاء الاصطناعي** لديها **قدرات كبيرة على تحليل وتقييم مخاطر الجريمة المالية بعيدا عن العواطف والتحيزات الشخصية لمديري المخاطر التي قد تؤثر سلبًا على إدارة المخاطر**، ومن منظور الباحث فإن **انخفاض التباين في الاستجابات** يُعد مؤشرًا

على أن المؤسسات المصرفية تركز بشكل كبير على تحليل المخاطر وتقييمها، **كما تشير لتوحّد الفهم لدى العينة بشأن قدرة الذكاء الاصطناعي على تحسين جودة تحليل وتقييم مخاطر الجريمة المالية**، وتقليل احتمالية التقدير الخاطئ أو التأخر في كشف التهديدات المحتملة، ومن ثمَّ تُعزز هذه النتيجة من موثوقية الدراسة وتدعم فرضيتها القائلة بأن **الذكاء الاصطناعي يُسهم بفاعلية في تطوير نظم تحليل وتقييم مخاطر الجريمة المالية في القطاع المصرفي**.

ويلاحظ في **الجدول رقم (18)** أن **العبارة رقم (7)** قد حصلت على **أعلى المتوسطات الحسابية**، حيث بلغ **(4.13)** **وبانحراف معياري (0.609)**، **ونسبة مئوية** بلغت **(82.67%)** وجاءت بدرجة **(مرتفعة)**، في حين حصلت **العبارة رقم (2)** على **أدنى المتوسطات الحسابية**، حيث بلغ **(3.61)**، **وبانحراف معياري** بلغ **(0.708)**، **ونسبة مئوية** بلغت **(72.19%)** وجاءت بدرجة **(مرتفعة)**.

وكما يتضح من **ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح**، نجد تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "**تقلل أدوات الذكاء الاصطناعي من الاعتماد على التقديرات الشخصية في تقييم المخاطر**" بنسبة **(82.67%)** وصولاً إلى عبارة: "**تسهل نظم الذكاء الاصطناعي تقييم درجة خطورة كل خطر جريمة مالية**" بنسبة **(72.19%)**.

ووفقا لما سبق أن أوضحناه في تحليل البُعد السابق من أبعاد المتغير التابع، يُعد تحليل المتوسطات الحسابية والانحرافات المعيارية أداة فعالة لفهم استجابات المشاركين وتقييم مدى إدراكهم **لأهمية الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية**، حيث يسهم هذا التحليل في إبراز العبارات التي تعكس **قبولاً مرتفعًا** لدى أفراد العينة، مقابل العبارات التي تشير إلى جوانب قد تستدعي **مزيدًا من التطوير أو الدراسة**، ووفقا لذلك فإن حصول **العبارة رقم (4): "تقلل أدوات الذكاء الاصطناعي من الاعتماد على التقديرات الشخصية في تقييم مخاطر الجريمة المالية"** على **أعلى متوسط حسابي بين العبارات المرتبطة بهذا البُعد** يُشير بوضوح إلى **اتفاق كبير بين المشاركين على الدور المحوري لأدوات الذكاء الاصطناعي في تعزيز موضوعية ودقة تقييم المخاطر بعيدًا عن التحيزات الفردية أو الاجتهادات الشخصية**، ويعكس من ثمَّ **درجة عالية من الثقة** في هذه الأدوات على أنها **داعم رئيسي في عمليات تقييم مخاطر الجريمة المالية القائمة على البيانات والتحليل المتقدم**.

في المقابل، يعني حصول **العبارة رقم (2): "تسهل نظم الذكاء الاصطناعي تقييم درجة خطورة كل خطر جريمة مالية"** على أدنى ترتيب من حيث المتوسط الحسابي يُشير إلى **ضعف نسبي** في مستوى القبول أو الاقتناع **بقدرة هذه النظم على تحديد مستوى الخطورة بدقة لكل نوع من مخاطر الجريمة المالية**، وربما يُعزى ذلك إلى **التحديات التقنية أو الإجرائية في تنفيذ هذه الوظيفة على نحو دقيق داخل بيئات العمل الفعلية**.

ومن وجهة نظر الباحث، يمكن **استخلاص عدد من الدلالات من هذه النتائج** كما يلي:

1. **تمييز مجالات الأداء القوي:** يُعد **ارتفاع المتوسط الحسابي للعبارة (4)** مؤشرًا على إدراك المشاركين **لأهمية تقليل الاعتماد على الاجتهادات الشخصية في التقييم**؛ مما يعزز **الحاجة إلى توسيع تطبيق أدوات الذكاء الاصطناعي في مراحل التحليل المتقدم لمخاطر الجريمة المالية.**
2. **تحديد مجالات التحسين: النتائج الأقل إيجابية للعبارة (2)** تُسلط الضوء على **احتمالية وجود فجوة بين القدرات التقنية المتاحة والتطبيق العملي لأنظمة تقييم درجة خطورة الجريمة المالية**، مما يتطلب **مراجعة آليات التقييم ورفع كفاءة النظم المستخدمة.**
3. **دعم التوجهات المستقبلية:** تُسهم هذه المؤشرات في توجيه الاهتمام البحثي والتطبيقي نحو **تعزيز النظم التي أثبتت فاعليتها، ومعالجة نقاط الضعف القائمة**؛ مما يُعزز **كفاءة مؤسسات القطاع المصرفي في التنبؤ بمخاطر الجريمة المالية وتقييمها بدقة.**

بناءً عليه، فإن **هذه النتائج** لا تقتصر على الوصف الكمي لاستجابات المشاركين، بل **تُوفر رؤية تحليلية إستراتيجية تعكس واقع استخدام الذكاء الاصطناعي في تقييم مخاطر الجرائم المالية، وتُسهم في تطوير الممارسات المؤسسية** المرتبطة بهذا المجال الحيوي.

3. نتائج التحليل الوصفي لبُعد المتغير التابع (معالجة مخاطر الجريمة المالية):

يتناول **الجدول رقم (19)** نتائج التحليل الوصفي **لبُعد المتغير التابع (معالجة مخاطر الجريمة المالية)** لتوضيح مدى **تأثير الذكاء الاصطناعي وتطبيقاته** على بُعد معالجة مخاطر **الجرائم المالية** في مؤسسات القطاع المصرفي القطري.

جدول رقم (19) المتوسطات والانحرافات المعيارية واستجابات عينة الدراسة نحو بُعد (معالجة مخاطر الجريمة المالية) ن = 270

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية
1	تسهم تطبيقات الذكاء الاصطناعي في تنفيذ إجراءات وقائية فعالة ضد الجرائم المالية.	3.64	72.89	0.634	3	مرتفعة
2	تساعد الأتمتة في الحد من الأخطاء البشرية أثناء معالجة مخاطر الجريمة المالية.	3.77	75.41	0.691	4	مرتفعة
3	تُمكن نظم الذكاء الاصطناعي من اتخاذ إجراءات تصحيحية بسرعة عند اكتشاف خطر جريمة مالية.	3.61	72.15	0.608	5	مرتفعة
4	يقلل استخدام الروبوتات في العمليات من احتمالية التلاعب المالي.	4.00	80.00	0.638	1	مرتفعة
5	تسهم أدوات الذكاء الاصطناعي في تطبيق سياسات مكافحة الجرائم المالية بشكل أكثر فاعلية.	3.59	71.86	0.667	6	مرتفعة
6	تقلل الأتمتة من التكلفة والوقت اللازم لمعالجة مخاطر الجريمة المالية.	3.78	75.56	0.652	2	مرتفعة
7	تدعم أنظمة الذكاء الاصطناعي وضع خطط استجابة مرنة لمخاطر الجريمة المالية المكتشفة.	3.56	71.14	0.588	7	مرتفعة
إجمالي بُعد معالجة مخاطر الجريمة المالية		**3.73**	**74.57**	**0.594**	**مرتفعة**	

*** تم وضع أرقام العبارات بترتيب وجودها بقائمة الاستبانة في جميع جداول الدراسة.**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يُظهر **الجدول رقم (19) المتوسطات الحسابية والانحرافات المعيارية** لاستجابات عينة الدراسة تجاه عبارات **بُعد معالجة مخاطر الجريمة المالية**، وتشير الدرجة الكلية الواردة في الجدول أن **درجة بُعد معالجة مخاطر الجريمة المالية** لعينة الدراسة (**مرتفعة**)، حيث بلغ **المتوسط الحسابي** للدرجة الكلية **لبُعد معالجة مخاطر الجريمة المالية (3.73)** وبانحراف **معياري (0.594)** ونسبة **مئوية** بلغت **(74.57%)**؛ مما يدل على **انخفاض التشتت** في آراء عينة الدراسة **وتقارب الآراء**، ويعكس هذا التجانس في الآراء إدراكًا مشتركًا لدى المبحوثين **بفاعلية الذكاء الاصطناعي في دعم إستراتيجيات المعالجة والتصدي لمخاطر الجريمة المالية** داخل المؤسسات المصرفية، وأهمية تطبيق تقنياته المختلفة، مثل الأتمتة والروبوتات التي تُسهم في تنفيذ إجراءات وقائية، والحد من الأخطاء البشرية لمعالجة الحالات المشبوهة بكفاءة أعلى.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Awasthi, 2022) بعنوان: "Using Artificial Intelligence to Prevent Banking Fraud والتي توصلت إلى أن **تقنيات الذكاء الاصطناعي** لديها **قدرات عالية على معالجة مخاطر الجريمة المالية وتعزيز الإجراءات الأمنية في القطاع المصرفي**، ومن منظور الباحث فإن **هذا الاتساق في التقييمات** يُدلل على أن **المؤسسات تتخذ إجراءات فعالة لمعالجة المخاطر عند تحديدها وتقييمها**، وعلى أن **الذكاء الاصطناعي يُمثل أداة محورية في تحسين قدرات المؤسسات المصرفية على اتخاذ إجراءات فعالة وسريعة لمعالجة مخاطر الجريمة المالية**، بما في ذلك تجميد المعاملات المشبوهة، وتفعيل آليات الإنذار المبكر، وتعزيز سرعة التدخل، كما يُضفي هذا **الانخفاض في التباين** بين استجابات العينة **مزيدًا من الموثوقية على النتائج، ويعزّز من إمكانية تعميمها**، مؤكّدًا أن الذكاء الاصطناعي لا يُستخدم فقط في الكشف والتحليل، بل **يُسهم بشكل مباشر وفعّال في معالجة مخاطر الجريمة المالية وتقليل آثارها المختلفة**.

ويلاحظ في **الجدول رقم (19)** أن **العبارة رقم (4)** قد حصلت على **أعلى المتوسطات الحسابية**، حيث بلغ **(4.00)** وبانحراف **معياري (0.638)**، ونسبة مئوية بلغت **(80.00%)** وجاءت بدرجة **(مرتفعة)**، في حين حصلت **العبارة رقم (7)** على **أدنى المتوسطات الحسابية**، حيث بلغ **(3.56)**، وبانحراف **معياري** بلغ **(0.588)**، ونسبة **مئوية** بلغت **(71.14%)** وجاءت بدرجة **(مرتفعة)**.

وكما يتضح من **ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح** نجد تدرج أهمية العبارات لعينة الدراسة حيث ترى عينة الدراسة مدى أهمية عبارة **(يقلل استخدام الروبوتات في العمليات من احتمالية التلاعب المالي)** بنسبة **(80.00%)** وصولاً إلى عبارة **(تدعم أنظمة الذكاء الاصطناعي وضع خطط استجابة مرنة لمخاطر الجريمة المالية المكتشفة)** بنسبة **(71.14%)**.

وكما أوضحنا سابقا، يسهم تحليل المتوسطات الحسابية والانحرافات المعيارية في تقديم تصور دقيق حول اتجاهات استجابات أفراد العينة فيما يتعلق **بتأثير الذكاء الاصطناعي** على بُعد معالجة مخاطر **الجريمة المالية**، حيث يساعد هذا التحليل في **تحديد مواطن القوة والجوانب التي قد تستدعي تطويرًا أو تعزيزًا مستقبليًا**، وعليه فإن حصول **العبارة رقم (4): "يقلل استخدام الروبوتات في العمليات من احتمالية التلاعب المالي"** على **أعلى متوسط حسابي بين العبارات المرتبطة بهذا البُعد** يعكس **مستوى مرتفعًا من القبول والاتفاق بين المشاركين** بشأن **الدور الفعّال** الذي تلعبه **تقنيات الأتمتة الذكية والروبوتات في تقليص فرص التلاعب، وتحقيق قدر أكبر من النزاهة والرقابة في المعاملات المالية**، كما يشير هذا إلى **ثقة المشاركين في قدرة الذكاء الاصطناعي على دعم بيئة تشغيل أكثر أمانًا وشفافية**.

وفي المقابل، فإن مجيء **العبارة رقم (7): "تدعم أنظمة الذكاء الاصطناعي وضع خطط استجابة مرنة لمخاطر الجريمة المالية المكتشفة"** في **أدنى مرتبة من حيث المتوسط الحسابي** يشير إلى **تباين أو انخفاض نسبي في مستوى الاتفاق بين أفراد العينة حيال هذه الوظيفة المحددة**، وقد يُعزى ذلك إلى **ضعف في التطبيق العملي أو محدودية التجربة المؤسسية لدى المشاركين** فيما **يتعلق باستخدام الذكاء الاصطناعي في بناء وتفعيل خطط استجابة ديناميكية**.

ويرى الباحث إنه يمكن استخلاص عدد من الدلالات من هذه النتائج كالتالي:

1. **تمييز الوظائف الأكثر قبولاً وفاعلية:** تُظهر **النتائج المرتفعة للعبارة رقم (4)** أن **الأتمتة المعتمدة على الذكاء الاصطناعي** تُعد إحدى **أدوات المعالجة الفعالة لمخاطر الجريمة المالية**، وينبغي **دعمها وتوسيع نطاق استخدامها في النظم المصرفية**.
2. **رصد الفجوات في التطبيق أو الإدراك:** توضح **النتائج المنخفضة للعبارة رقم (7) وجود فجوة إدراكية** أو **عملية تستدعي تعزيز قدرات الذكاء الاصطناعي في مجال تصميم وتنفيذ استجابات مرنة لمخاطر الجريمة المالية**، إما من خلال **تطوير الأنظمة**، أو **رفع مستوى وعي الكوادر العاملة بإمكاناتها**.

3. **توجيه الجهود التطويرية والإستراتيجية:** تساعد هذه المؤشرات صنّاع القرار والباحثين على تحديد النقاط التي تستدعي **تدخلاً تطويريًا، مقابل تلك التي أثبتت فعاليتها** في نظر المستجيبين، ما يدعم **رسم سياسات دقيقة لتعزيز دور الذكاء الاصطناعي في المعالجة الفعالة لمخاطر الجريمة المالية.**

وعليه، فإن هذا التحليل لا يُعد توصيفًا رقميًا فحسب، بل يمثل أداة **تحليلية وإستراتيجية تعززمن فهم و اقع توظيف الذكاء الاصطناعي في مجال معالجة المخاطر**، وتوجه الجهود نحو تطوير استخداماته بما **يعزز الحوكمة والامتثال المالي داخل المؤسسات المصرفية.**

4. نتائج التحليل الوصفي لبُعد المتغير التابع (مر اقبة ومراجعة مخاطر الجريمة المالية):

يتناول **الجدول رقم (20)** نتائج التحليل الوصفي لبُعد المتغير التابع (**مر اقبة ومراجعة مخاطر الجريمة المالية**) لتوضيح مدى تأثير الذكاء الاصطناعي وتطبيقاته على بُعد مراقبة ومراجعة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي القطري.

جدول رقم (20) المتوسطات والانحر افات المعيارية واستجابات عينة الدراسة نحو بُعد (مر اقبة ومراجعة مخاطر الجريمة المالية) ن = 270

رقم العبارة	العبارات	المتوسط	المتوسط المئوي المرجح	الانحراف المعياري	ترتيب أهمية العبارات	مستوى الأهمية
1	تُمكن نظم الذكاء الاصطناعي من المراجعة الدورية لمخاطر الجرائم المالية.	3.75	75.08	0.583	3	مرتفعة
2	تساعد أدوات التحليل الذكية في رصد التطورات الجديدة في أنماط الجرائم المالية.	3.88	77.67	0.636	4	مرتفعة
3	تُمكن المراقبة المستمرة باستخدام التقنيات الذكية من تحديث إستراتيجيات إدارة مخاطر الجرائم المالية.	3.72	74.31	0.559	5	مرتفعة
4	تسهم تقنيات التعلم العميق في التعرف على التغيرات في أساليب ارتكاب الجرائم المالية.	4.12	82.40	0.587	1	مرتفعة
5	توفر نظم الذكاء الاصطناعي تقارير دورية دقيقة عن حالة المخاطر ذات الصلة بالجرائم المالية.	3.70	74.02	0.614	6	مرتفعة
6	تُمكن نظم الذكاء الاصطناعي من مراقبة ومراجعة المخاطر بشكل دوري؛ مما يمكن من تعديل إجراءات إدارة مخاطر الجريمة المالية بشكل فعال.	3.89	77.83	0.600	2	مرتفعة
7	تسهل أدوات الذكاء الاصطناعي عملية تتبع الأداء في إدارة مخاطر الجرائم المالية.	3.67	73.27	0.541	7	مرتفعة
إجمالي بُعد مر اقبة ومراجعة مخاطر الجريمة المالية		**3.82**	**76.37**	**0.511**	**مرتفعة**	

*** تم وضع أرقام العبارات بترتيب وجودها بقائمة الاستبانة في جميع جداول الدراسة.**

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يُظهر **الجدول رقم (20) المتوسطات الحسابية والانحر افات المعيارية** لاستجابات عينة الدراسة تجاه عبارات **بُعد مر اقبة ومراجعة مخاطر الجريمة المالية**، وتشير الدرجة الكلية الواردة في الجدول أن **درجة بُعد مر اقبة ومراجعة مخاطر الجريمة المالية** لعينة الدراسة (**مرتفعة**)، حيث بلغ **المتوسط الحسابي** للدرجة الكلية **لبُعد معالجة مخاطر الجريمة المالية (3.82)** وبانحراف **معياري (0.511)** ونسبة **مئوية** بلغت **(76.37%)**؛ مما يدل على **انخفاض التشتت** في آراء عينة الدراسة **وتقارب**

الآراء، وهو ما يعكس **تجانسًا نسبيًا في تقييم المشاركين لدور الذكاء الاصطناعي في دعم عمليات المراقبة المستمرة والمراجعة الدورية لمخاطر الجريمة المالية** داخل بيئة العمل في المؤسسات المصرفية، ويُشير هذا التقارب في الآراء إلى **وجود إدراك مشترك** لدى أفراد العينة **بأهمية توظيف أدوات الذكاء الاصطناعي**، مثل **تقنيات التعلم العميق والتحليلات التنبؤية الذكية في تعزيز كفاءة الرقابة الداخلية، وتحديث تقييمات المخاطر بشكل دوري استنادًا إلى بيانات حية ومتغيرة**.

وتتفق هذه النتيجة مع ما توصلت إليه دراسة (Hilal et al., 2022) بعنوان: "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances" من **قيام المحتالين بتطوير أساليبهم بشكل مستمر لاستغلال نقاط الضعف، وهو ما يستلزم أنظمة متقدمة ومتطورة باستمرار للكشف عن الجرائم المالية وأساليبها المتغيرة والمتطورة دائما**، وبينت الدراسة **القدرات الكبيرة لنماذج وتطبيقات الذكاء الاصطناعي لمواجهة هذا التغير والتطور المستمر في الجرائم المالية**، ومن **وجهة نظر الباحث** يُعد هذا **الاتساق في استجابات العينة مؤشرًا مهمًا** على أن **الذكاء الاصطناعي يُسهم بفاعلية في تمكين المؤسسات المصرفية من مراقبة التغيرات في أنماط الجريمة المالية ومراجعة إستراتيجيات المواجهة على نحو ديناميكي وتفاعلي**، كما أن **انخفاض التباين في الآراء يعزّز من ثقة الباحث في نتائج الدراسة**، ويؤكد أن الذكاء **الاصطناعي لا يقتصر دوره على الكشف والمعالجة**، بل يمتد أيضًا إلى **تحقيق الاستمرارية في الرقابة وتحسين القدرة المؤسسية على التكيّف مع التهديدات المتجددة في مجال الجرائم المالية**.

ويلاحظ في **الجدول رقم (20)** أن **العبارة رقم (4)** قد حصلت على **أعلى المتوسطات الحسابية**، حيث بلغ **(4.12)** و**بانحراف معياري (0.587)**، و**نسبة مئوية** بلغت **(82.40%)** وجاءت بدرجة **(مرتفعة)**، في حين حصلت **العبارة رقم (7)** على **أدنى المتوسطات الحسابية**، حيث بلغ **(3.67)**، و**بانحراف معياري** بلغ **(0.541)**، و**نسبة مئوية** بلغت **(73.27%)** وجاءت بدرجة **(مرتفعة)**.

وكما يتضح من **ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح** نجد تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "**تسهم تقنيات التعلم العميق في التعرف على تغيرات في أساليب الجرائم المالية**" بنسبة **(82.40%)** وصولاً إلى عبارة: "**تسهل أدوات الذكاء الاصطناعي عملية تتبع الأداء في إدارة مخاطر الجرائم المالية**" بنسبة **(73.27%)**.

وكما سبق أن أوضحنا، يُعد تحليل المتوسطات الحسابية والانحرافات المعيارية أداة تحليلية مهمة لفهم اتجاهات استجابات المشاركين حول **مدى تأثير الذكاء الاصطناعي** على **بُعد مراقبة ومراجعة مخاطر الجريمة المالية**؛ إذ يُسهم هذا التحليل في إبراز **الجوانب التي تحظى بدرجة عالية من القبول**، مقابل تلك التي قد **تتطلب اهتمامًا أكبر أو تطويرًا إضافيًا**، وبناءً على ذلك يعني حصول **العبارة رقم (4): "تسهم تقنيات التعلم العميق في التعرف على التغيرات في أساليب ارتكاب الجرائم المالية "على أعلى متوسط حسابي بين العبارات المرتبطة بهذا البُعد** وجود **اتفاق واسع بين المشاركين حول أهمية تقنيات التعلم العميق في رصد وتحليل الأنماط المتغيرة للجرائم المالية**، كما يعكس **إدراكًا إيجابيًا لإمكانات الذكاء الاصطناعي في دعم عمليات المراقبة المستمرة ومراجعة المخاطر بشكل أكثر دقة واستباقية**.

في المقابل، فإن حصول **العبارة رقم (7): "تسهل أدوات الذكاء الاصطناعي عملية تتبع الأداء في إدارة مخاطر الجرائم المالية "** على أدنى ترتيب من حيث المتوسط الحسابي يُشير بوضوح إلى **ضعف نسبي في مستوى القبول أو التوافق بشأن فاعلية هذه الأدوات في هذا المجال المحدد**، وقد يُعزى ذلك إلى **محدودية استخدام أدوات التتبع الذكية بشكل فعلي في المؤسسات المصرفية** أو **غياب آليات واضحة لتقييم تأثيرها المباشر على الأداء الرقابي**.

ويرى الباحث إنه يمكن استخلاص عدد من الدلالات من هذه النتائج كالتالي:

1. **تمييز التطبيقات الفاعلة:** تُشير **النتائج المرتفعة** لعبارات **مثل العبارة (4)** إلى **وجود وعي متقدم بقيمة تقنيات الذكاء الاصطناعي**، خاصة **التعلم العميق**، في **كشف التغيرات السلوكية للجريمة المالية**؛ ما يدعم **التوسع في استخدامها ضمن عمليات المراقبة المستمرة.**
2. **رصد جوانب التحسين: النتائج المنخفضة** للعبارات مثل **العبارة (7)** تُبرز **الحاجة إلى تعزيز أدوات الذكاء الاصطناعي المستخدمة في تتبع الأداء**، سواء من **خلال تطوير قدراتها التقنية** أو **تعزيز توظيفها ضمن نظم الرقابة المؤسسية.**
3. **توجيه الخطط التطويرية:** تمثل هذه المؤشرات **مرشدًا عمليًا لصنّاع القرار في المجال المصرفي لتحديد الأولويات، والتركيز على التقنيات التي أثبتت فاعليتها**، والعمل على **سد الفجوات التي كشفت عنها نتائج الدراسة.**

وعليه، فإن تحليل استجابات المشاركين حول هذا البُعد لا يقتصر على عرض بيانات وصفية، بل يُقدم **منظورًا تحليليًا وإستراتيجيًا** يُسهم في **توجيه الاستخدام الأمثل للذكاء الاصطناعي في تعزيز كفاءة مراقبة ومراجعة إدارة مخاطر الجريمة المالية.**

ثالثا: اختبار فروض الدراسة:

تُعدّ الفروض بمثابة الحلول أو المقترحات التي تعالج مختلف جوانب المشكلة التي تمثل مرتكز الدراسة، ومن ثمَّ يمكن القول بأن الفروض هي القرارات التي يتخذها الباحث كحلول لمشكلة دراسته، بناء على المعلومات المحسوبة من عينة الدراسة بالأساليب الإحصائية المتبعة، ومن ثم يجب عليه اتخاذ هذه القرارات بأقل قدر ممكن من الخطأ، ويتناول هذا الجزء اختبار فروض الدراسة كما يلي:

1.التوزيع الطبيعي لمتغيرات الدراسة:

قبل الشروع في إجراء التحليل الإحصائي لاختبار فروض الدراسة، حرص الباحث على **التحقق من طبيعة توزيع البيانات** التي تم جمعها من أفراد العينة، وذلك من خلال اختبار ما إذا كانت **تتبع التوزيع الطبيعي** أم لا؛ وذلك نظرًا لما يترتب على ذلك من قرارات منهجية تتعلق بنوع التحليل المستخدم، ويُقصد بالتوزيع الطبيعي أن تتوزع القيم حول المتوسط بشكل متماثل يشبه شكل الجرس (المنحنى الطبيعي)، حيث تكون معظم القيم متركزة قرب المتوسط، وتقل تدريجيًا باتجاه الأطراف على نحو متوازن، ويُعرف هذا النمط من التوزيع أيضًا باسم **"توزيع جاوس"**، ويُعد شرطًا أساسيًا لاعتماد العديد من **الاختبارات الإحصائية المعلمية.**

وفي المقابل، فإن **عدم خضوع البيانات للتوزيع الطبيعي** يعني أنها تتوزع بصورة غير متماثلة، كأن تكون مائلة باتجاه معين، أو تحتوي على ذيول طويلة، أو تتضمن قيمًا شاذة؛ مما يُؤثر على دقة بعض الأساليب الإحصائية، وفي هذه الحالة قد يُلجأ إلى استخدام **الاختبارات غير المعلمية**، التي لا تفترض وجود توزيع طبيعي للبيانات.

وتنبع أهمية التحقق من التوزيع الطبيعي من كون **الاختبارات المعلمية**، مثل اختبار (t) وتحليل التباين (ANOVA)، تعتمد في فرضياتها الأساسية على كون البيانات تتبع هذا التوزيع، وهو ما يُكسبها قدرة عالية على الكشف عن الفروق والعلاقات بدقة وموثوقية إحصائية مرتفعة، أما **الاختبارات غير المعلمية**، كاختبار مان-ويتني أو كاي-تربيع، فرغم فائدتها عند عدم تحقق شروط الاختبارات المعلمية، إلا أنها تكون في العادة **أقل حساسية ودقة** عندما تكون البيانات طبيعية؛ مما يجعل استخدامها في غير موضعه يؤدي إلى فقدان جزء من القوة التفسيرية والدقة في النتائج.

وبناءً على ما سبق، تُعد **اختبارات التحقق من التوزيع الطبيعي** خطوة حاسمة في اختيار الأسلوب الإحصائي الأنسب، لضمان صحة الفرضيات وجودة الاستنتاجات في الدراسة

ويوضح **الجدول رقم (21)** نتائج الاختبار الذي قام به الباحث في هذا الصدد، حيث إن القيمة الاحتمالية لكل بُعد **أكبر من 0.05**، وهذا يدل على أن **البيانات تتبع التوزيع الطبيعي، ويجب استخدام الاختبارات المعلمية**، وقد قام الباحث باختبار التوزيع الطبيعي للبيانات باستخدام اختبار **كلو مجروف – سيمنروف (Smirnova-Kolmogorov)**، حيث إن عينة البحث **أكبر من 50:**

جدول رقم (21) اختبار التوزيع الطبيعي للبيانات

Variable	Kolmogorov-Smirnov[a]		
	Statistic	Df	Sig.
الذكاء الاصطناعي	.051	269	.494
إدارة مخاطر الجرائم المالية	.054	269	.416
a. Lilliefors Significance Correction			

المصدر: جدول التوزيع الطبيعي برنامج SPSS

ويتضح من **الجدول رقم (21)** أن **قيمة (Sig)** في اختباري **(Kolmogorov-Smirnov) أكبر من (0.05)**، وعليه سيتم **استخدام الأساليب الإحصائية المعلمية في اختبار فروض الدراسة**.

2.اختبار فروض الدراسة:

قامت الدراسة على إثبات صحة أو نفي الفروض التالية:

الفرض الرئيس للدراسة:

يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ولإثبات صحة **الفرض الرئيس** تم **اختبار صحة الفروض الفرعية** التالية:

أ. الفرض الفرعي الأول:

(H1) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ولإثبات صحة الفرضية الفرعية الأولى السابقة، قام الباحث بإجراء الاختبارات التالية:

أولاً: اختبار الانحدار الخطي البسيط بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (تحديد مخاطر الجريمة المالية)، وكانت النتائج كما يلي:

جدول رقم (22) يوضح نتائج اختبارات الفرضية الفرعية الأولى لقياس تأثير الذكاء الاصطناعي على تحديد مخاطر الجريمة المالية

المتغير التابع	الارتباط (R)	معامل التحديد R^2	التغير في معامل التحديد R^2	المحسوبة F	مستوى الدلالة Sig	درجات الحرية DF	معامل الانحدار β	المحسوبة T	مستوى الدلالة Sig

تحديد مخاطر الجريمة المالية	.724[a]	.524	.524	261.60	0.01	الانحدار	1	.770	16.17	0.01
						البواقي	268			
						المجموع	269			

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (22) وجود تأثير للذكاء الاصطناعي** على **تحديد مخاطر الجريمة المالية**؛ إذ بلغ **معامل الارتباط R (.724[a]) عند مستوى معنوية 0.01**، أما **معامل التحديد R^2** فقد بلغ (.524)، أي أن **ما قيمته (.524) من التغير في تحديد مخاطر الجريمة المالية ناتج عن التغير في الذكاء الاصطناعي**، كما بلغت **قيمة درجة التأثير β (77.0%)**، وتؤكد **معنوية هذا التأثير قيمة F المحسوبة** والتي بلغت **(261.609)** وهي **دالة عند مستوى معنوية 0.01**، كما بلغت **قيمة T المحسوبة (16.174)** وهي **دالة عند مستوى معنوية 0.01، وهو ما يعكس وجود تأثير جوهري للمتغير المستقل (الذكاء الاصطناعي)** على **(تحديد مخاطر الجريمة المالية)**، كما يشير ذلك أيضا إلى **أن هذا التأثير لا يمكن أن يصل إلى الصفر، بمعنى** وجود **تأثير جوهري**، وهو تأثير لا يمكن اعتباره **طفيفًا أو عارضًا**، بل **يُعد دالاً من الناحيتين الإحصائية والتطبيقية**؛ فعدم اقتراب هذا التأثير من الصفر يُشير إلى **قوته وفاعليته**، ويُعزز من **صحة الفرضية** التي ترى أن **الذكاء الاصطناعي يلعب دورًا فعّالاً في رفع دقة وكفاءة تحديد مخاطر الجريمة المالية** داخل المؤسسات المصرفية، وتؤكد هذه النتيجة **أن العلاقة بين المتغير المستقل (الذكاء الاصطناعي) وبُعد تحديد المخاطر ليست علاقة عشوائية أو ناتجة عن الصدفة، بل تعكس ارتباطًا حقيقيًا يسهم في تفسير التغيرات ذات الصلة بهذا الجانب الحاسم من إدارة المخاطر**.

ومن وجهة نظر الباحث، فإن هذه النتيجة تُبرز الأهمية العملية للذكاء الاصطناعي كأداة فاعلة في **التعرف المبكر على المخاطر وتوجيه الجهود الرقابية بفعالية أعلى**؛ مما يُعزز **موثوقية الدراسة**، ويُؤكد على **أن نتائجها تستند إلى معطيات و اقعية قابلة للتطبيق في بيئة العمل المصرفي**.

كما يُعدّ خط الانحدار ملائمًا للبيانات ومعبرًا عن العلاقة بين المتغيرات، ويتضح ذلك من قيمة معنوية الاختبار؛ مما يعكس القوة التفسيرية العالية لنموذج الانحدار الخطي البسيط من الناحية الإحصائية.

مما سبق يمكن صياغة **معادلة الانحدار الخطي البسيط** التي تحكم العلاقة بين **المتغير المستقل (الذكاء الاصطناعي)** و**المتغير التابع (تحديد مخاطر الجريمة المالية)** على النحو التالي:

الذكاء الاصطناعي = الثابت +.770 (تحديد مخاطر الجريمة المالية).

مما سبق يتم قبول الفرض الفرعي الأول:

(H1) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ب. الفرض الفرعي الثاني:

(H2) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ولإثبات صحة الفرضية السابقة قام الباحث بإجراء الاختبارات التالية:

أولاً: اختبار الانحدار الخطي البسيط بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (تحليل وتقييم مخاطر الجريمة المالية)، وكانت النتائج كما يلي:

جدول رقم (23) يوضح نتائج اختبارات الفرضية الفرعية الثانية لقياس تأثير الذكاء الاصطناعي على تحليل وتقييم مخاطر الجريمة المالية

المتغير التابع	الارتباط (R)	معامل التحديد R^2	التغير في معامل التحديد R^2	المحسوبة F	مستوى الدلالة Sig	درجات الحرية DF		معامل الانحدار β	المحسوبة T	مستوى الدلالة Sig
تحليل وتقييم مخاطر الجريمة المالية	.797[a]	.635	.635	414.76	0.01	الانحدار	1	.827	20.36	0.01
						البواقي	268			
						المجموع	269			

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من الجدول رقم (23) وجود تأثير للذكاء الاصطناعي على تحليل وتقييم مخاطر الجريمة المالية؛ إذ بلغ معامل الارتباط R (.797[a]) عند مستوى معنوية 0.01، أما معامل التحديد R^2 فقد بلغ (.635)، أي أن ما قيمته (.635) من التغير في تحليل وتقييم مخاطر الجريمة المالية ناتج عن التغير في الذكاء الاصطناعي، كما بلغت قيمة درجة التأثير β (82.7%)، وتؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت (414.762) وهي دالة عند مستوى معنوية 0.01، كما بلغت قيمة T المحسوبة (20.366) وهي دالة عند مستوى معنوية 0.01، وهو ما يعكس وجود تأثير جوهري للمتغير المستقل (الذكاء الاصطناعي) على (تحليل وتقييم مخاطر الجريمة المالية)، وهو تأثير لا يُمكن تجاهله أو اعتباره ضئيلاً؛ إذ لا يقترب من الصفر، مما يُعزز من الفرضية القائلة بأن هذا التأثير حقيقي وفعّال، ويُفهم من ذلك أن الذكاء الاصطناعي يُسهم بشكل ملحوظ في تحسين جودة ودقة عمليات التحليل والتقييم لمخاطر الجريمة المالية، من خلال قدرته على معالجة كميات ضخمة من البيانات، واكتشاف الأنماط غير الاعتيادية، والتنبؤ بالسلوكيات المشبوهة بكفاءة عالية، وتؤكد هذه النتيجة أن العلاقة بين الذكاء الاصطناعي وتحليل وتقييم المخاطر ليست علاقة عشوائية أو نتيجة خطأ إحصائي، بل هي علاقة ذات دلالة علمية تُعكس في الأداء العملي للمؤسسات المصرفية.

ومن منظور الباحث، تُبرز هذه النتيجة الدور الحيوي للذكاء الاصطناعي في دعم اتخاذ القرار وتقليل التقدير الخاطئ لمخاطر الجريمة المالية، مما يمنح الدراسة موثوقية أكبر، ويضفي على نتائجها قيمة تفسيرية قابلة للتطبيق في بيئات مصرفية تعتمد على الدقة والاستباقية في إدارة مخاطر الجريمة المالية.

كما يُعدّ خط الانحدار ملائمًا للبيانات ومعبرًا عن العلاقة بين المتغيرات، ويتضح ذلك من قيمة معنوية الاختبار؛ مما يعكس القوة التفسيرية العالية لنموذج الانحدار الخطي البسيط من الناحية الإحصائية.

مما سبق يمكن صياغة معادلة الانحدار الخطي البسيط التي تحكم العلاقة بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (تحليل وتقييم مخاطر الجريمة المالية) على النحو التالي:

الذكاء الاصطناعي = الثابت +.827 (تحليل وتقييم مخاطر الجريمة المالية).

مما سبق يتم قبول الفرض الفرعي الثاني:

(H2) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ج. الفرض الفرعي الثالث:

(H3) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في معالجة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ولإثبات صحة الفرضية السابقة قام الباحث بإجراء الاختبارات التالية:

أولاً: اختبار الانحدار الخطي البسيط بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (معالجة مخاطر الجريمة المالية)، وكانت النتائج كما يلي:

جدول رقم (24) يوضح نتائج اختبارات الفرضية الفرعية الثالثة لقياس تأثير للذكاء الاصطناعي على معالجة مخاطر الجريمة المالية

المتغير التابع	الارتباط (R)	معامل التحديد R^2	التغير في معامل التحديد R^2	المحسوبة F	مستوى الدلالة Sig	درجات الحرية DF		معامل الانحدار β	المحسوبة T	مستوى الدلالة Sig
معالجة مخاطر الجريمة المالية	.772[a]	.596	.596	351.51	0.01	الانحدار	1	.829	18.74	0.01
						البواقي	268			
						المجموع	269			

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (24) وجود تأثير للذكاء الاصطناعي على معالجة مخاطر الجريمة المالية**؛ إذ بلغ **معامل الارتباط R (.772[a]) عند مستوى معنوية 0.01**، أما **معامل التحديد R^2** فقد بلغ **(.596)**، أي أن **ما قيمته (.596) من التغير في معالجة مخاطر الجريمة المالية ناتج عن التغير في الذكاء الاصطناعي**، كما بلغت **قيمة درجة التأثير β (82.9%)**، **وتؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت (351.515)، وهي دالة عند مستوى معنوية 0.01**، كما بلغت **قيمة T المحسوبة (18.749)، وهي دالة عند مستوى معنوية 0.01، وهو ما يعكس وجود تأثير جوهري للمتغير المستقل (الذكاء الاصطناعي)** على **(معالجة مخاطر الجريمة المالية)**، وهو تأثير **لا يمكن اعتباره طفيفًا أو عرضيًا؛ إذ لم يقترب من الصفر**، مما **يُعزز من الفرضية** القائلة بأن هذا التأثير **فعّال وحقيقي من الناحيتين الإحصائية والتطبيقية**، ويُستدل من ذلك على أن **الذكاء الاصطناعي يُسهم بشكل مباشر في تعزيز قدرة المؤسسات المصرفية على التصدي الفوري والفعّال لمخاطر الجرائم المالية** من خلال أدوات ذكية تتيح سرعة الاستجابة، والتعامل مع الحالات المشبوهة، وتفعيل الإجراءات التصحيحية تلقائيًا أو بشكل شبه تلقائي، وتُشير هذه النتيجة إلى أن **العلاقة بين الذكاء الاصطناعي وفاعلية معالجة المخاطر ليست نتيجة صدفة أو تباين غير مفسر**، بل تمثل **ارتباطًا ذا دلالة واضحة يعكس الدور المحوري للتقنيات الذكية في دعم إستراتيجيات إدارة المخاطر التشغيلية والامتثال.**

ومن وجهة نظر الباحث، تُعد هذه النتيجة مؤشرًا قويًا على أن الذكاء الاصطناعي لا يقتصر دوره على الكشف والتحليل فحسب، بل يمتد أيضًا ليشمل **مرحلة التدخل والمعالجة الفعلية للمخاطر**، وهو ما يمنح نتائج الدراسة **موثوقية أكبر**، **ويُعززمن قابليتها للتطبيق العملي في البيئات المصرفية المختلفة**.

كما يُعدّ خط الانحدارملائمًا للبيانات ومعبرًا عن العلاقة بين المتغيرات، ويتضح ذلك من قيمة معنوية الاختبار؛ مما يعكس القوة التفسيرية العالية لنموذج الانحدارالخطي البسيط من الناحية الإحصائية.

مما سبق يمكن صياغة **معادلة الانحدارالخطي البسيط** التي تحكم العلاقة بين **المتغيرالمستقل (لذكاء الاصطناعي)** و**المتغير التابع (معالجة مخاطرالجريمة المالية)** على النحو التالي:

الذكاء الاصطناعي = الثابت +.829 (معالجة مخاطرالجريمة المالية).

مما سبق يتم قبول الفرض الفرعي الثالث:

H3 يوجد تأثيرذودلالة معنوية لاستخدام الذكاء الاصطناعي في معالجة مخاطرالجريمة المالية في مؤسسات القطاع المصرفي القطري.

د. الفرض الفرعي الرابع:

(H4) يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ولإثبات صحة الفرضية السابقة قام الباحث بإجراء الاختبارات التالية:

أولاً: اختبار الانحدار الخطي البسيط بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (مراقبة ومراجعة مخاطر الجريمة المالية)، وكانت النتائج كما يلي:

جدول رقم (25) يوضح نتائج اختبارات الفرضية الفرعية الرابعة لقياس تأثيرللذكاء الاصطناعي على مراقبة ومراجعة مخاطرالجريمة المالية

المتغيرالتابع	الارتباط (R)	معامل التحديد R^2	التغيرفي معامل التحديد R^2	المحسوبة F	مستوى الدلالة Sig	درجات الحرية DF		معامل الانحدار β	المحسوبة T	مستوى الدلالة Sig
مراقبة ومراجعة مخاطرالجريمة المالية	.811[a]	.658	.658	380.44	0.01	الانحدار	1	.883	19.22	0.01
						البواقي	268			
						المجموع	269			

المصدر: من إعداد الباحث من بيانات الدراسة الميدانية، مخرجات SPSS 29.0.1

يتضح من **الجدول رقم (25)** وجود تأثير **للذكاء الاصطناعي على مراقبة ومراجعة مخاطر الجريمة المالية**؛ إذ بلغ **معامل الارتباط R (.811[a])** عند **مستوى معنوية 0.01**، أما **معامل التحديد R^2** فقد بلغ **(.658)**، أي أن ما قيمته **(.658)** من **التغيرفي مراقبة ومراجعة مخاطرالجريمة المالية ناتج عن التغيرفي لذكاء الاصطناعي**، كما بلغت **قيمة درجة التأثير β (88.3%)**، وتؤكد **معنوية هذا التأثير قيمة F المحسوبة والتي بلغت (380.445)**، وهي **دالة عند مستوى معنوية 0.01**، كما **بلغت قيمة T المحسوبة (19.222)**، وهي **دالة عند مستوى معنوية 0.01**، وهو **ما يعكس وجود تأثير جوهري للمتغير المستقل(الذكاء**

الاصطناعي) على **(مراقبة ومراجعة مخاطر الجريمة المالية)**، وهو تأثير **لا يُمكن اعتباره هامشيًا أو عارضًا؛ إذ لم يقترب من الصفر**، مما يدل على أن هذا التأثير **حقيقي وذو دلالة إحصائية واضحة**، ويُفهم من ذلك أن **الذكاء الاصطناعي يُسهم بشكل فعّال في تعزيز كفاءة عمليات المراقبة المستمرة والمراجعة الدورية لمخاطر الجريمة المالية** من خلال أدوات ذكية تتيح الرصد اللحظي للتغيرات، وتحليل البيانات المتجددة، وتوليد تقارير تنبيهية تساعد في اتخاذ قرارات رقابية أكثر دقة واستباقية، وهذا يدل على أن **العلاقة بين الذكاء الاصطناعي وقدرة المؤسسات المصرفية على مراقبة وتحديث إستراتيجياتها في مواجهة الجريمة المالية ليست علاقة عشوائية**، بل **علاقة منهجية قائمة على تأثير واضح وملموس.**

ومن منظور الباحث، فإن هذه النتيجة تبرز **الدور المستدام للذكاء الاصطناعي في تمكين المؤسسات المصرفية من التكيف السريع مع التهديدات المتغيرة وتطوير نماذج الرقابة الداخلية**، وهو ما **يُكسب الدراسة قيمة تطبيقية عالية ويعزز من موثوقية نتائجها**، ويؤكد أن ما تم التوصل إليه **يُعبر عن واقع عملي يمكن البناء عليه في السياسات المصرفية المستقبلية.**

كما يُعدّ خط الانحدار ملائمًا للبيانات ومعبرًا عن العلاقة بين المتغيرات، ويتضح ذلك من قيمة معنوية الاختبار؛ مما يعكس القوة التفسيرية العالية لنموذج الانحدار الخطي البسيط من الناحية الإحصائية.

مما سبق يمكن صياغة **معادلة الانحدار الخطي البسيط** التي تحكم العلاقة بين **المتغير المستقل (لذكاء الاصطناعي) والمتغير التابع (مراقبة ومراجعة مخاطر الجريمة المالية)** على النحو التالي:

الذكاء الاصطناعي = الثابت +.883 (مراقبة ومراجعة مخاطر الجريمة المالية).

مما سبق يتم قبول الفرض الفرعي الرابع:

H4 يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري

مما سبق يتم قبول الفرض الرئيس للدراسة:

يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

وفي ضوء التحليل السابق، والذي بيّنت نتائجه وجود تأثير إحصائي معنوي لاستخدام تقنيات الذكاء الاصطناعي في مختلف مراحل إدارة مخاطر الجريمة المالية، بما يشمل: التحديد، التحليل التقييم، المعالجة، المراقبة والمراجعة داخل مؤسسات القطاع المصرفي القطري، فإن ذلك يدعم قبول الفرضية الرئيسية والفرضيات الفرعية للدراسة، ويُعد هذا التأثير مؤشرًا واضحًا على فاعلية الذكاء الاصطناعي كأداة رئيسية تسهم في تعزيز كفاءة أنظمة الرقابة والحد من مستويات التعرض للمخاطر.

ومن خلال هذه النتائج وتحليلها، يرى الباحث أن الذكاء الاصطناعي يمثل عنصرًا إستراتيجيًا لا غنى عنه في تطوير آليات الحوكمة وإدارة الامتثال في البنوك، بما يسهم في تحسين الأداء المؤسسي وضمان استدامة القطاع المالي، كما أن الدلالة الإحصائية للنتائج تعزز من قناعة الباحث بأهمية توسيع نطاق تطبيقات الذكاء الاصطناعي وتكاملها ضمن السياسات والإجراءات التشغيلية للمؤسسات المالية، مما يعزز قدرتها على مواجهة التهديدات المتنامية في بيئة الأعمال الرقمية.

الفصل الرابع

نتائج وتوصيات الدراسة

- مقدمة
- نتائج الدراسة
- تحليل نتائج الدراسة
- توصيات الدراسة
- صعوبات (محددات) الدراسة
- دراسات مستقبلية مقترحة

الفصل الرابع
نتائج وتوصيات الدراسة

مقدمة:

يُشكّل هذا الفصل المرحلة الختامية من الدراسة، حيث يتم تلخيص أبرز النتائج التي توصل إليها الباحث استنادًا إلى التحليل الإحصائي للبيانات الميدانية، بما يعكس مدى تحقق أهداف الدراسة والإجابة عن تساؤلاتها الرئيسة، وقد تم بناء هذا الفصل على ما سبق عرضه من نتائج تطبيقية وإطار نظري ومنهجي، بما يضمن التكامل بين مختلف مراحل البحث، ويتيح استخلاص مؤشرات دقيقة حول العلاقة بين الذكاء الاصطناعي وإدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

ويتضمن هذا الفصل عرضًا موجزًا لأهم النتائج، مع تحليل لأبرز دلالاتها العلمية والعملية، وبيان انعكاساتها على الواقع المصرفي المحلي في ضوء متطلبات الحوكمة والامتثال لمعايير مكافحة الجرائم المالية. كما يعرض هذا الفصل أيضا مجموعة من التوصيات العملية الموجهة إلى صانعي القرار في القطاع المصرفي والجهات الرقابية، إضافة إلى اقتراحات بحثية مستقبلية يمكن أن تُسهم في تطوير الدراسات في هذا المجال.

ويسعى الباحث - من خلال هذا الفصل - إلى ربط النتائج النظرية والتطبيقية بإطارها العملي، وصولاً إلى صياغة مقترحات قابلة للتنفيذ تسهم في تعزيز توظيف تقنيات الذكاء الاصطناعي كأداة فعّالة في إدارة مخاطر الجريمة المالية، وسيتم تحقيق أهداف هذا الفصل من خلال مناقشة العناصر التالية:

أولا: نتائج الدراسة.

ثانيا: تحليل نتائج الدراسة.

ثالثا: توصيات الدراسة.

رابعا: محددات (صعوبات الدراسة).

خامسا: دراسات مستقبلية مقترحة.

أولا: نتائج الدراسة:

بعد استكمال إجراءات جمع البيانات وتحليلها باستخدام الأساليب الإحصائية المناسبة، تبيّن عدد من النتائج المهمة التي تُسهم في الإجابة عن أسئلة الدراسة والتحقق من فروضها. ويستعرض الباحث - فيما يلي - أبرز النتائج التي تم التوصل إليها، **مرتبة وفق محاور الدراسة ومجالاتها الرئيسة**، بما يُسهم في توضيح طبيعة العلاقة بين المتغيرات محل البحث، ومدى تحقق أهداف الدراسة.

1. أشارت الدرجة الكلية للتحليل الوصفي إلى أن درجة بُعد الذكاء الاصطناعي لعينة الدراسة (مرتفعة)، حيث بلغ المتوسط الحسابي للدرجة الكلية لبُعد الذكاء الاصطناعي (3.73) وبانحراف معياري (0.379) ونسبة مئوية بلغت (74.69%)؛ مما يدل على انخفاض التشتت في آراء عينة الدراسة وتقارب الآراء.
2. اتضح من ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "يتيح الذكاء الاصطناعي التوليدي تصميم نماذج وتوقعات دقيقة لمخاطر الجرائم المالية" بنسبة (85.78%)، وصولاً إلى عبارة: "تسهم الأتمتة الروبوتية في تقليل الأخطاء البشرية وتحسين سرعة استجابة المؤسسات لمخاطر الجرائم المالية" بنسبة (68.00%).
3. أشارت الدرجة الكلية الخاصة بالمتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة تجاه عبارات بُعد تحديد مخاطر الجريمة المالية إلى أن درجة بُعد تحديد مخاطر الجريمة المالية لعينة الدراسة (مرتفعة)، حيث بلغ المتوسط

الحسابي للدرجة الكلية لبُعد تحديد مخاطر الجريمة المالية (3.96) وبانحراف معياري (0.669) ونسبة مئوية بلغت (79.18%)؛ مما يدل على انخفاض التشتت في آراء عينة الدراسة وتقارب الآراء.

4. اتضح من ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "تسهم نظم الذكاء الاصطناعي في التعرف المبكر على مؤشرات الجرائم المالية" بنسبة (84.15%)، وصولاً إلى عبارة: "يُحسن الاعتماد على النظم الخبيرة من عملية تحديد المخاطر المحتملة" بنسبة (76.89%).

5. أظهرت المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة تجاه عبارات بُعد تحليل وتقييم مخاطر الجريمة المالية أن درجة بُعد تحليل وتقييم مخاطر الجريمة المالية لعينة الدراسة (مرتفعة)، حيث بلغ المتوسط الحسابي للدرجة الكلية لبُعد تحليل وتقييم مخاطر الجريمة المالية (3.825) وبانحراف معياري (683.0) ونسبة مئوية بلغت (76.50%)؛ مما يدل على انخفاض التشتت في آراء عينة الدراسة وتقارب الآراء.

6. كما اتضح من ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "تقلل أدوات الذكاء الاصطناعي من الاعتماد على التقديرات الشخصية في تقييم المخاطر" بنسبة (82.67%)، وصولاً إلى عبارة: "تسهل نظم الذكاء الاصطناعي تقييم درجة خطورة كل خطر مالي" بنسبة (72.19%).

7. أشارت الدرجة الكلية الخاصة بالمتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة تجاه عبارات بُعد معالجة مخاطر الجريمة المالية إلى أن درجة بُعد معالجة مخاطر الجريمة المالية لعينة الدراسة (مرتفعة)، حيث بلغ المتوسط الحسابي للدرجة الكلية لبُعد معالجة مخاطر الجريمة المالية (3.73) وبانحراف معياري (0.594) ونسبة مئوية بلغت (74.57%)؛ مما يدل على انخفاض التشتت في آراء عينة الدراسة وتقارب الآراء.

8. كما اتضح من ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "يقلل استخدام الروبوتات في العمليات من احتمالية التلاعب المالي" بنسبة (80.00%)، وصولاً إلى عبارة: "تدعم أنظمة الذكاء الاصطناعي وضع خطط استجابة مرنة للمخاطر المكتشفة" بنسبة (71.14%).

9. أظهرت المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة تجاه عبارات بُعد مراقبة ومراجعة مخاطر الجريمة المالية أن درجة بُعد مراقبة ومراجعة مخاطر الجريمة المالية لعينة الدراسة (مرتفعة)، حيث بلغ المتوسط الحسابي للدرجة الكلية لبُعد معالجة مخاطر الجريمة المالية (3.82) وبانحراف معياري (0.511) ونسبة مئوية بلغت (76.37%)؛ مما يدل على انخفاض التشتت في آراء عينة الدراسة وتقارب الآراء.

10. كما اتضح من ترتيب أهمية العبارات المبنية على المتوسط المئوي المرجح تدرج أهمية العبارات لعينة الدراسة، حيث ترى عينة الدراسة مدى أهمية عبارة: "تسهم تقنيات التعلم العميق في التعرف على تغيرات في أساليب الجرائم المالية" بنسبة (82.40%)، وصولاً إلى عبارة: "تسهل أدوات الذكاء الاصطناعي عملية تتبع الأداء في إدارة مخاطر الجرائم المالية" بنسبة (73.27%).

11. يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

12. يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحديد مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

13. يمكن صياغة معادلة الانحدار الخطي البسيط التي تحكم العلاقة بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (تحديد مخاطر الجريمة المالية) على النحو التالي: الذكاء الاصطناعي = الثابت +.770 (تحديد مخاطر الجريمة المالية).

14. يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في تحليل وتقييم مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.

15. يمكن صياغة معادلة الانحدار الخطي البسيط التي تحكم العلاقة بين المتغير المستقل (الذكاء الاصطناعي) والمتغير التابع (تحليل وتقييم مخاطر الجريمة المالية) على النحو التالي: الذكاء الاصطناعي = الثابت +.827 (تحليل وتقييم مخاطر الجريمة المالية).
16. يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في معالجة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.
17. يمكن صياغة معادلة الانحدار الخطي البسيط التي تحكم العلاقة بين المتغير المستقل (لذكاء الاصطناعي) والمتغير التابع (معالجة مخاطر الجريمة المالية) على النحو التالي: لذكاء الاصطناعي = الثابت +.829 (معالجة مخاطر الجريمة المالية).
18. يوجد تأثير ذو دلالة معنوية لاستخدام الذكاء الاصطناعي في مراقبة ومراجعة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري.
19. يمكن صياغة معادلة الانحدار الخطي البسيط التي تحكم العلاقة بين المتغير المستقل (لذكاء الاصطناعي) والمتغير التابع (مراقبة ومراجعة مخاطر الجريمة المالية) على النحو التالي: الذكاء الاصطناعي = الثابت +.883 (مراقبة ومراجعة مخاطر الجريمة المالية).

ثانيا: تحليل نتائج الدراسة:

أظهرت نتائج الدراسة الدلالات العلمية والعملية التالية، فيما يتعلق بتأثير الذكاء الاصطناعي على إدارة مخاطر الجريمة المالية في مؤسسات القطاع المصرفي القطري:

1. هناك قبول واسع داخل المؤسسات المصرفية القطرية لاستخدام تقنيات الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية بسبب دورها في تحسين الفاعلية التشغيلية.
2. بالرغم من الثقة العالية بفوائد الذكاء الاصطناعي، فإن المشاركين يدركون وجود تحديات مرتبطة بتطبيقه، مثل التكلفة وأمن البيانات.
3. يسهم الذكاء الاصطناعي في توفير الشفافية وتعزيز الثقة في أنظمة الرقابة الداخلية.
4. يسهم الذكاء الاصطناعي في رفع مستوى الكفاءة داخل القطاع المصرفي؛ حيث يعزز القدرة على التنبؤ بمخاطر الجرائم المالية بدقة أكبر، مع فوائده التي تفوق المخاطر المرتبطة باستخدامه.
5. يحسن الذكاء الاصطناعي من دقة تحديد مؤشرات الجرائم المالية المحتملة؛ مما يساعد على الاكتشاف المبكر وتقليل فرص وقوعها.
6. يستطيع الذكاء الاصطناعي تحليل كميات ضخمة من البيانات بسرعة ودقة، بما يؤدي إلى تنبؤات أفضل بمستويات مخاطر الجرائم المالية.
7. يقلل الاعتماد على الذكاء الاصطناعي من التقديرات الشخصية عند تحليل وتقييم مخاطر الجرائم المالية؛ مما يعزز موضوعية القرارات.
8. يساعد الذكاء الاصطناعي في اكتشاف أنماط خفية للجرائم المالية قد لا يتمكن المحللون البشريون من رصدها.
9. يمتلك الذكاء الاصطناعي قدرة ديناميكية على التكيف مع تغير أساليب الجرائم المالية وتعلم كيفية مواجهتها بمرور الوقت.
10. يسهم الذكاء الاصطناعي في أتمتة العمليات المصرفية المرتبطة بإدارة مخاطر الجرائم المالية؛ مما يقلل من الأخطاء البشرية ويُحسن من سرعة الاستجابة.
11. يعزز الذكاء الاصطناعي من قدرة المؤسسات على معالجة مخاطر الجرائم المالية عبر تطوير خطط استجابة أكثر مرونة.
12. تسهم تقنيات التعلم العميق في مراقبة ومراجعة مخاطر الجرائم المالية من خلال رصد التغيرات المستمرة في أنماطها.

13. أثبتت النتائج وجود تأثير معنوي واضح للذكاء الاصطناعي على جميع أبعاد إدارة مخاطر الجرائم المالية (التحديد، التحليل والتقييم، المعالجة، المراقبة والمراجعة).
14. أوضحت معادلات الانحدار الخطي أن أقوى تأثير للذكاء الاصطناعي كان في بُعد المراقبة والمراجعة (معامل 0.883)، يليه بُعد المعالجة (0.829)، مما يؤكد دوره الإستراتيجي في تحسين منظومة الرقابة المصرفية.
15. بشكل عام، يمكن القول إن الذكاء الاصطناعي يمثل أداة محورية في تطوير أنظمة إدارة مخاطر الجرائم المالية داخل القطاع المصرفي القطري، من خلال زيادة الدقة، تقليل الاعتماد على العنصر البشري، وتحقيق استجابة أسرع وأكثر كفاءة للتحديات المالية المعقدة.

ثالثا: توصيات الدراسة:

في ضوء النتائج التي كشفت عنها الدراسة، يختتم الباحث عمله بجملة من التوصيات العلمية والعملية الهادفة إلى تعزيز توظيف تقنيات الذكاء الاصطناعي في دعم منظومة إدارة مخاطر الجرائم المالية ضمن مؤسسات القطاع المصرفي القطري، وتنبثق هذه التوصيات من القناعة بأهمية دمج الذكاء الاصطناعي كأداة إستراتيجية قادرة على إحداث نقلة نوعية في أساليب الكشف المبكر، والتحليل الذكي للمخاطر، واتخاذ قرارات قائمة على البيانات في الوقت الحقيقي، وفي هذا السياق يقترح الباحث عددًا من الآليات التنفيذية الملائمة، التي من شأنها تيسير تفعيل تلك التوصيات على أرض الواقع، من خلال تطوير البنية التحتية الرقمية، وتأهيل الكوادر المصرفية، وتعزيز التكامل بين الأنظمة الذكية وإجراءات الامتثال التنظيمي، وتأتي هذه المقترحات ضمن إطار يسعى إلى تحقيق التوازن المنشود بين متطلبات الابتكار التكنولوجي من جهة، والضوابط الرقابية والحوكمة والشفافية من جهة أخرى، بما يضمن ترسيخ بيئة مصرفية مرنة وآمنة ومتقدمة تقنيًا في دولة قطر، ويوضح **الجدول رقم (26) أهم التوصيات التي توصل إليها الباحث.**

جدول رقم (26): توصيات الدراسة

التوصية	الهدف	آلية التنفيذ	الجهة المسئولة	الإدارات المختصة بالجهة المسئولة
إنشاء وتطوير بنية تحتية رقمية متقدمة وآمنة تدعم تطبيقات الذكاء الاصطناعي	تطوير بنية تحتية تكنولوجية متقدمة وآمنة تمكّن القطاع المصرفي القطري من تبني تطبيقات الذكاء الاصطناعي في مجال إدارة مخاطر الجرائم المالية بفعالية، مع ضمان الكفاءة التشغيلية، والامتثال التنظيمي، والحفاظ على خصوصية وأمن البيانات.	• تحديث البنية الأساسية لتكنولوجيا المعلومات، بما يشمل الخوادم، وقواعد البيانات، وأدوات المعالجة عالية الأداء، لدعم نشر وتشغيل نماذج الذكاء الاصطناعي المتقدمة. • اعتماد حلول الحوسبة السحابية الآمنة لضمان المرونة وسرعة الأداء، مع الامتثال للمعايير الوطنية للأمن السيبراني وحماية البيانات. • دمج أنظمة التحليل التنبؤي والذكاء الاصطناعي ضمن البنية المصرفية الأساسية لتعزيز القدرات التنبؤية لأنظمة المراقبة والإنذار المبكر. • تطوير شبكات الاتصالات الداخلية لضمان تدفق سلس للبيانات ومعالجة العمليات في الزمن الفعلي مع تفعيل آليات الرصد الذكي والاكتشاف المبكر للحوادث. • ضمان الاستدامة التقنية بوضع خطط دورية للتقييم والتحديث ومواكبة التقنيات الناشئة.	• مؤسسات القطاع المصرفي تحت إشراف مصرف قطر المركزي	• **في مصرف قطر المركزي:** ▪ إدارة التكنولوجيا المالية والابتكار. ▪ إدارة الإشراف على التكنولوجيا المالية. • **في المؤسسات المصرفية:** ▪ إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات. ▪ إدارات الامتثال / الالتزام ومكافحة الجرائم المالية. ▪ إدارات المخاطر.

التوصية	الهدف	آلية التنفيذ	الجهة المسئولة	الإدارات المختصة بالجهة المسئولة
زيادة الاستثمار في تطوير أنظمة ذكاء اصطناعي متكاملة متخصصة في إدارة مخاطر الجرائم المالية	تعزيز قدرة المؤسسات المصرفية على اكتشاف ومنع الجرائم المالية في الوقت الفعلي من خلال أدوات تحليل تنبؤية وتعلم آلي.	• تطوير حلول مخصصة تعتمد على الذكاء الاصطناعي، كالتعلم العميق ومعالجة اللغة الطبيعية بالتعاون مع شركات التكنولوجيا المالية FinTech. • تحديد السيناريوهات والأنماط السلوكية المرتبطة بالجرائم المالية محليا ودوليا. • التكامل مع قواعد البيانات الداخلية والخارجية (مثل بيانات العملاء، المعاملات، العقوبات).	**مؤسسات القطاع المصرفي تحت إشراف مصرف قطر المركزي**	• إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات. • إدارات الامتثال / الالتزام ومكافحة الجرائم المالية. • إدارات المخاطر.
تطبيق ضوابط أمن سيبراني متقدمة للذكاء الاصطناعي	تأمين الأنظمة الذكية من الاختراق والتلاعب لضمان نزاهة النتائج.	• اعتماد التشفير متعدد الطبقات، والتحقق الثنائي، ومراقبة الأداء. • الاحتفاظ بسجلات تدقيق دقيقة لكل إجراء. • مراجعة دورية لضوابط الوصول والتحكم.	مؤسسات القطاع المصرفي، تحت إشراف مصرف قطر المركزي	• إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات. • إدارات الشؤون القانونية. • إدارات التدقيق الداخلي. • إدارات الحوكمة.
تعزيز حماية البيانات والخصوصية	ضمان سلامة وأمن البيانات المصرفية المستخدمة في نماذج الذكاء الاصطناعي، وحماية الخصوصية وفقًا للمعايير الدولية، وضمان الامتثال لقانون حماية خصوصية البيانات الشخصية القطري (القانون رقم 13 لسنة 2016).	• إعداد سياسات خصوصية متوافقة مع القانون القطري والمعايير الدولية ذات الصلة مثلGDPR . • تطبيق سياسات صارمة لإدارة الهوية والتحقق من الأذونات والأدوار قبل الوصول إلى البيانات الحساسة. • تحديد مسؤوليات واضحة لمعالجة البيانات. • تبني بروتوكولات تشفير متقدمة.	مؤسسات القطاع المصرفي، تحت إشراف مصرف قطر المركزي	• إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات • إدارات الامتثال/ الالتزام ومكافحة الجرائم المالية) • إدارات الشؤون القانونية • إدارات المخاطر
إنشاء بروتوكولات إشراف بشري مباشر على أنظمة الذكاء الاصطناعي	ضمان التدخل البشري عند وجود قرارات عالية المخاطر أو غير عادلة.	• تدريب مشرفين بشريين على تقييم مخرجات الذكاء الاصطناعي. • تحديد حالات "التدخل الإلزامي" في النظام. • وضع آلية توثيق لكل قرار يتم تعديله يدويًا.	مؤسسات القطاع المصرفي، تحت إشراف مصرف قطر المركزي	• إدارات الامتثال / الالتزام ومكافحة الجرائم المالية • إدارات المخاطر • إدارات التدقيق الداخلي • إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات
تطوير مؤشرات أداء رئيسية (KPIs)	قياس مدى فاعلية أنظمة الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية.	• تحديد مؤشرات للأداء مثل: عدد الإنذارات الصحيحة، معدل الخطأ في التنبؤ، سرعة الاستجابة، وغيرها. • دمج مؤشرات الأداء في لوحات تحكم (Dashboards) تعرض تقارير آنية عن مسار المخاطر وتطورها.	**مؤسسات القطاع المصرفي تحت إشراف مصرف قطر المركزي**	• إدارات تكنولوجيا المعلومات وإدارة أمن المعلومات • إدارات الامتثال/ الالتزام ومكافحة الجرائم المالية • إدارات المخاطر • إدارات التدقيق الداخلي
تطوير أطر حوكمة الذكاء الاصطناعي	ضمان استخدام تقنيات الذكاء الاصطناعي في مؤسسات القطاع المصرفي	• وضع سياسات وإجراءات داخلية فعالة لاستخدام الذكاء الاصطناعي	مؤسسات القطاع المصرفي تحت إشراف حثيث وقوي من مصرف قطر المركزي في ضوء الإستراتيجية الثالثة	• إدارات الحوكمة المؤسسية • إدارات التدقيق الداخلي • إدارات الامتثال / الالتزام • مكافحة الجرائم المالية

التوصية	الهدف	آلية التنفيذ	الجهة المسئولة	الإدارات المختصة بالجهة المسئولة
	بمسؤولية وعدالة وشفافية ضمن أطر تنظيمية واضحة.	بشكل عام، وفي مجال إدارة مخاطر الجرائم المالية بشكل خاص. • تشكيل لجان حوكمة داخلية تراجع وتراقب الأنظمة وتطبيق هذه السياسات والإجراءات. • تبني مبادئ مثل: الإنصاف، القابلية للتفسير، المساءلة.	للقطاع المالي وإستراتيجية التكنولوجيا المالية بشكل عام، وإرشادات الذكاء الاصطناعي الصادرة عن المصرفي في عام 2024 بشكل خاص، والقواعد الأخرى ذات الصلة.	• إدارات الشئون القانونية
تطوير خطط طوارئ للأنظمة	ضمان استمرارية الأعمال واستعادة الأنظمة الذكية بسرعة في حال حدوث اختراقات أو أعطال.	• إعداد خطط تعافي من الكوارث (DRPs). • اختبار هذه الخطط بشكل دوري. • إنشاء مراكز بيانات احتياطية وخطط بديلة لتدفق العمل.	مؤسسات القطاع المصرفي تحت إشراف البنك المركزي.	• إدارة استمرارية الأعمال • إدارة تكنولوجيا المعلومات إدارة أمن المعلومات
بناء قدرات الموارد البشرية	تأهيل الموظفين والمسئولين في مؤسسات القطاع المصرفي للتعامل مع أدوات وتقنيات الذكاء الاصطناعي في مجالات مكافحة الجرائم المالية.	• تنظيم برامج ودورات تدريبية متخصصة لموظفي ومسئولي المؤسسات المصرفية. • عقد ورش عمل تطبيقية داخلية وخارجية. • حصول موظفي ومسئولي الإدارات المختصة على شهادات مهنية دولية متخصصة في الجال. • التعاون بين المؤسسات المصرفية والمراكز البحثية والجامعات الوطنية والدولية.	مؤسسات القطاع المصرفي، تحت إشراف مصرف قطر المركزي	• إدارات الامتثال / الالتزام ومكافحة الجرائم المالية • إدارات المخاطر • إدارات الموارد البشرية
إنشاء مراكز لذكاء المخاطر	توفير بيئة تحليلية مركزية تستفيد من الذكاء الاصطناعي لتقييم أنماط المخاطر المعقدة والمستجدة في مجال الجرائم المالية.	• إنشاء فرق مشتركة من محللي البيانات والمخاطر والإدارات المختصة الأخرى. • بناء أنظمة تحليل بيانات كبيرة. • ربط المركز بالأنظمة التشغيلية والرقابية في القطاع المصرفي.	مصرف قطر المركزي، مع تشجيع مؤسسات القطاع المصرفي على إنشاء مراكز داخلية مماثلة	• إدارة المخاطر المؤسسية • إدارة أمن المعلومات • إدارة الإشراف على التكنولوجيا المالية • إدارة مكافحة الجرائم المالية • إدارة البيانات
تعزيز التعاون الإقليمي	تبادل الخبرات والبيانات الاستخباراتية المتعلقة بالجرائم المالية والتقنيات الذكية المستخدمة في إداراتها بين دول مجلس التعاون الخليجي.	• إنشاء منصات تبادل معلومات مالية مدعومة بالذكاء الاصطناعي. • توقيع مذكرات تفاهم مع البنوك والمصارف المركزية الخليجية. • تنظيم مؤتمرات ودورات تجريبية وورش عمل وندوات إقليمية دورية متخصصة.	**مصرف قطر المركزي** بالتنسيق مع المؤسسات المصرفية	• إدارة التعاون الدولي • مركز إدارة المواهب للتدريب والتطوير • إدارة المخاطر المؤسسية • إدارة أمن المعلومات • إدارة الإشراف على التكنولوجيا المالية • إدارة مكافحة الجرائم المالية • إدارة البيانات

المصدر: من إعداد الباحث بناء على نتائج الدراسة

رابعا: صعوبات (محددات) الدراسة:

اعترضت الباحث مجموعة من الصعوبات (المحددات) عند إعداده لهذه الدراسة، وهذه الصعوبات أو المحددات كانت كما يلي:

أ- المحددات في الجانب النظري:

1. التطور الكبير والسريع في تقنيات الذكاء الاصطناعي وتطبيقاته بشكل لا يمكن اللحاق به، ويصعب معه من ثمَّ حصر هذه التطبيقات ودراستها بشكل كاف.
2. قلة الدراسات والمراجع العربية حول الذكاء الاصطناعي وتطبيقاته وتقنياته بشكل عام من ناحية، وحول استخداماته في القطاع المصرفي من ناحية أخرى، بالإضافة إلى ندرة هذه الدارسات - سواء العربية أو الأجنبية منها - فيما يتعلق بدراسة العلاقة الذكاء الاصطناعي وتطبيقاته وتقنياته والأبعاد المختلفة لعملية إدارة مخاطر الجريمة المالية؛ لذلك اعتمد الباحث بشكل رئيسي على الدراسات السابقة الأجنبية ذات الصلة بأحد أو بعض جوانب هذه الدراسة ومتغيراتها.

ب- المحددات في الجانب العملي (التطبيقي):

1. عدم فهم مصطلحات الدراسة من قبل بعض الموظفين في بعض المؤسسات المصرفية.
2. صعوبة الحصول على بيانات دقيقة وكافية حول الجريمة المالية، حيث إن العديد من المؤسسات المصرفية ليس لديها الرغبة في مشاركة معلومات ترى من وجهة نظرها أنها حساسة وسرية أو قد تؤثر على سمعتها وصورتها الذهنية.

خامسا: دراسات مستقبلية مقترحة:

في ضوء النتائج التي توصلت إليها الدراسة، وتأكيدها على التأثير الفاعل لتقنيات الذكاء الاصطناعي في تعزيز إدارة مخاطر الجرائم المالية في القطاع المصرفي القطري، تبرز الحاجة إلى توسيع نطاق البحث في هذا المجال الحيوي، وتأسيسًا على ذلك، يقترح الباحث مجموعة من الدراسات المستقبلية التي من شأنها تعميق الفهم، واختبار متغيرات جديدة، واستكشاف تطبيقات مبتكرة تسهم في تطوير الممارسات المصرفية وتعزيز كفاءتها في مواجهة التحديات الأمنية والرقابية المتزايدة، وهي كالتالي:

1. دراسة تأثير الذكاء الاصطناعي على جودة القرارات الرقابية داخل وحدات الامتثال ومكافحة غسل الأموال في مؤسسات القطاع المصرفي في دولة قطر.
2. دراسة تأثير الحوكمة المؤسسية وأخلاقيات الذكاء الاصطناعي على مستوى المخاطر التشغيلية في المصارف القطرية.
3. تحليل إدراك العاملين في مؤسسات القطاع المصرفي في دولة قطر لمخاطر التحيز الخوارزمي وتأثيره على عدالة اتخاذ القرار المالي.
4. دراسة تأثير البرامج التدريبية المخصصة للعاملين في مؤسسات القطاع المصرفي في دولة قطر على تحسين قدرتهم في التعامل مع أنظمة الذكاء الاصطناعي.
5. تحليل تأثير التكامل بين الذكاء الاصطناعي وتحليلات البيانات الضخمة (Big Data Analytics) في تعزيز دقة تقارير الامتثال المالي في مؤسسات القطاع المصرفي في دولة قطر.
6. تحليل العوامل النفسية والاجتماعية لقبول الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في مؤسسات القطاع المصرفي في دولة قطر.

قائمة المصادر والمراجع

أولاً: المصادر والمراجع باللغة العربية

1. الأسد، صالح. (2023). الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية .مجلة إضافات اقتصادية، 7(1)، 165.184–
2. إبراهيم، رفيدة قمر الدولة محمد. (2019). المخاطر التي تتعرض لها المصارف والمؤسسات المالية. الكلية التطبيقية، جامعة الأمير سطام بن عبد العزيز. مسترجع من https://cc.psau.edu.sa/ar/node/10253
3. الجابر، غدير. (2020). أثر الذكاء الاصطناعي على كفاءة الأنظمة المحاسبية في البنوك الأردنية (رسالة ماجستير غير منشورة). جامعة الشرق الأوسط، عمّان، الأردن.
4. الخوالدة، سري ياسر. (2020). دور النظم الخبيرة في العلاقة بين بطاقة الأداء المتوازن وتحسين القرارات المالية في الشركات الصناعية المساهمة العامة الأردنية (رسالة ماجستير غير منشورة). كلية الاقتصاد والعلوم الإدارية، جامعة آل البيت، الأردن.
5. الشرق. (2025، 25 فبراير). محافظ "المركزي": مختبر ابتكار لشركات التكنولوجيا المالية قريبًا. صحيفة الشرق. تم الاسترجاع في 21 يونيو 2025 من https://al-sharq.com/article/25/02/2025/محافظ-المركزي-مختبر-ابتكار-لشركات-التكنولوجيا-المالية-قريبا
6. الضحيان، سعود بن ضحيان .(2002) . التحليل الإحصائي لمعالجة البيانات للبحوث التربوية والنفسية والرياضية باستخدام برامج - Excel Statistics - SPSS. دار الفكر العربي، القاهرة.
7. النسور، مرح فراس محمد، وبقيلة، بسام خليل عطا الله. (2022). أثر الذكاء الاصطناعي في التدقيق المبني على المخاطر: الدور الوسيط لجودة التدقيق في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من http://search.mandumah.com/Record/1334614
8. الهيئة السعودية للبيانات والذكاء الاصطناعي. (2024، أبريل). الذكاء الاصطناعي. سلسلة الذكاء الاصطناعي للتنفيذيين. https://www.sdaia.gov.sa
9. إسماعيل، عمار فتحي موسى، والمطيري، نهار برجس نهار. (2022). دور النظم الخبيرة في تحسين جودة الخدمة – دراسة تطبيقية .المجلة العلمية للدراسات والبحوث المالية والإدارية، كلية التجارة، جامعة مدينة السادات، 14(1)، 714.687–
10. بن علي، سمية. (2023). مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام تطبيق الأمن السيبراني: بنك Danske الدنماركي أنموذجًا .مجلة أبعاد اقتصادية، 13(2)، 63.39–
11. بوبعاية، نصيرة، والوافي، شهرزاد، وبوتغان، حمزة. (2021). دور البيانات الضخمة والذكاء الاصطناعي في مواجهة وباء كورونا: تجارب دولية ناجحة . مجلة وحدة البحث في تنمية الموارد البشرية، 16(3)، 148.122–
12. بوعلام، رجاء محمود .(2001) .التحليل الإحصائي للبيانات باستخدام برنامج .SPSS دار النشر للجامعات المصرية.
13. حسانين، محمد إبراهيم إبراهيم. (2023). الذكاء الاصطناعي والمسؤولية المدنية عن أضرار تطبيقه: دراسة تحليلية تأصيلية .المجلة القانونية، 15(1)، 270.177–
14. حسن، محمود السيد محمود علي. (2025). دور آليات الذكاء الاصطناعي عند التنبؤ بالأرباح .مجلة البحوث المالية والتجارية، كلية التجارة، جامعة بورسعيد، 26(1)، 691.671–
15. زهرة، إيمان. (2023). نحو منظور مستقبلي لتضمين الذكاء الاصطناعي في تعليم الاتصال التسويقي في مصر .المجلة المصرية لبحوث الإعلام، 84(2)، 146.91–
16. زوانب، غريسية، وحاج علي، أمينة. (2021). تأثير تكنولوجيا المعلومات والاتصال على المخاطر التشغيلية بالبنوك: دراسة استقصائية على عدد من البنوك الجزائرية .مجلة البحوث والدراسات التجارية، 5(1)، 224.207–
17. سالمي، نصر الدين، وكمال، بن دقفل. (2020). دور الذكاء الاصطناعي في عملية تخطيط المنتج في شركة الاتصالات أوريدو .مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، 13(1)، 193.179–
18. عزيز، محمد الخزامي. (2023). دور الذكاء الاصطناعي في العلوم الاجتماعية والإنسانية .سمينار، 1(2)، 35.1–
19. طايل، إيمان محمد خيري. (2022). الذكاء الاصطناعي وأثاره على سوق العمل .مجلة الدراسات القانونية والاقتصادية، 4(8)، 749.713–
20. قمورة، سامية، ومحمد، باي، وكروش، حيزية. (2018). الذكاء الاصطناعي بين الواقع والمأمول: دراسة تقنية وميدانية. بحث مقدم إلى الملتقى الدولي: الذكاء الاصطناعي تحدٍ جديد للقانون، الجزائر، نوفمبر 2018.

ثانيًا: المصادر والمراجع باللغة الإنجليزية

1. Abbasov, R. (2022). Artificial intelligence in banking: Advanced risk management techniques and practical applications for enhanced financial security and operational efficiency. Journal of Artificial Intelligence Research, 2(1), 82–130.
2. Abumughli, A. A., Aysan, A. F., Arslan, A., Gölgeci, İ., & Bouguerra, A. (2024). From the periphery to a global player: Historical evolution of the Qatari banking sector. In M. Bulut, B. Altay, & C. Korkut (Eds.), Islamic financial institutions from the early modern period to the 20th century: Comparative perspectives on the history and development of cash waqfs (pp. 111–140). Palgrave Macmillan.
3. Achim, M. V., Borlea, S. N., & Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. Technological and Economic Development of Economy, 27(1), 1–39.
4. Achim, M. V., Văidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The impact of the development of society on economic and financial crime: Case study for European Union member states. Risks, 9(5), 97.
5. Adaga, E. M., Egieya, Z. E., Ewuga, S. K., Abdul, A. A., & Abrahams, T. O. (2024). A comprehensive review of ethical practices in banking and finance. Finance & Accounting Research Journal, 6(1), 1–20.
6. Adel, N., & Naili, M. (2024). Geopolitical risk and banking performance: Evidence from emerging economies. Journal of Risk Finance, 25(4), 646–663.
7. Afjal, M., Salamzadeh, A., & Dana, L. P. (2023). Financial fraud and credit risk: Illicit practices and their impact on banking stability. Journal of Risk and Financial Management, 16(9), 1–30.
8. Agarwal, A., Agarwal, H., & Agarwal, N. (2023). Fairness score and process standardization: Framework for fairness certification in artificial intelligence systems. AI and Ethics, 3(1), 1–15.
9. Ahmad, A. Y. A. B. (2024, April). Fraud prevention in insurance: Biometric identity verification and AI-based risk assessment. In Proceedings of the 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS) (pp. 1–6). IEEE.
10. Ahmed, I. E., Mehdi, R., & Mohamed, E. A. (2023). The role of artificial intelligence in developing a banking risk index: An application of adaptive neural network-based fuzzy inference system (ANFIS). Artificial Intelligence Review, 56(11), 13873–13895.
11. Ahmed, I., Jeon, G., & Piccialli, F. (2022). From artificial intelligence to explainable artificial intelligence in Industry 4.0: A survey on what, how, and where. IEEE Transactions on Industrial Informatics, 18(8), 5031–5042.
12. Ahmadi, S. (2024). Open AI and its impact on fraud detection in financial industry. Journal of Knowledge, Learning and Science Technology, 12, 263–281.
13. Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2022). Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. Annals of Operations Research, 308, 7–39.
14. Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative artificial intelligence and cyber security in central banking (BIS Papers No. 145). Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap145.htm
15. Al-Fatlawi, A., Al-Khazaali, A. A. T., & Hasan, S. H. (2024). AI-based model for fraud detection in bank systems. Journal of Fusion: Practice and Applications, 14(1), 302–330.
16. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637–9664.
17. Ali, A. N. F., Sulaima, M. F., Razak, I. A. W. A., Kadir, A. F. A., & Mokhlis, H. (2023). Artificial intelligence application in demand response: Advantages, issues, status, and challenges. IEEE Access, 11, 1–16.
18. Aloumi, D., Malik, S., Alkhaldi, A., & Ordóñez de Pablos, P. (2024). Factors influencing consumer interactions with FinTech services. In Building climate neutral economies through digital business and green skills (pp. 1–20). IGI Global.
19. Altmann, J., & Sauer, F. (2020). Autonomous weapon systems and strategic stability. Survival, 59(5), 117–142.
20. Alzboon, M. S., Bader, A. F., Abuashour, A., Alqaraleh, M. K., Zaqaibeh, B., & Al-Batah, M. (2023). The two sides of AI in cybersecurity: Opportunities and challenges. In Proceedings of the 2023 International Conference on Intelligent Computing and Next Generation Networks (ICNGN) (pp. 1–10). IEEE.
21. Amar, N. (2023, January 14). Deep learning and artificial neural networks. ACAIA. https://acaiaworld.com/blog/deep-learning-and-artificial-neural-networks/
22. Anwar, H., Al Mubarak, M., & Bakir, A. (2023). Artificial intelligence in marketing and organizational decision-making: Some challenges and concerns. In M. A. A. Mahdi, A. Ameen, & A. K. Al-Shami (Eds.), Technological sustainability and business competitive advantage (pp. 9–23). Springer.
23. Antonov, O., & Lineva, E. (2021). The concept, types and structure of corruption (arXiv No. 2106.09498). arXiv.
24. Arab Monetary Fund. (2024). Financial security in Arab banks. https://www.amf.org.ae
25. Arthur, K. K., Asongu, S. A., Darko, P., Ansah, M. O., Adom, S., & Hlortu, O. (2025). Financial crimes in Africa and economic growth: Implications for achieving sustainable development goals (SDGs). Journal of Economic Surveys, 39(3), 1212–1251.

26. Arsenyan, J., & Piepenbrink, A. (2023). Artificial intelligence research in management: A computational literature review. IEEE Transactions on Engineering Management, 71, 5088–5100.
27. Arjunan, T. (2024). Fraud detection in NoSQL database systems using advanced machine learning. International Journal of Innovative Science and Research Technology (IJISRT), 13(3), 248 – 253.
28. Association of Certified Fraud Examiners. (2022). Occupational fraud 2022: A report to the nations. https://www.acfe.com/about-the-acfe/newsroom-for-media/press-releases/press-release-detail?s=2022-RTTN-launch
29. Association of Certified Fraud Examiners (ACFE). (2024). Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse. https://www.acfe.com
30. Awasthi, A. (2022). Using artificial intelligence to prevent banking frauds. International Journal for Research in Applied Science and Engineering Technology, 10(10), 358 – 359.
31. Awosika, T., Shukla, R. M., & Pranggono, B. (2023). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection (arXiv preprint arXiv:2312.13334). arXiv
32. Ayinaddis, S. G., Taye, B. A., & Yirsaw, B. G. (2023). Examining the effect of electronic banking service quality on customer satisfaction and loyalty: An implication for technological innovation. Journal of Innovation and Entrepreneurship, 12(1), 1–18.
33. Azuma-Kotei, Z. A., & Ibrahim, A. E. A. (2024). The concept of corporate risk: Perspectives of risk disclosure's users and preparers. Journal of Risk Research. Advance online publication, 1-24
34. Bait Al Mashura Finance Consultations. (2025, June 9). 8th annual report on Islamic finance in the State of Qatar [Annual report]. Bait Al Mashura. Retrieved from https://b-mashura.com/en/2025/06/09/
35. Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. (2023). The power of generative AI: A review of requirements, models, input–output formats, evaluation metrics, and challenges. Future Internet, 15(8), 1–60.
36. Banh, L., & Strobel, G. (2023). Generative artificial intelligence. Electronic Markets, 33(1), 1-17.
37. Bank for International Settlements. (2021). Annual economic report 2021. Retrieved from: https://www.bis.org/publ/arpdf/ar2021e.htm
38. Bao, W., Xiao, J., Deng, T., Bi, S., & Wang, J. (2024). Challenges and opportunities of financial technology innovation to bank financing business and risk management. Financial Engineering & Risk Management, 7(2), 82 – 88.
39. Basel Institute on Governance. (2023). Annual AML Index. https://www.baselgovernance.org
40. Basheer Ahmed, M. I., Zaghdoud, R., Ahmed, M. S., Sendi, R., Alsharif, S., Alabdulkarim, J., & Krishnasamy, G. (2023). A real-time computer vision-based approach to detection and classification of traffic incidents. Big Data and Cognitive Computing, 7(1), 1–22.
41. Behiry, M. H., & Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(1), Article 16, 1–39.
42. Berente, N., Gu, B., Recker, J., & Santhanam, R. (2021). Managing artificial intelligence. MIS Quarterly, 45(3), 1433–1450.
43. Berry, M., Salinas, M., & Gundur, R. V. (2023). Financial risk management strategies of small to medium illicit drug enterprises: Considering low-level money laundering. Trends in Organized Crime, 1–39. Advance online publication.
44. Bezshtank, D. (2025). AI and bank's operational risk management. Three Seas Economic Journal, 6(2), 22–27.
45. Biliavskyi, V., Biliavska, Y., Umantsiv, Y., Shestack, Y., Zhurba, O., & Khavanov, A. (2024). Digital technologies in the financial sector of the economy. Financial & Credit Activity: Problems of Theory & Practice, 57, 171–183.
46. Birhane, A. (2022). Automating ambiguity: Challenges and pitfalls of artificial intelligence (PhD thesis, University College Dublin, Dublin, Ireland). University College Dublin Research Repository. (arXiv preprint No. 2206.04179). arXiv.
47. Bi, S., & Bao, W. (2024). Innovative application of artificial intelligence technology in bank credit risk management (arXiv preprint No. 2404.18183). arXiv.
48. Bocola, L., & Lorenzoni, G. (2023). Risk sharing externalities. Journal of Political Economy, 131(3), 595–632.
49. Brici, I. (2022). New tendency of economic and financial crime in the context of the digital age: A literature review. DIEM: Dubrovnik International Economic Meeting, 7(1), 130–141.
50. Bouveret, A. (2022). Cyber risk for the financial sector: A framework for quantitative assessment (IMF Working Paper No. 18/143). International Monetary Fund.
51. Bueno, L. A., Sigahi, T. F. A. C., Rampasso, I. S., Leal Filho, W., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. International Journal of Information Management Data Insights, 4(1), 100230, 1–10.
52. Butt, I., Ul-Haq, S., Shareef, M. A., Chowdhury, A. H., & Ahmed, J. U. (2022). Ethical reputation and retail bank selection: A sequential exploratory mixed-methods study in an emerging economy. International Journal of Bank Marketing, 40(7), 1346–1388.
53. Butz, M. V. (2021). Towards strong AI. Artificial Intelligence Review, 54(1), 369–406.
54. Cardoso, M., Saleiro, P., & Bizarro, P. (2022). LaundroGraph: Self-supervised graph representation learning for anti-money laundering (arXiv preprint arXiv:2209.03025). arXiv.
55. Castelnovo, A. (2024). Towards responsible AI in banking: Addressing bias for fair decision-making (arXiv preprint arXiv:2401.08691). arXiv.

56. Castelo, N., Bos, M. W., & Lehmann, D. R. (2022). The influence of artificial intelligence on human decision-making. Journal of Marketing, 86(1), 98–115.
57. Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1), 31–48.
58. Che, C., Zheng, H., Huang, Z., Jiang, W., & Liu, B. (2024). Intelligent robotic control system based on computer vision technology (arXiv preprint arXiv:2404.01116). arXiv.
59. Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review (arXiv preprint arXiv:2502.00201). arXiv.
60. Cheng, X., Liu, S., Sun, X., Wang, Z., Zhou, H., Shao, Y., & Shen, H. (2021). Combating emerging financial risks in the big data era: A perspective review. Fundamental Research, 1(5), 674–682.
61. Chianumba, E. C., Omo Kanye, A. O., Ajayi, A. M., Olowu, O., Adeleye, A. O., & Omole, O. M. (2022). AI-powered financial crime prevention with cybersecurity, IT, and data science in modern banking. International Journal of Science and Research Archive, 13(2), 570–579.
62. Chui, M., Manyika, J., & Miremadi, M. (2021). The future of work in the age of AI. McKinsey Global Institute Discussion Paper. https://www.mckinsey.com/
63. Cipriani, M., Goldberg, L. S., & La Spada, G. (2023). Financial sanctions, SWIFT, and the architecture of the international payment system. Journal of Economic Perspectives, 37(1), 31–54.
64. Clintworth, M., Lyridis, D., & Boulougouris, E. (2023). Financial risk assessment in shipping: A holistic machine learning-based methodology. Maritime Economics & Logistics, 25(1), 134–157.
65. Cybersecurity Advisors Network. (2025). Cybersecurity investments in global banking: Comparative analysis and case studies. https://cybersecurityadvisors.network/2025/03/04/cybersecurity-investments-in-global-banking-comparative-analysis-and-case-studies
66. Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. IEEE Access, 11, 1–20.
67. Davidson, K. (2025). Super AI: The next frontier in artificial intelligence research. QIT Press – International Journal of Super AI Research and Development (QITP IJSAIRD), 6(1), 1–5.
68. Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O., & Ewuga, S. K. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. Computer Science & IT Research Journal, 4(3), 220–243.
69. Demekas, D. G., Liu, Y., & Wang, H. (2023). Financial crime risk management in digital banking. Journal of Financial Regulation, 9(1), 1–29.
70. Demirović, L., Isaković-Kaplan, Š., & Proho, M. (2022). Risk management of preventing money laundering and terrorist financing. Journal of Forensic Accounting Profession, 2(2), 23–38.
71. Dhiman, D., Bisht, A., Thakur, G., & Garg, A. (2025). Artificial intelligence and machine learning-enabled cybersecurity tools and techniques. In Advanced techniques and applications of cybersecurity and forensics (pp. 35–56). Chapman and Hall/CRC.
72. Dimcheva, G. (2024, August 1). Opportunities for application of artificial intelligence in telecommunication projects [Conference presentation]. International Conference on Electronics, Engineering Physics and Earth Science (EEPES'24), Kavala, Greece, 19–21 June 2024. Engineering Proceedings, 70(1), 1–10.
73. Dorris, R., & Cummings, L. (2023). Preventing asset misappropriation: Best practices for internal controls. Journal of Financial Crime, 30(3), 719–730.
74. Duggan, J., Sherman, U., Carbery, R., & McDonnell, A. (2022). Artificial intelligence and work: A critical review of recent research from the social sciences. AI & Society, 37(2), 675–691.
75. Efing, M., Goldbach, S., & Nitsch, V. (2023). Freeze! Financial sanctions and bank responses. The Review of Financial Studies, 36(11), 4393–4436.
76. Elgammal, A., Liu, B., Elhoseiny, M., & Mazzone, M. (2021). CAN: Creative adversarial networks, generating "art" by learning about styles and deviating from style norms. AI Magazine, 42(3), 48–68.
77. El Hajj, M., & Hammoud, J. (2023). Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. Journal of Risk and Financial Management, 16(10), 434.
78. El Hajj, S., & Hammoud, R. (2023). AI-driven risk evaluation models in financial institutions. Journal of Risk and Financial Management, 16(3), 112–125.
79. El Jabri, S., & El Khider, A. (2022). Corruption: Towards a new approach to classification. International Journal of Accounting, Finance, Auditing, Management and Economics, 3(4 2), 130–142.
80. Erport, Y., & Fadlon, T. (2023). Economic maneuvering: How states evade economic sanctions. A Multidisciplinary Journal on National Security, 26(2), 90–109.
81. Esmail, F. S., Alsheref, F. K., & Aboutabl, A. E. (2023). Enhancing loan fraud detection process in the banking sector using data mining techniques. Indonesian Journal of Electrical Engineering and Computer Science, 32(2), 956–967.
82. Eubanks, V. (2021). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

83. Fahad, M., Basri, T., Hamza, M. A., Faisal, S., Akbar, A., Haider, U., & Hajjami, S. E. (2024). The benefits and risks of artificial general intelligence (AGI). In Artificial general intelligence (AGI) security: Smart applications and sustainable technologies (pp. 27–52). Springer Nature Singapore.

84. Fan, J., Shar, L. K., Zhang, R., Liu, Z., Yang, W., Niyato, D., Mao, B., & Lam, K.-Y. (2025). Deep learning approaches for anti-money laundering on mobile transactions: Review, framework, and directions (arXiv preprint arXiv:2503.10058v1). arXiv

85. Fanni, S. C., Febi, M., Aghakhanyan, G., & Neri, E. (2023). Natural language processing. In E. Neri, S. C. Fanni, & M. Febi (Eds.), Introduction to artificial intelligence (pp. 87–99). Springer.

86. Fares, O. H., Butt, I., & Lee, S. H. M. (2023). Utilization of artificial intelligence in the banking sector: A systematic literature review. Journal of Financial Services Marketing, 28(4), 276–286.

87. Farayola, O. A. (2024). Revolutionizing banking security: Integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. Finance & Accounting Research Journal, 6(4), 402–418.

88. Fatmawati, E., & Bebasari, N. (2023). The impact of financial resources, risk acceptance, customer pressure on financial technology. East Asian Journal of Multidisciplinary Research, 2(4), 1813–1820.

89. Federal Reserve. (2025). Estimating the volume of counterfeit U.S. currency in circulation. https://www.federalreserve.gov/econres/ifdp/estimating-the-volume-of-counterfeit-us-currency-in-circulation.htm

90. Ferrer, X., van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2020). Bias and discrimination in AI: A cross-disciplinary perspective (arXiv preprint arXiv:2008.07309). arXiv.

91. Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2024). Generative AI. Business & Information Systems Engineering, 66(1), 111–126.

92. Financial Action Task Force (FATF). (2012). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations (Updated February 2025). https://www.fatf-gafi.org/en/publications/Fatfrecommendations/FATF-Recommendations.html

93. Financial Action Task Force (FATF). (2021). Guidance on proliferation financing risk assessment and mitigation. FATF. https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

94. Fitch Ratings. (2024, December 23). Qatari banks to maintain sound metrics in 2025. https://www.fitchratings.com/research/banks/qatari-banks-to-maintain-sound-metrics-in-2025-23-12-2024

95. Gafsi, N. (2025). Machine learning approaches to credit risk: Comparative evidence from participation and conventional banks in the UK. Journal of Risk and Financial Management, 18(7), 1–18.

96. Gaganis, C., Pasiouras, F., Tasiou, M., & Zopounidis, C. (Eds.). (2023). Sustainable finance and ESG: Risk, management, regulations, and implications for financial institutions. Springer Nature.

97. Gao, J., Pacelli, J., Schneemeier, J., & Wu, Y. (2023). Dirty money: How banks influence financial crime. 1- 71.

98. Gao, W., & Liu, Y. (2023). Risk management in the banking sector during the COVID-19 crisis: Challenges & responses. Advances in Economics, Management and Political Sciences, 31, 48–53.

99. Gaviyau, W., & Sibindi, A. B. (2023). Global anti-money laundering and combating terrorism financing regulatory framework: A critique. Journal of Risk and Financial Management, 16(7), 313, 1–21.

100. Ghasemaghaei, M., & Kordzadeh, F. (2024). Adoption of artificial intelligence-driven fraud detection in banking: The role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. Journal of Financial Services Research, 18(4), 217–234.

101. Gillet, K. (2022, May 30). The rise and rise of Qatar's Islamic banking sector. The Banker. Retrieved June 14, 2025, from https://www.thebanker.com/content/8104a572-7cdb-594c-a413-83ad69c11f57

102. Global Finance. (2025). World's best bank awards 2025 – Middle East winners. Global Finance. Retrieved June 20, 2025, from https://gfmag.com/award/award-winners/best-banks-in-middle-east-2025/

103. Go-Globe. (2024, August 7). FinTech Qatar: Driving innovation and digital transformation in 2024. Retrieved June 21, 2025, from https://www.go-globe.com/qatar-fintech-and-financial-market-in-2024/

104. Gupta, A., Dwivedi, D. N., & Shah, J. (2023). Artificial intelligence applications in banking and financial services: Anti money laundering and compliance. Springer Nature Singapore.

105. Gupta, D., Miryala, N. K., & Srivastava, A. (2023). Leveraging artificial intelligence for countering financial crimes. International Journal of Artificial Intelligence & Machine Learning, 2(1), 103–120.

106. Gupta, H., & Stocker, M. (2020). Big data application in banking: A bibliometric analysis of the literature. Journal of Business Analytics, 3(2), 85–112.

107. Gupta, S., Dwivedi, Y. K., & Shah, M. (2023). Financial crime risk management in banking: The role of artificial intelligence and regulatory collaboration. Journal of Banking & Finance, 147, 106–125.

108. Hadchity, M. (2025, June 10). Qatar's Islamic finance sector grows to $187 bn, report shows. Arab News. Retrieved June 21, 2025, from https://www.arabnews.com/node/2604030/business-economy

109. Harandi, S. R., Parsaee Tabar, A. & Abdolvand, N. (2021). Identifying the suspected cases of money laundering in banking using multiple attribute decision making (MADM). Journal of Money and Economy, 16(1), 1–20

110. Haya, H., & Mishra, S. (2024). The impact of AI-based cyber security on the banking and financial sectors. Journal of Cybersecurity and Information Management, 14(1), 8–19.

111. Herm, L. V., Janiesch, C., Helm, A., Imgrund, F., Hofmann, A., & Winkelmann, A. (2023). A framework for implementing robotic process automation projects. Information Systems and e-Business Management, 21(1), 5–33.

112. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications, 189, 116429, 1–34.

113. Högberg, C. (2024). Stabilizing translucencies: Governing AI transparency by standardization. Big Data & Society, 11(1), Article 1, 5–12.

114. Hsiung, H., & Wang, J. (2022). Research on the introduction of a robotic process automation (RPA) system in small accounting firms in Taiwan. Economies, 10(8), 200, 1–18.

115. Ide, E., & Talamas, E. (2025). Artificial intelligence in the knowledge economy (834–836). arXiv.

116. Inscribe AI. (2025). 2025 document fraud report. https://www.inscribe.ai/2025-document-fraud-report

117. International Monetary Fund. (2024, February 6). Qatar: 2023 Article IV consultation—Press release and staff report (IMF Country Report No. 2024/043). https://www.imf.org/en/Publications/CR/Issues/2024/02/06/Qatar-2023-Article-IV-Consultation-Press-Release-and-Staff-Report-544471

118. International Monetary Fund, Legal Department. (2023, December 5). Background paper II: AML/CFT risk-based supervision of banks—The impact of financial integrity failures on financial stability (1–2). International Monetary Fund. Retrieved from IMF eLibrary.

119. Interpol. (2020). Financial crime. Interpol. https://www.interpol.int/Crimes/Financial-crime

120. Ivanov, S. (2023). The dark side of artificial intelligence in higher education. The Service Industries Journal, 43(13–14), 889–907.

121. Jaeger, L. (2023). Ada Lovelace: Inventor of computer algorithms. In Women of genius in science (71–82). Springer International Publishing. 1815–1852.

122. Jawan Partners. (2024). Qatar Central Bank sets out regulatory framework for digital banks. Retrieved from https://www.jawanpartners.com/insights/qatar-central-bank-sets-out-regulatory-framework-for-digital-banks.

123. Jerfy, A., Selden, O., & Balkrishnan, R. (2024). The growing impact of natural language processing in healthcare and public health. INQUIRY: The Journal of Health Care Organization, Provision, and Financing, 61, 1–10.

124. Jiao, M. (2023). Big data analytics for anti-money laundering compliance in the banking industry. Highlights in Science, Engineering and Technology, 49, 302–309. Paper presented at the AMMSAC 2023 Conference.

125. Jofre, M., Bosisio, A., & Riccardi, M. (2024). Financial crime risk assessment: Machine learning insights into ownership structures in secrecy firms. Global Crime, 25(3–4), 242–267.

126. Johannessen, F., & Jullum, M. (2023). Finding money launderers using heterogeneous graph neural networks (arXiv preprint arXiv:2311.05239). arXiv.

127. Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Mahmud, M. A. A. (2024). AI-powered fraud detection in banking: Safeguarding financial transactions. The American Journal of Management and Economics Innovations, 6(6), 8–22.

128. Johari, R. J., Rozak, I. R., Talib, N. A., & Helmi, I. M. (2022). Role of code of ethics in building a fraud-resilient organization: The case of the developing economy. Journal of Governance and Regulation, 11(2), 32-40.

129. Josyula, H. P. (2023). Unraveling the adoption drivers of FinTech in India: An empirical analysis. International Journal of Computer Trends and Technology, 71(12), 109–115.

130. Kassenova, T., & Early, B. R. (2023). Countering the challenges of proliferation financing. Carnegie Endowment for International Peace. https://carnegieendowment.org/posts/2023/07/countering-the-challenges-of-proliferation-financing.

131. Kavakli, K. C., Marcolongo, G., & Zambiasi, D. (2023). Sanction evasion through tax havens (BAFFI CAREFIN Centre Research Paper No. 212). University of Rochester, Bocconi University, and Newcastle University.

132. Kedarya, T., Elalouf, A., & Cohen, R. S. (2023). Calculating strategic risk in financial institutions. Global Journal of Flexible Systems Management, 24(3), 311–326.

133. Kemp, S. (2025). Digital 2025: Qatar. DataReportal. Retrieved June 20, 2025, from https://datareportal.com/reports/digital-2025-qatar?rq=Qatar

134. Khinvasara, T., Ness, S., & Tzenios, N. (2023). Risk management in the medical device industry. Journal of Engineering Research and Reports, 25(8), 30–140.

135. Khelil, I., Khlif, H., & Achek, I. (2024). The economic consequences of money laundering: A review of empirical literature. Journal of Money Laundering Control, 27(5), 901–916.

136. Khlaif, Z. N., Mousa, A., Hattab, M. K., Itmazi, J., Hassan, A. A., Sanmugam, M., & Ayyoub, A. (2023). The potential and concerns of using AI in scientific research: ChatGPT performance evaluation. JMIR Medical Education, 9, e47049, 1–17.

137. Khurana, D., Koli, A., Khatter, K., & Singh, S. (2023). Natural language processing: State of the art, current trends, and challenges. Multimedia Tools and Applications, 82(3), 4051–4079.

138. Kok, S. L., & Siripipatthanakul, S. (2023). Artificial intelligence (AI) adoption: The case of the Malaysian financial industry. Advance Knowledge for Executives, 2(4), 1–10.

139. Koppisetti, V. S. K. (2024). Robotic process automation: Streamlining operations in the digital era. ESP International Journal of Advancements in Computational Technology (ESP-IJACT), 2(2), 25–35.

140. Korzeb, Z., Niedziółka, P., Szpilko, D., & di Pietro, F. (2024). ESG and climate-related risks versus traditional risks in commercial banking: A bibliometric and thematic review. Future Business Journal, 10, Article 106

141. Kountur, R., & Sari, M. R. (2023). Risk identification approaches and the number of risks identified: The use of work breakdown structure and business process. Humanities and Social Sciences Communications, 10(1), Article 20

142. Kovacevic, A., Radenkovic, S. D., & Nikolic, D. (2024). Artificial intelligence and cybersecurity in the banking sector: Opportunities and risks (arXiv preprint arXiv:2412.04495). arXiv.

143. Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2023). ImageNet classification with deep convolutional neural networks. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(7), 1097–1105.

144. Kufel, J., Bargieł-Łączek, K., Kocot, S., Koźlik, M., Bartnikowska, W., Janik, M. & Lis, A. (2023). What is machine learning, artificial neural networks and deep learning?—Examples of practical applications in medicine. Diagnostics, 13(15), Article 2582.

145. Kuldova, T. Ø. (2022). Artificial intelligence, algorithmic governance, and the manufacturing of suspicion and risk. In Compliance-industrial complex (pp. 115–151). Springer Nature Switzerland.

146. Kulmie, D. A., Hilif, M. D., & Hussein, M. S. (2023). Socioeconomic consequences of corruption and financial crimes. International Journal of Economics and Financial Issues, 13(5), 88–95.

147. Kumar, S., Lim, W. M., Sivarajah, U., & Kaur, J. (2023). Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. Information Systems Frontiers, 25(2), 545–564

148. Kuo, C.-L., & Hsu, C.-Y. (2024). Reducing risk assessment bias through AI-powered decision support systems. Expert Systems with Applications, 235, 120598.

149. Kuo, Y.-F., & Hsu, C.-L. (2024). Artificial intelligence in risk management. In Artificial Intelligence for Risk Mitigation in the Financial Industry, 1–25. Wiley.

150. Kurshan, E., Shen, H., & Chen, J. (2020). Towards self-regulating AI: Challenges and opportunities of AI model governance in financial services (arXiv preprint arXiv:2010.04827). arXiv

151. Kurshan, E., & Shen, H. (2024, August). Graph computing for financial crime and fraud detection: Trends, challenges, and outlook. Princeton University & University of Alabama in Huntsville.

152. Levytska, S., Pershko, L., Akimova, L., Akimov, O., Havrilenko, K., & Kucherovskii, O. (2022). A risk-oriented approach in the system of internal auditing of the subjects of financial monitoring. International Journal of Applied Economics, Finance and Accounting, 14(2), 194–206.

153. Litvishko, O. (2020). Impact of the digital economy on the banking sector. E3S Web of Conferences, 159, Article 04033

154. McKinsey & Company. (2024). Managing bank IT spending: Five questions for tech leaders. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/managing-bank-it-spending-five-questions-for-tech-leaders

155. Mahony, J. (2022). Best practices in combating fraud in financial institutions. Journal of Risk Management in Financial Institutions, 15(3), 270–277.

156. Majumder, T. (2024). The evaluating impact of artificial intelligence on risk management and fraud detection in the commercial bank in Bangladesh. International Journal of Applied and Natural Sciences, 1(1), 67–76.

157. Malusare, L. B. (2024). A study of artificial intelligence in the banking sector: A study of customer and bank employee perception toward AI based banking services. International Journal for Research Trends and Innovation, 8(10), 1–7.

158. Manoharan, G., Durai, S., & Rajesh, G. A. (2023). A study on the application of expert systems as a support system for business decisions. In Artificial Intelligence and Knowledge Processing, 1-11.

159. Meissner, K. L., & Mello, P. A. (2022). The unintended consequences of UN sanctions: A qualitative comparative analysis. Contemporary Security Policy, 43(2), 243–273.

160. MENA Fintech Association. (2024, September 18). Fintech in Qatar: Collaborative innovation for a digital future. Retrieved June 21, 2025. Retrieved from https://mena-fintech.org/fintech-in-qatar-collaborative-innovation-for-a-digital-future/

161. Meindl, B., & Mendonça, J. (2021). Mapping Industry 4.0 technologies: From cyber-physical systems to artificial intelligence (arXiv preprint No. 2111.14168). arXiv.

162. Mirishli, S. (2025). Regulating AI in financial services: Legal frameworks and compliance challenges (arXiv preprint arXiv:2503.14541). arXiv.

163. Moody's Investors Service. (2025, February 25). Banking system outlook – Qatar [PDF]. Moody's Investors Service. https://dkf1ato8y5dsg.cloudfront.net/uploads/52/504/outlook-banking-system-outlook-qatar-25feb2025-pbc-1432763.pdf

164. Mosqueira-Rey, E., Hernández-Pereira, E., Alonso-Ríos, D., Bobes-Bascarán, J., & Fernández-Leal, Á. (2023). Human-in-the-loop machine learning: A state of the art. Artificial Intelligence Review, 56(4), 1513–1589.

165. Mucci, T. (2024, October 21). The history of artificial intelligence. IBM. https://www.ibm.com/think/topics/history-of-artificial-intelligence

166. Muhammad, S., Meerjat, F., Meerjat, A., Naz, S., & Dalal, A. (2024). Enhancing cybersecurity measures for robust fraud detection and prevention in US online banking. International Journal of Advanced Engineering Technologies and Innovations, 1(3), 45–59.

167. Muminovic, H. (2021). Typologies of financial crime. Journal of Law & Politics (IBU), 2(2), 43–53. International Balkan University.

168. Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. Big Data and Cognitive Computing, 7(2), Article 93.

169. Nah, F. F.-H., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. Journal of Information Technology Case and Application Research, 25(3), 163–174.

170. Nasdaq & Verafin. (2024). 2024 global financial crime report (p. 3). Nasdaq. Retrieved from https://www.verafin.com/resources/2024-global-financial-crime-report/

171. Naser, M. Z., & Alavi, A. H. (2021). Error metrics and performance fitness indicators for artificial intelligence and machine learning in engineering and sciences. Architecture, Structures and Construction, 1, Article 00015.

172. National Planning Committee. (2025). Annual banks and insurance report 2025. https://www.npc.qa/en/statistics/Statistical%20Releases/Economic/Banking%20and%20Insurance/Annual_Banks_Insurance_2020_AE.pdf

173. Nazarian-Jashnabadi, J., Bonab, S. R., Haseli, G., Tomaskova, H., & Hajiaghaei-Keshteli, M. (2023). A dynamic expert system to increase patient satisfaction with an integrated approach of system dynamics, ISM, and ANP methods. Expert Systems with Applications, 234, 121010.

174. Nedilko, B. (2020). Concept and main characteristics of artificial intelligence: Domestic and foreign approaches. International Journal of Library & Information Science, 9(1), 15–21.

175. Ngigi Nyakarimi, S., Nduati Kariuki, S., & 'Ombe Kariuki, P. W. (2020). Risk assessment and fraud prevention in banking sector. The Journal of Social Sciences Research, 6(1), 13–20.

176. Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial Intelligence (AI) in banking industry & consumer's perspective. Sustainability, 15(4), Article 3682.

177. Nzeako, G., Akinsanya, M. O., Popoola, O. A., Chukwurah, E. G., & Okeke, C. D. (2024). The role of AI-driven predictive analytics in optimizing IT industry supply chains. International Journal of Management & Entrepreneurship Research, 6(5), 1489–1497.

178. Okolie, P. I. P., Chukwuma, O. V., Eneh, N. A., & Ejike, S. I. (2023). Exploring the role of machine learning in detecting and preventing financial statement fraud: A case study analysis. International Journal of Multidisciplinary Research and Growth Evaluation, 4(1), 223–226.

179. Oleiwi, H. Z. (2024). The role of artificial intelligence and machine learning in digital banking technology. American Journal of Business Management, Economics and Banking, 20, 11–26.

180. Olimov, J. M. (2025). Bribery, secrecy, and communication: Theory and evidence from firms (arXiv preprint arXiv:2502.10877). arXiv.

181. Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges (arXiv preprint arXiv:2102.04661). arXiv.

182. Oxford Business Group. (2024). Qatar banking growth due to prudent governance, innovative strategies [Annual series report]. Oxford Business Group.

183. Palakurti, N. R. (2025). The role of artificial intelligence in risk assessment and mitigation in the financial sector. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 5(2), 633 – 641.

184. Paramesha, M., Rane, N. L., & Rane, J. (2024, July). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. Partners Universal Multidisciplinary Research Journal, 1(2), 68–83.

185. Patel, S., Kasztelnik, K., & Zelihic, M. (2023). The observational study financial fraud offense themes and financial fraud risk of money laundering to increase financial global sustainability compliance. Journal of Accounting and Finance, 23(4), 1–19.

186. Paulin, G., & Ivašić-Kos, M. (2023). Review and analysis of synthetic dataset generation methods and techniques for application in computer vision. Artificial Intelligence Review, 56(9), 7441–7485

187. Piao, G., & Xiao, B. (2022). Risk management analysis of modern commercial banks using behavioral finance theory and artificial neural networks. Wireless Communications and Mobile Computing, 2022, Article 1161784.

188. Pieth, M. (2022). Countering terrorist financing through international cooperation. Terrorism and Political Violence, 34(5), 1033–1048.

189. Pilat, O. V., Sharenko, M. S., & Sumtsova, S. O. (2025). Financial sanctions as an instrument of international policy. Uzhhorod National University Herald Series Law, 4(86), 25–31.

190. Ping Identity. (n.d.). Prevent bank fraud with digital identity. Retrieved August 3, 2025, from https://hub.pingidentity.com/financial-services/4074-prevent-bank-fraud-digital-identity

191. Pradesyah, R., Yuslem, N., & Batubara, C. (2021). Fraud in financial institutions. Journal of International Conference Proceedings, 4(2), 341–348.

192. Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). The influence of internal audit, risk management, whistleblowing system, and big data analytics on the financial crime behavior prevention. Cogent Economics & Finance, 10(1), Article 2148363.

193. PwC Middle East. (2024, November). Qatar banking sector report 2024 [PDF]. PwC Middle East. https://www.pwc.com/m1/en/publications/documents/2024/qatar-banking-sector-report-2024.pdf

194. Qatar Central Bank. (2023). Financial Stability Sector. Retrieved June 15, 2025, from https://www.qcb.gov.qa/en/FinancialStability/Pages/Financial-Stability-Sector.aspx

195. Qatar Central Bank. (2023, March). Summary of FinTech sector strategy in the State of Qatar [PDF]. Qatar Central Bank. https://www.qcb.gov.qa/Documents/SuperVision/FENTECHStrategy_EN.pdf

196. Qatar Central Bank. (2024, October). Strategy: Pillars, themes and initiatives [PDF]. Qatar Central Bank. https://www.qcb.gov.qa/PublicationFiles/Strategy%20PPT%20to%20design%20V6.pdf

197. Qata Development Bank-QDB & Qatar National Bank-QNB. (2025, February 23). QDB, QNB renew partnership to foster innovation in fintech. https://www.qdb.qa/about/news/news/qdb-x-qnb-agreement-web-summit

198. Qatar Islamic Bank - QIB (2025, May). Annual Report 2024 [PDF]. https://www.qib.com.qa/wp-content/uploads/2025/05/QIB-Annual-Report-2024-English.pdf

199. Qatar National Bank-QNB Q.P.S.C. (2025, April). Annual Report 2024 [PDF]. Qatar National Bank. https://www.qnb.com/sites/qnb/qnbqatar/document/en/enAnnualReport2024

200. Qatar National Bank - QNB Financial Services. (2025, April 21). Strong fundamentals bolster stability in Qatar's banking sector. Qatar Tribune. Retrieved from https://www.qatar-tribune.com

201. Qi, B., Marie, M., Abdelwahed, A., Khatatbeh, I., Omran, M., & Fayad, A. (2023). Bank risk literature (1978–2022): A bibliometric analysis and research front mapping. Sustainability, *15*(5), Article 4508.

202. Radanliev, P., De Roure, D., Maple, C., Nurse, J. R. C., Nicolescu, R., & Ani, U. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7, Article 1402745.

203. Rayan Bank PLC. (2025). Annual reports. Investor Relations – Financial Information. Retrieved June 20, 2025, from https://www.alrayan.com/en/investor-relations/financial-information/annual-reports

204. Raza, A. (2023). Risk management practices in the banking sector: A comparative analysis. Governance Accounting Archive Review, 1(1), 25–31.

205. Reserve Bank of Australia. (2022). Recent trends in banknote counterfeiting. Reserve Bank of Australia Bulletin. https://www.rba.gov.au/publications/bulletin/2022/jun/recent-trends-in-banknote-counterfeiting.html

206. Roosan, D., Padua, P., Khan, R., Khan, H., Verzosa, C., & Wu, Y. (2024). Effectiveness of ChatGPT in clinical pharmacy and the role of artificial intelligence in medication therapy management. Journal of the American Pharmacists Association, 64(2), 204–210.

207. Rouhollahi, Z. (2021). Towards artificial intelligence enabled financial crime detection (arXiv preprint arXiv:2105.10866). arXiv.

208. Sayed, E., & Mansour, K. (2023, February). Impact of digital transformation on banks' profitability and liquidity in emerging markets: Evidence from Egypt. The IUP Journal of Bank Management, 22(1), 5–30.

209. Sakamoto, L. S., & Abe, J. M. (2023). An expert system for decision making in the face of imprecise, inconsistent, and paracomplete data: Metaverse security application using DLP. In N. Bourbakis, G. A. Tsihrintzis, M. Virvou, & L. C. Jain (Eds.), Extended selected papers of the 14th International Conference on Information, Intelligence, Systems, and Applications (IISA 2023) (pp. 46–72). Springer.

210. Salamah, S. N. (2023). Financial management strategies to improve business performance. Journal of Contemporary Administration and Management (ADMAN), 1(1), 9–12.

211. Sanusi, Z. M. (2022). Money laundering risk: From the bankers' and regulators' perspectives. Procedia Economics and Finance, 28, 7–13.

212. Sarker, I. H. (2022). AI-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems. SN Computer Science, 3, Article 158

213. Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. Annals of Data Science, 10(6), 1473–1498.

214. Srivastava, A., Pandiya, B., & Nautiyal, N. S. (2024). Application of artificial intelligence in risk assessment and mitigation in banks. In Artificial intelligence for risk mitigation in the financial industry (pp. 27–52). Wiley.

215. Schneider, F. (2022). Money laundering and terrorist financing: An economic analysis. Journal of Financial Crime, 29(2), 550–561.

216. Schwab, K. (2016, January 14). The Fourth Industrial Revolution: What it means and how to respond. World Economic Forum. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond

217. Scott, A., Amajuoyi, P., & Adeusi, K. B. (2024). Advanced risk management solutions for mitigating credit risk in financial operations. Magna Scientia Advanced Research and Reviews, 12(1), 212–223.

218. Shafique, R., Alemany, W., Rustam, F., Lee, E., Mehmood, A., & Choi, G. S. (2023). Role of artificial intelligence in online education: A systematic mapping study. IEEE Access, 11, Article 3345678.

219. Shingornikar, S., & Bhandari, R. R. (2023). Proactive early threat detection and securing Oracle Database with IBM QRadar, IBM Security Guardium Database Protection, and IBM Copy Services Manager by using IBM Flash System Safeguarded Copy (IBM Redbooks publication, REDP-5686-01). IBM Redbooks

220. Shyam, R., & Chakraborty, R. (2021). Machine learning and its dominant paradigms. Journal of Advancements in Robotics, 8(2), 1–10.

221. Sibe, R. T., & Kaunert, C. (2024). Implications for financial crime in Nigeria. In Cybercrime, digital forensic readiness, and financial crime investigation in Nigeria (149–177). Springer Nature Switzerland.

222. Siddiq, F. R., & Sutopo, B. (2024). The fraud hexagon as an analytical framework for predicting financial statement fraud: A systematic literature review. Aplikatif Journal of Research Trends in Social Sciences and Humanities, 3(2), 158-176

223. Simion, M., & Kelp, C. (2023). Trustworthy artificial intelligence. Asian Journal of Philosophy, 2(1), Article 8.

224. Singh, A., & Aggarwal, A. (2023). Securing microservices using OKTA in cloud environment: Implementation strategies and best practices. Journal of Science & Technology, 4(1), 11–39

225. Singh, V. B., Singh, P., Guha, S. K., Shah, A. I., Samdani, A., Nomani, M. Z. M., & Tiwari, M. (2024). The future of financial crime prevention and cybersecurity with distributed systems and computing approaches. In Meta-Heuristic Algorithms for Advanced Distributed Systems (19), 321–340. Wiley.

226. Singh, C. (2023). Artificial intelligence and deep learning: Considerations for financial institutions for compliance with the regulatory burden in the United Kingdom. Journal of Financial Crime, 31(2), 259–266.

227. Sleimi, M. T. (2020). Effects of risk management practices on banks' performance: An empirical study of the Jordanian banks. Management Science Letters, 10(2), 489–496.

228. Smit, J. (2024). A literature review on the impact of artificial intelligence on the future of banking and how to achieve a smooth transition. Open Journal of Business and Management, 12(1), 509–520.

229. Soltani, M., Kythreotis, A., & Roshanpoor, A. (2023). Two decades of financial statement fraud detection literature review: Combination of bibliometric analysis and topic modeling approach. Journal of Financial Crime, 30(5), 1367–1388.

230. Soori, M., Arezoo, B., & Dastres, R. (2023). Artificial intelligence, machine learning, and deep learning in advanced robotics: A review. Cognitive Robotics, 3, 100123, 54–70.

231. Southworth, R., & Levi, M. (2024). Application of the risk-based approach (RBA) for financial crime risk management by banks. In D. Goldarsht & L. de Koker (Eds.), Financial crime and the law: Identifying and mitigating risks, 115 (1), 101–121. Cham: Springer.

232. S&P Global. (2025, May). Qatar banking sector outlook 2025. Retrieved from https://www.spglobal.com

233. Srilatha, D., & Thillaiarasu, N. (2023). Implementation of intrusion detection and prevention with deep learning in cloud computing. Journal of Information Technology Management, 15(Special Issue), 1–18.

234. Srivastava, A., Pandiya, B., & Nautiyal, N. S. (2024). Application of artificial intelligence in risk assessment and mitigation in banks. Artificial Intelligence for Risk Mitigation in the Financial Industry, 1–25

235. Srivastava, A., Gupta, D., & Miryala, N. K. (2024). Leveraging Artificial Intelligence for Countering Financial Crimes. International Journal of Artificial Intelligence and Machine Learning, 2(1), 1–11.

236. Stryker, C., & Kavlakoglu, E. (2024, August 9). What is artificial intelligence (AI)? IBM. https://www.ibm.com/think/topics/artificial-intelligence

237. Tahiri, A., & El Arif, F. Z. (2024). Toward a mapping of compliance risk in banks. Journal of Financial Regulation and Compliance, 32(5), 633–645

238. Talati, D. (2024). AI (Artificial Intelligence) in daily life (techrxiv.170751714.46556037/v1). TechRxiv.

239. Tapeh, A. T. G., & Naser, M. Z. (2023). Artificial intelligence, machine learning, and deep learning in structural engineering: A scientometrics review of trends and best practices. Archives of Computational Methods in Engineering, 30(1), 1–80.

240. Tatineni, S., & Mustyala, A. (2024). Enhancing financial security: Data science's role in risk management and fraud detection. ESP International Journal of Advancements in Computational Technology (ESP-IJACT), 2(2), 94–105.

241. The Guardian. (2025, June 15). UK banks spend hundreds of millions combating cyberattacks. https://www.theguardian.com/business/2025/jun/15/uk-banks-hackers-attacks-cybersecurity

242. Thiebes, S., Lins, S., & Sunyaev, A. (2021). Trustworthy artificial intelligence. Electronic Markets, 31(2), 447–464.

243. Thommandru, A., & Chakka, B. (2024). Banking's new frontier: Overcoming anti-money laundering challenges with innovative technology. International Journal of Intellectual Property Management, 14(4), 367–381.

244. Todaro, D. (2024). Public sector AI applications in Shanghai. In The use of artificial intelligence in the public sector in Shanghai: Ambition, capacity, and reality (pp. 45–68). Singapore: Springer Nature Singapore.

245. Velez, S. B. (2024). Compliance and financial crime risk in banks: A practitioner's guide. Emerald Publishing Limited.

246. Waliullah, M., Hossain George, M. Z., Hasan, M. T., Alam, M. K., Khatun Munira, M. S., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review, (Preprint arXiv:2503.22710.) arXiv

247. Wang, B. (2024). A financial risk identification model based on artificial intelligence. Wireless Networks, 30(5), 4157–4165.

248. Wang, Y., Fu, E. Y., Zhai, X., Yang, C., & Pei, F. (2024). Introduction of artificial intelligence. In X. Huang & W. C. Tam (Eds.), Intelligent building fire safety and smart firefighting (pp. 65-97). Springer Nature Switzerland AG.

249. Wang, Y., Xu, Z., Yao, Y., Liu, J., & Lin, J. (2024). Leveraging convolutional neural network transformer synergy for predictive modeling in risk-based applications, (arxiv.org/abs/2412.18222). arXiv.

250. World Bank. (2024, Spring). Gulf economic update: Unlocking prosperity – Transforming education for economic breakthrough in the GCC [Report No. IDU18aa68e891ea20146a119b9512b9f6b39facc]. International Bank for Reconstruction and Development.

251. Xu, N. H., Niu, N. K., Lu, N. T., & Li, N. S. (2024). Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects. Engineering Science & Technology Journal, 5(8), Article 1363.

252. Yan, Z., & Juma'h, A. H. (2023). The role of big data analytics in preventing financial crimes. International Journal of Financial Studies, 11(1), 1-39.

253. Younis, H. A., Eisa, T. A. E., Nasser, M., Sahib, T. M., Noor, A. A., Alyasiri, O. M., Salisu, S., Hayder, I. M., & Younis, H. A. (2024). A systematic review and meta-analysis of artificial intelligence tools in medicine and healthcare: Applications, considerations, limitations, motivation and challenges. Diagnostics, 14(1), Article 109, 1–38.

254. Yu, Q., Xu, Z., & Ke, Z. (2024). Deep learning for cross-border transaction anomaly detection in anti-money laundering systems, (arxiv.org/abs/2405.08842). arXiv.

255. Zador, A., Escola, S., Richards, B., Ölveczky, B., Bengio, Y., Boahen, K., Botvinick, M., Chklovskii, D., Churchland, A., Clopath, C., DiCarlo, J., Ganguli, S., Hawkins, J., Körding, K., Koulakov, A., LeCun, Y., Lillicrap, T., Marblestone, A., Olshausen, B., Tolias, A. S. (2023). Catalyzing next-generation Artificial Intelligence through NeuroAI. Nature Communications, 14(1), Article 1597.

256. Zarpala, L., & Casino, F. (2021). A blockchain-based forensic model for financial crime investigation: The embezzlement scenario. Digital Finance, 3, 301-332.

257. Zhang, B., Zhu, J., & Su, H. (2023). Toward the third-generation artificial intelligence. Science China Information Sciences, 66, 121101.

258. Zhang, C. J., Gill, A. Q., Liu, B., & Anwar, M. J. (2025). AI-based identity fraud detection: A systematic review, (preprint arXiv:2501.09239). arXiv

259. .Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224.

260. Zhang, H., Hong, J., Dong, F., Drew, S., Xue, L., & Zhou, J. (2023). A privacy-preserving hybrid federated learning framework for financial crime detection [Preprint arXiv.2302.03654]. arXiv

261. Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era: A survey. The Innovation, 2(4), 100176.

262. Zhuk, A. (2023). Artificial intelligence impact on the environment: Hidden ecological costs and ethical-legal issues. Journal of Digital Technologies and Law, 1(4), 932-954.

الملاحق

ملحق رقم (1)

تأثير الذكاء الاصطناعي على
إدارة مخاطر الجريمة المالية في القطاع المصرفي القطري

(استبيان أطروحة الدكتوراة في إدارة الأعمال/ النسخة الاستطلاعية)

نشأت جابر

باحث دكتوراة في إدارة الأعمال

الاكاديمية العربية للعلوم الإدارية والمالية والمصرفية

إشراف

أ.د. محمد شريف

أستاذ التمويل و الاستثمار

كلية التجارة – جامعة القاهرة

2024

استبيان أطروحة الدكتوراة في إدارة الأعمال

تأثير الذكاء الاصطناعي على
إدارة مخاطر الجريمة المالية في القطاع المصرفي القطري

أعزائي المشاركين

السلام عليكم ورحمة الله وبركاته

تحية طيبة وبعد

في إطار الأطروحة التي أقوم بإعدادها كمتطلب للحصول على درجة الدكتوراة في إدارة الأعمال، أجري استبيانا استقصائيا يتعلق بـ "تأثير الذكاء الاصطناعي على إدارة مخاطر الجرائم المالية في القطاع المصرفي بالتطبيق على القطاع المصرفي في دولة قطر". و في هذا السياق، أقدر لكم دعمكم لهذه الدراسة من خلال تخصيص 60 دقيقة من وقتكم الكريم للمشاركة في هذا الاستبيان الاستقصائي.

يهدف هذا الاستبيان الاستقصائي إلى استطلاع آرائكم الشخصية وخبراتكم حول هذا الموضوع؛ واضعين في الاعتبار أنه لا توجد إجابات صحيحة أو أخرى خاطئة لأسئلة هذا الاستبيان. كما نؤكد لكم أن جميع الإجابات التي تقدمونها في سياق هذا الاستبيان الاستقصائي ستظل سرية، ولن تستخدم إلا لأغراض البحث العلمي، و أنه لن يتم تقديم أي معلومات أو الإفصاح عن هوية أي فرد شارك في هذا الاستبيان، علما بأنكم غير مطالبين بضرورة ذكر الاسم. وعلاوة على ذلك، سيتم مناقشة نتائج هذا الاستبيان الاستقصائي بشكل عام إجمالي لا يفصح عن هوية أي من المشاركين فيه.

ويتكون الاستبيان من ثلاثة (3) أجزاء رئيسية على النحو التالي:

1. **الجزء الأول: المعلومات الشخصية للمشاركين ومعلومات عن جهة العمل (جميعها معلومات عامة غير سرية).**
2. **الجزء الثاني: أسئلة محددة حول إدارة مخاطر الجرائم المالية والذكاء الاصطناعي واستخداماته في البنك.**
3. **الجزء الثالث: الاستبيان الاستقصائي: يستخدم هذا الجزء مقياس ليكرت ذي الخمس نقاط والذي تتراوح درجات التقييم فيه من "لا أو افق بشدة" إلى "أو افق بشدة". وفيما يلي تصنيفات هذا المقياس:**

1	لا أو افق بشدة	2	لا أو افق	3	محايد	4	أو افق	5	أو افق بشدة

وختاما، أتقدم لحضراتكم جميعا بجزيل الشكر والعرفان على تعاونكم في استكمال أسئلة هذا الاستبيان وعلى تحرى الدقة والموضوعية عند الإجابة على كل سؤال.

تحياتي و تقديري

نشأت جابر

باحث دكتوراة إدارة الأعمال

الاكاديمية العربية للعلوم الإدارية والمالية والمصرفية

بيانات الاتصال

جوال وو اتس آب : 0097455932969

بريد اليكتروني

nashatgaber@hotmail.com

الجزء الأول: البيانات الشخصية وبيانات جهة العمل:

أ)- البيانات الشخصية:

الاسم:	..... (اختياري)				
النوع:	☐ ذكر	☐ أنثى			
العمر:	☐ أقل من 25 سنة	☐ 25 – 35 سنة	☐ 36 – 45 سنة	☐ 46 – 55 سنة	☐ أكبر من 55 سنة
المؤهل الدراسي:	☐ مؤهل فوق متوسط / ما يعادله	☐ بكالوريوس/ ما يعادله	☐ ماجستير/ ما يعادله	☐ دكتوراة / ما يعادلها	
مجال الدراسة:	.....				
الشهادات المهنية:	☐ نعم	☐ لا	للإجابة بنعم، رجاء ذكر الشهادة:		

ب) بيانات جهة العمل:

المنصب / المسمى الوظيفي الحالي:	.....	المستوى الوظيفي:	.....		
طبيعة الوظيفة:	☐ دوام كامل	☐ دوام جزئي	☐ تعاقد خارجي (Outsourced)		
الخبرة في القطاع المصرفي:	☐ 5 سنوات أو أقل	☐ 6 - 10	☐ 11 - 15	☐ 16 - 20	☐ 21 سنة أو أكثر
الإدارة:	.....	القسم / الوحدة:	.....		
البنك / المصرف:	.....				
ملكية البنك / المصرف:	☐ بنك مملوك للدولة	☐ بنك شبه حكومي	☐ بنك ذو ملكية خاصة		
جهة الترخيص و الإشراف الرقابي:	☐ مصرف قطر المركزي - QCB	☐ مركز قطر للمال – QFC			
نموذج الأعمال – Business Model:	☐ مصرف/ بنك اسلامي	☐ بنك تجاري تقليدي	☐ بنك متخصص		
الخدمات المقدمة:	☐ مصرفية الأفراد - Retail	☐ مصرفية الشركات - Corporate	☐ خدمات الاستثمار		
النطاق الجغرافي:	☐ بنك عالمي	☐ بنك أجنبي	☐ بنك وطني ذو تواجد دولي	☐ بنك وطني ذو تواجد محلي فقط	
أصول البنك:	☐ 10 مليار دولار أو أقل	☐ 11- 25 مليار دولار	☐ 26- 50 مليار دولار	☐ 51- 100 مليار دولار	☐ 101 مليار دولار أو أكثر
عدد فروع البنك في قطر:	.....	عدد فروع البنك خارج قطر:	.....		
عدد موظفي البنك:	.....	عدد موظفي الإدارة التي تعمل بها:	.....		

الجزء الثاني: أسئلة محددة عن إدارة المخاطر و الذكاء الاصطناعي في البنك لديكم:

أ)- إدارة مخاطر الجرائم المالية في البنك لديكم:

1- ما هي أنواع الجرائم المالية التي يواجهها البنك الذي تعمل به بشكل متكرر؟ (اذكر كل ما ينطبق)

- ☐ غسل الأموال
- ☐ تمويل الإرهاب
- ☐ تمويل انتشار أسلحة الدمار الشامل
- ☐ الاحتيال المالي
- ☐ خرق قرارات العقوبات و الجزاءات المالية المستهدفة
- ☐ الاحتيال السيبراني
- ☐ التزوير و التزييف
- ☐ الرشوة و الفساد
- ☐ أخرى، برجاء التكرم بذكرها أدناه:

2- ما هو معدل تعرض البنك الذي تعمل به للجرائم المالية؟

☐ بشكل يومي ☐ بشكل أسبوعي ☐ بشكل شهري ☐ بشكل سنوي ☐ نادرا

3- هل يتبع البنك الذي تعمل به إطارًا أو معيارًا محددًا لإدارة المخاطر (على سبيل المثال ISO 31000)؟

☐ نعم ☐ لا ☐ لا أعلم

4- إذا كانت الإجابة بنعم، يرجى تحديد الإطار أو المعيار المستخدم لإدارة مخاطر الجرائم المالية في البنك الذي تعمل به.

☐ ISO 31000 ☐ ISO/IEC 27001 ☐ ISO 37001 ☐ COSO Framework ☐ أخرى، برجاء التكرم بذكرها أدناه:

5- ما هو معدل قيام البنك الذي تعمل به بإجراء تقييم للمخاطر لتحديد نقاط الضعف المحتملة للجرائم المالية؟

☐ بشكل سنوي ☐ بشكل نصف سنوي ☐ بشكل ربع سنوي ☐ بشكل شهري ☐ دائما / باستمرار

6- في البنك الذي تعمل به، ما هو متوسط وقت الاستجابة لمعالجة حادث الاشتباه في وقوع جريمة مالية؟

☐ أقل من ساعة ☐ 1-3 ساعات ☐ 3-6 ساعات ☐ 6-12 ساعة ☐ أكثر من 12 ساعة

ب)- استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في البنك لديكم:

1- هل يستخدم البنك الذي تعمل به حاليًا أي حلول مدعومة بالذكاء الاصطناعي لإدارة مخاطر الجرائم المالية؟

☐ نعم ☐ لا ☐ لست متأكداً

2- إذا كانت الإجابة بنعم، يرجى تحديد أنظمة الذكاء الاصطناعي المستخدمة لإدارة مخاطر الجرائم المالية في البنك الذي تعمل به.

- ☐ تطبيقات تعلم الآلة / Machine Learning Applications
- ☐ تطبيقات التعلم العميق/ Deep Learning Applications
- ☐ تطبيقات معالجة اللغات الطبيعية/ Natural Language Processing
- ☐ تطبيقات التحليل الشبكي / Graph Analytics Applications
- ☐ تطبيقات التحليل التنبؤي/ Predictive Analytics Applications
- ☐ تقنيات الكشف عن الحالات الشاذة / Anomaly Detection Apps
- ☐ تطبيقات النظم الخبيرة / Expert Systems Applications
- ☐ تطبيقات رؤية الحاسب / Computer Vision Applications
- ☐ تطبيقات تحليل السلاسل الزمنية / Time Series Analysis Apps
- ☐ أخرى، برجاء التكرم بذكرها أدناه:

-3 إذا كانت الإجابة بنعم، منذ متى يستخدم البنك الذي تعمل به تطبيقات الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية؟

☐ أقل من عام ☐ 1-2 عام ☐ 3-5 أعوام ☐ أكثر من 5 أعوام

-4 إذا كانت الإجابة بنعم، كم حجم الميزانية السنوية التي يخصصها البنك للمبادرات المتعلقة بالذكاء الاصطناعي لإدارة مخاطر الجرائم المالية؟

☐ أقل من 1 مليون دولار ☐ 1-5 مليون دولار ☐ 6 – 10 مليون دولار ☐ أكثر من 10 مليون دولار ☐ لست متأكداً

-5 إذا كانت الإجابة بنعم، كيف تقيم مستوى معرفتك وخبرتك في استخدام أدوات الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية؟

☐ ليس لدي خبرة ☐ مبتدئ ☐ متوسط ☐ متقدم ☐ خبير

-6 هل تلقيت أي تدريب حول تكنولوجيا الذكاء الاصطناعي و/أو استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية؟

☐ نعم، تلقيت تدريباً ☐ لا، لم أتلق تدريباً.

-7 إذا كانت الإجابة بنعم، ما هو مستوى التدريب الذي تلقيته؟

☐ أساسي /تمهيدي ☐ متوسط ☐ متقدم / متخصص

-8 إذا كانت الإجابة بنعم، ما هي المدة الإجمالية للتدريب الذي تلقيته؟

☐ أقل من أسبوع ☐ 1 أسبوع – 1 شهر ☐ 1- شهر – 6 أشهر ☐ 6 أشهر أو أكثر

الجزء الثالث: الاستبيان الاستقصائي:

يرجى وضع علامة (✓) في المساحة التي تمثل رأيك فيما يتعلق بكل من العبارات التالية.

أولا: إدارة المخاطر والجرائم المالية في القطاع المصرفي

م	العبارة	الاجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
-1	يواجه البنك الذي أعمل به مخاطر كبيرة ناجمة عن الجرائم المالية.					
-2	يزيد تعقيد المعاملات الحالية من تعرض البنك لمخاطر الجرائم المالية.					
-3	يواجه البنك مخاطر كبيرة بسبب الجرائم المالية الناجمة عن التقنيات الناشئة.					
-4	كان للجرائم المالية تأثير مالي كبير على البنك الذي أعمل به في الماضي.					
-5	لقد أثرت الجرائم المالية سلبًا على سمعة البنك الذي أعمل به في الماضي.					
-6	واجه البنك عقوبات قانونية وتنظيمية بسبب الجرائم المالية في الماضي.					
-7	يتمتع البنك الذي أعمل به بثقافة قوية للامتثال والسلوك الأخلاقي.					
-8	يتمتع البنك بإطار عمل دقيق وشامل لإدارة مخاطر الجرائم المالية.					
-9	تشكل مكافحة الجرائم المالية أولوية قصوى في استراتيجية إدارة المخاطر في البنك.					
-10	يضع مجلس إدارة والإدارة العليا في البنك مكافحة الجرائم المالية على رأس أولوياتهم.					
-11	يتابع مجلس إدارة البنك والإدارة العليا بشكل دوري وجاد تنفيذ ومراجعة وتحديث سياسات مكافحة الجرائم المالية.					
-12	يتعامل البنك مع حوادث الجرائم المالية من خلال عملية واضحة للإبلاغ والتحقيق واتخاذ الإجراءات المناسبة.					
-13	يقوم البنك بإجراء عمليات تدقيق داخلية وخارجية بشكل منتظم لتقييم ممارسات إدارة مخاطر الجرائم المالية.					
-14	يوجد لدى البنك فريق متخصص مسؤول عن إدارة مخاطر الجرائم المالية.					
-15	نشجع موظفي البنك على الإبلاغ عن أي أنشطة مشبوهة دون خوف من الانتقام.					
-16	يوفر البنك للموظفين تدريبًا كافيًا ومستمرًا لمكافحة الجرائم المالية.					

ثانيا: استخدام الذكاء الاصطناعي في إدارة المخاطروالجر ائم المالية في القطاع المصرفي

القسم الأول: المعرفة العامة حول استخدام الذكاء الاصطناعي في إدارة مخاطر الجر ائم المالية في القطاع المصرفي

م	العبارة	الاجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
-17	لدي فهم جيد للذكاء الاصطناعي وتطبيقاته واستخداماته في إدارة مخاطر الجرائم المالية.					
-18	أعتقد أن الذكاء الاصطناعي أداة قيمة ويمكنه تحسين وتعزيز كفاءة ودقة إدارة مخاطر الجرائم المالية في القطاع المصرفي.					
-19	أنا منفتح للغاية على دمج تطبيقات الذكاء الاصطناعي في أنشطتي اليومية في إدارة مخاطر الجرائم المالية.					
-20	أوصي زملائي بشدة باستخدام الذكاء الاصطناعي في القطاع المصرفي.					

القسم الثاني: و اقع الاستخدام الحالي للذكاء الاصطناعي في إدارة مخاطر الجر ائم المالية في القطاع المصرفي

أ)- الاستخدام العام وتأثير الذكاء الاصطناعي على إدارة مخاطر الجر ائم المالية

-21	الذكاء الاصطناعي هو جزء لا يتجزأ من استراتيجية إدارة المخاطر الشاملة في البنك.					
-22	يتبنى البنك بفاعلية نماذج الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية.					
-23	أدى تبني الذكاء الاصطناعي إلى تحسين الكفاءة والدقة الشاملة لعمليات إدارة مخاطر الجرائم المالية في البنك.					
-24	أدى استخدام الذكاء الاصطناعي إلى تقليل التكاليف التشغيلية لإدارة مخاطر الجرائم المالية في البنك.					
-25	أدى تبني الذكاء الاصطناعي إلى تحسين التعاون بين الإدارات في إدارة مخاطر الجرائم المالية.					

م	العبارة	الاجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
-26	أدى تبني الذكاء الاصطناعي إلى تحسين القدرة الشاملة على حماية البنك وأصحاب المصلحة من الجرائم المالية.					
-27	أدى استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية إلى زيادة ثقة جميع أصحاب المصلحة في البنك.					
-28	إن استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية يمنح البنك ميزة تنافسية.					
-29	يتبع البنك سياسات وإرشادات واضحة لضمان الاستخدام الأخلاقي للذكاء الاصطناعي في إدارة مخاطر الجرائم المالية.					
-30	يتم تدقيق ومراجعة أنظمة الذكاء الاصطناعي المستخدمة لإدارة مخاطر الجرائم المالية في البنك بانتظام للتأكد من أنها تعمل بشكل صحيح وفعال.					
-31	يلتزم مجلس إدارة البنك والإدارة العليا باستخدام الحلول القائمة على الذكاء الاصطناعي لتعزيز إدارة مخاطر الجرائم المالية.					
-32	يلتزم البنك باستكشاف وزيادة استثماراته باستمرار لتبني حلول جديدة تعتمد على الذكاء الاصطناعي لتعزيز إدارة مخاطر الجرائم المالية.					

ب)- استخدام الذكاء الاصطناعي وتأثيره في تحديد مخاطر الجرائم المالية						
-33	عززت أدوات الذكاء الاصطناعي من قدرة البنك على إجراء مراقبة المعاملات في الوقت الفعلي للجرائم المالية المحتملة.					
-34	أعتقد أن نماذج الذكاء الاصطناعي موثوقة في توفير تنبؤات وتوقعات أكثر دقة وكفاءة وفي الوقت المناسب فيما يتعلق بإدارة مخاطر الجرائم المالية في البنك.					
-35	أدى استخدام نماذج الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في البنك إلى تقليل عدد التنبيهات التي تتطلب التحقيق.					
-36	الذكاء الاصطناعي دقيق وفعال في التمييز بين المعاملات المشروعة وأنشطة الجرائم المالية المحتملة وبالتالي قلل من عدد نتائج التطابق الايجابي الكاذبة (False Positives)					
-37	أدى تبني الذكاء الاصطناعي إلى زيادة قدرة البنك على ربط الأنشطة المشبوهة ذات الصلة عبر حسابات أو عملاء مختلفين بشكل أكثر فعالية من العمليات اليدوية.					
-38	أدى تبني الذكاء الاصطناعي إلى تقليل التحيز البشري في تحديد الجرائم المالية المحتملة.					
ج)- استخدام الذكاء الاصطناعي وتأثيره في تحليل وتقييم مخاطر الجرائم المالية						
-39	حسّن الذكاء الاصطناعي سرعة ودقة وكفاءة تحليل مخاطر الجرائم المالية لدينا.					
-40	يوفر الذكاء الاصطناعي تحليلاً فعالاً للمعاملات في الوقت الفعلي، مما يتيح الكشف بشكل أسرع عن الأنشطة المشبوهة وتعزيز قدرتنا على تحليل مخاطر الجرائم المالية					
-41	قدمت التحليلات المدعومة بالذكاء الاصطناعي رؤى أعمق وأكثر قابلية للتنفيذ لدعم قرارات إدارة مخاطر الجرائم المالية لدينا.					
-42	ساعدنا الذكاء الاصطناعي على فهم العلاقة بين العديد من مخاطر الجرائم المالية بشكل أفضل.					
-43	ساعدتنا نماذج الذكاء الاصطناعي على فهم الدوافع وراء الجرائم المالية بشكل أفضل.					
-44	حسّن الذكاء الاصطناعي جودة وعمق تقارير تحليل مخاطر الجرائم المالية لدينا.					
-45	أصبح تقييم مخاطر الجرائم المالية أسرع وأكثر شمولاً ودقة وفعالية مع استخدام أدوات الذكاء الاصطناعي.					
-46	أدت أدوات تقييم مخاطر الجرائم المالية المدعومة بالذكاء الاصطناعي في البنك إلى تحسين تحديد أولويات الحالات عالية المخاطر لمزيد من التحقيق.					
-47	أدوات الذكاء الاصطناعي موثوقة في تقييم شدة وتأثير مخاطر الجرائم المالية التي تم تحديدها..					
-48	أدى الذكاء الاصطناعي إلى تحسين موضوعية تقييمات المخاطر لدينا، مما قلل من التحيزات المحتملة.					
د)- استخدام الذكاء الاصطناعي وتأثيره في معالجة مخاطر الجرائم المالية						
-49	عزز الذكاء الاصطناعي من قدرة البنك على منع وقوع الجرائم المالية.					
-50	عزز الذكاء الاصطناعي قدرتنا على اكتشاف الأنشطة المشبوهة والاستجابة لها بسرعة أكبر.					
-51	يلعب الذكاء الاصطناعي دورًا حاسمًا في اقتراح وتنفيذ وتطوير التدابير المناسبة للتخفيف من مخاطر الجرائم المالية التي تم تحديدها.					
-52	يساعد الذكاء الاصطناعي البنك في تنفيذ تدابير استباقية ضد الجرائم المالية.					
-53	أدى الذكاء الاصطناعي إلى زيادة سرعة الاستجابة لحوادث الجرائم المالية المحتملة بشكل كبير.					
هـ)- استخدام الذكاء الاصطناعي وتأثيره في مراقبة ومراجعة مخاطر الجرائم المالية						

-54	أنا راضٍ عن مستوى الأتمتة الذي جلبته الذكاء الاصطناعي لمهام مراقبة ومراجعة مخاطر الجرائم المالية.					
-55	حسنت أنظمة الذكاء الاصطناعي الدقة وقللت من الأخطاء في مراقبة ومراجعة مخاطر الجرائم المالية في البنك.					
-56	أدى الرصد الآلي المدعوم بالذكاء الاصطناعي إلى تقليل عبء العمل على فريق مكافحة الجرائم المالية لدينا.					
-57	تعمل أنظمة الذكاء الاصطناعي على تقليل الوقت المطلوب لمراقبة ومراجعة مخاطر الجرائم المالية.					
-58	توفر أدوات الذكاء الاصطناعي تقارير شاملة تساعد في المراقبة المستمرة للمخاطر وتحسين جودة وتوقيت هذه التقارير.					
-59	أدى دمج الذكاء الاصطناعي إلى تحسين قدرة البنك على التعامل مع كميات كبيرة من البيانات لمراقبة المخاطر ومراجعتها.					
و)- استخدام الذكاء الاصطناعي وتأثيره على الالتزام / الامتثال التنظيمي						
-60	يساعد الذكاء الاصطناعي البنك في ضمان الامتثال للوائح ومتطلبات الجرائم المالية.					
-61	عمل الذكاء الاصطناعي على تبسيط عمليات إعداد التقارير التنظيمية لدينا، مما يجعل هذه التقارير أكثر كفاءة ودقة وشمولاً وعمقًا لتلبية المتطلبات التنظيمية.					
-62	يشارك فريق الالتزام/ الامتثال التنظيمي بالبنك بنشاط في تنفيذ الحلول القائمة على الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية.					
القسم الثالث: التحديات والعوائق التي تواجه استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي						
-63	يثير تطبيق الذكاء الاصطناعي في مراقبة الجرائم المالية مخاوف أخلاقية بشأن خصوصية البيانات واستخدامها.					
-64	تشكل جودة البيانات وتوافرها تحديًا كبيرًا للبنك في تطبيق الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية.					
-65	يواجه البنك تحديات تكنولوجية في دمج أنظمة إدارة مخاطر الجرائم المالية القائمة على الذكاء الاصطناعي مع الأنظمة الحالية.					
-66	تشكل التكلفة العالية لتطبيق الذكاء الاصطناعي عائقًا كبيرًا أمام البنك لتبني الذكاء الاصطناعي لإدارة مخاطر الجرائم المالية.					
-67	يثير تطبيق الذكاء الاصطناعي مخاوف كبيرة بشأن الأمن السيبراني وخاصة إمكانية التلاعب بأنظمة الذكاء الاصطناعي أو تجاوزها من قبل المجرمين.					
-68	إن الافتقار إلى الموظفين المهرة والخبرة في استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية يشكل تحديًا يواجهه البنك.					
-69	هناك مقاومة كبيرة من أصحاب المصلحة في تبني تقنيات الذكاء الاصطناعي في عمليات إدارة مخاطر الجرائم المالية.					
-70	يخلق الافتقار إلى التوجيه التنظيمي الواضح بشأن استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية حالة من عدم اليقين.					
القسم الرابع: مستقبل استخدام الذكاء الاصطناعي في إدارة مخاطر الجرائم المالية في القطاع المصرفي						
-71	أعتقد أن الذكاء الاصطناعي سيلعب دورًا متزايد الأهمية في إدارة مخاطر الجرائم المالية في القطاع المصرفي في المستقبل القريب.					
-72	أعتقد أن الذكاء الاصطناعي سيقلل بشكل أكبر من الجهد اليدوي المطلوب في إدارة مخاطر الجرائم المالية					
-73	أعتقد أن الذكاء الاصطناعي سيخلق أدوارًا وفرص عمل جديدة في إدارة مخاطر الجرائم المالية في القطاع المصرفي.					

ملحق رقم (2)

تأثير الذكاء الاصطناعي على
إدارة مخاطر الجريمة المالية في القطاع المصرفي القطري

(النسخة النهائية المعتمدة من استبانة أطروحة الدكتوراة في إدارة الأعمال)

نشأت جابر

باحث دكتوراه في إدارة الأعمال

الأكاديمية العربية للعلوم الإدارية والمالية والمصرفية

إشراف

أ.د. محمد شريف

أستاذ التمويل والاستثمار

كلية التجارة – جامعة القاهرة

2025

استبانة أطروحة الدكتوراه في إدارة الأعمال

تأثير الذكاء الاصطناعي على
إدارة مخاطر الجريمة المالية في القطاع المصرفي القطري

السادة المشاركين،

السلام عليكم ورحمة الله وبركاته

تحية طيبة وبعد؛

في إطار الأطروحة التي أقوم بإعدادها كمتطلب للحصول على درجة الدكتوراه في إدارة الأعمال، أجريت استبانة استقصائية تتعلق بـ **"تأثير الذكاء الاصطناعي على إدارة مخاطر الجرائم المالية في القطاع المصرفي بالتطبيق على القطاع المصرفي في دولة قطر"**، وفي هذا السياق أقدر لكم دعمكم لهذه الدراسة من خلال تخصيص ما لا يزيد عن 30 دقيقة من وقتكم الكريم للمشاركة في هذه الاستبانة الاستقصائية.

تهدف هذا الاستبانة الاستقصائية إلى استطلاع آرائكم الشخصية وخبراتكم حول هذا الموضوع؛ واضعين في الاعتبار أنه لا توجد إجابات صحيحة أو أخرى خاطئة لأسئلة هذه الاستبانة، كما نؤكد لكم أن جميع الإجابات التي تقدمونها في سياق هذه الاستبانة الاستقصائية ستظل سرية، ولن تستخدم إلا لأغراض البحث العلمي، وأنه لن يتم تقديم أي معلومات أو الإفصاح عن هوية أي فرد شارك في هذا الاستقصاء، علما بأنكم غير مطالبين بضرورة ذكر الاسم، وعلاوة على ذلك سيتم مناقشة نتائج هذه الاستبانة الاستقصائية بشكل عام إجمالي لا يفصح عن هوية أي من المشاركين فيه.

وتتكون الاستبانة من جزئين رئيسيين على النحو التالي:

1. **الجزء الأول: المعلومات الشخصية للمشاركين ومعلومات عن جهة العمل (جميعها معلومات عامة غير سرية).**
2. **الجزء الثاني: الاستبانة الاستقصائية: يستخدم هذا الجزء مقياس ليكرت ذي الخمس نقاط، والذي تتراوح درجات التقييم فيه من: "لا أو افق بشدة"، إلى: "أو افق بشدة"، وفيما يلي تصنيفات هذا المقياس:**

1	لا أو افق بشدة	2	لا أو افق	3	محايد	4	أو افق	5	أو افق بشدة

وختاما، أتقدم لحضراتكم جميعا بجزيل الشكر والعرفان على تعاونكم في استكمال أسئلة هذا الاستقصاء، وعلى تحرى الدقة والموضوعية عند الإجابة عن كل سؤال.

تحياتي وتقديري

نشأت جابر

باحث دكتوراه إدارة الأعمال

الأكاديمية العربية للعلوم الإدارية والمالية والمصرفية

جوال وو اتس آب: 00974-55932969

بريد إلكتروني: nashatgaber@hotmail.com

الجزء الأول: البيانات الشخصية وبيانات جهة العمل:

أ)- البيانات الشخصية:

الاسم:	..... (اختياري)			
النوع:	☐ ذكر	☐ أنثى		
العمر:	☐ 25 – 35 سنة	☐ 36 – 45 سنة	☐ 46 – 55 سنة	☐ أكبر من 55 سنة
المؤهل الدراسي:	☐ بكالوريوس/ ما يعادله	☐ دبلوم دراسات عليا/ ما يعادله	☐ ماجستير/ ما يعادله	☐ دكتوراة / ما يعادلها

ب) بيانات جهة العمل:

المنصب / المسمى الوظيفي الحالي:	.....	المستوى الوظيفي:	.....		
طبيعة الوظيفة:	☐ دوام كامل	☐ دوام جزئي	☐ تعاقد خارجي (Outsourced)		
الخبرة في القطاع المصرفي:	☐ 5 سنوات أو أقل	☐ 6 - 10	☐ 11 - 15	☐ 16 - 20	☐ 21 سنة أو أكثر
الإدارة:	.....	القسم / الوحدة:	.....		
البنك / المصرف:	.....				
ملكية البنك / المصرف:	☐ بنك مملوك للدولة	☐ بنك ذو ملكية مشتركة	☐ بنك ذو ملكية خاصة		
نموذج الأعمال – Business Model:	☐ مصرف/ بنك إسلامي	☐ بنك تجاري تقليدي	☐ بنك متخصص		
الخدمات المقدمة:	☐ مصرفية الأفراد - Retail	☐ مصرفية الشركات - Corporate	☐ خدمات الاستثمار		
النطاق الجغرافي:	☐ بنك عالمي	☐ بنك أجنبي	☐ بنك وطني ذو تواجد دولي	☐ بنك وطني ذو تواجد محلي فقط	
أصول البنك:	☐ 10 مليار دولار أو أقل	☐ 11- 25 مليار دولار	☐ 26- 50 مليار دولار	☐ 51- 100 مليار دولار	☐ 101 مليار دولار أو أكثر
عدد فروع البنك في قطر:	.....	عدد فروع البنك خارج قطر:	.....		
عدد موظفي البنك:	.....	عدد موظفي الإدارة التي تعمل بها:	.....		

الجزء الثاني: تأثير الذكاء الاصطناعي على إدارة مخاطر الجرائم المالية في القطاع المصرفي

يرجى وضع علامة (✓) في المساحة التي تمثل رأيك فيما يتعلق بكل من العبارات التالية:

أولاً: الذكاء الاصطناعي						
م	العبارة	الإجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
-1	تعزز أنظمة الذكاء الاصطناعي القدرة على التنبؤ بحدوث مخاطر الجريمة المالية قبل وقوعها .					
-2	يسهم استخدام النظم الخبيرة في تحسين قدرة المؤسسات على كشف عمليات الاحتيال المالي بشكل أسرع وأكثر دقة .					
-3	تساعد النظم الخبيرة في وضع قواعد وإستراتيجيات مخصصة للكشف عن الأنشطة المشبوهة .					
-4	تسهم النظم الخبيرة في تحسين إدارة البيانات وتحليلها بشكل أكثر كفاءة .					
-5	يعزز تعلم الآلة من قدرة أنظمة إدارة المخاطر على التعرف على أنماط الجرائم المالية المستجدة .					
-6	يعزز تعلم الآلة من قدرة أنظمة المراقبة على التكيف مع تغير أساليب الجرائم المالية .					
-7	يرفع تعلم الآلة من مستوى الأمان في أنظمة المؤسسات المالية ضد عمليات الاحتيال والجرائم المالية .					
-8	يسهم التعلم العميق في التعرف على عمليات غسيل الأموال بشكل أكثر دقة وفعالية .					
-9	يساعد التعلم العميق في اكتشاف أنماط غير تقليدية في البيانات المالية قد تشير إلى عمليات غسيل أموال .					
-10	يسهم التعلم العميق في تحسين تصنيف المعاملات المشبوهة وتقليل الإنذارات الكاذبة .					
-11	يتيح الذكاء الاصطناعي التوليدي إنشاء تقارير وتحليلات دقيقة بشكل تلقائي لمساعدة فرق إدارة مخاطر الجريمة المالية.					
-12	يتيح الذكاء الاصطناعي التوليدي توليد سيناريوهات محتملة لحدوث الجرائم المالية لمزيد من الاستعداد .					
-13	يتيح الذكاء الاصطناعي التوليدي تصميم نماذج وتوقعات دقيقة لمخاطر الجرائم المالية.					
-14	تسهم الأتمتة الروبوتية في تقليل الأخطاء البشرية وتحسين سرعة استجابة المؤسسات لمخاطر الجرائم المالية .					
-15	تسهم العمليات الروبوتية في أتمتة إجراءات التحقيق وتقليل الوقت المستغرق فيها .					

ثانيًا: إدارة مخاطر الجرائم المالية في القطاع المصرفي

البُعد الأول: تحديد مخاطر الجريمة المالية

م	العبارة	الإجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
1	تساعد أتمتة عمليات الكشف عن مخاطر الجريمة المالية على تحديد الجرائم المالية بشكل أدق.					
2	تسهم نظم الذكاء الاصطناعي في التعرف المبكر على مؤشرات الجرائم المالية.					
3	يسهل تعلم الآلة عملية من تحديد أنماط الجرائم المالية غير الاعتيادية.					
4	تسهم تقنيات الذكاء الاصطناعي في توسيع نطاق الكشف عن مصادر الجرائم المالية.					
5	يُحسن الاعتماد على النظم الخبيرة من عملية تحديد مخاطر الجرائم المالية المحتملة.					
6	تساعد أدوات الذكاء الاصطناعي في تحديد مخاطر الجرائم المالية قبل وقوعها.					
7	تقلل تكنولوجيا الذكاء الاصطناعي من احتمالية التغاضي عن مخاطر الجرائم المالية.					

البُعد الثاني: تحليل وتقييم مخاطر الجريمة المالية

م	العبارة	الإجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
8	تتيح تقنيات التعلم العميق تحليل أكثر دقة لبيانات الجرائم المالية.					
9	تسهل نظم الذكاء الاصطناعي تقييم درجة خطورة كل خطر جريمة مالية.					
10	تساعد أدوات الذكاء الاصطناعي في تصنيف مخاطر الجرائم المالية حسب مستوى احتمالية حدوثها.					
11	تعلم تحليل البيانات باستخدام الآلة يسرع من عملية تقييم مخاطر الجريمة المالية.					
12	يسهم الذكاء الاصطناعي في تطوير نماذج تقييم مخاطر جريمة مالية أكثر موضوعية وفعالية					
13	يتم التقييم المستمر لمخاطر الجرائم المالية بشكل أكثر دقة باستخدام التقنيات الذكية.					
14	تقلل أدوات الذكاء الاصطناعي من الاعتماد على التقديرات الشخصية في تقييم مخاطر الجرائم المالية.					

البُعد الثالث: معالجة مخاطر الجريمة المالية

م	العبارة	الإجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
15	تسهم تطبيقات الذكاء الاصطناعي في تنفيذ إجراءات وقائية فعالة ضد الجرائم المالية.					
16	تساعد الأتمتة في الحد من الأخطاء البشرية أثناء معالجة مخاطر الجريمة المالية.					
17	تُمكن نظم الذكاء الاصطناعي من اتخاذ إجراءات تصحيحية بسرعة عند اكتشاف خطر جريمة مالية.					
18	يقلل استخدام الروبوتات في العمليات من احتمالية التلاعب المالي.					
19	تسهم أدوات الذكاء الاصطناعي في تطبيق سياسات مكافحة الجرائم المالية بشكل أكثر فاعلية.					
20	تقلل الأتمتة من التكلفة والوقت اللازم لمعالجة مخاطر الجريمة المالية.					
21	تدعم أنظمة الذكاء الاصطناعي وضع خطط استجابة مرنة لمخاطر الجريمة المالية المكتشفة.					

البُعد الرابع: مراقبة ومراجعة مخاطر الجريمة المالية						
م	العبارة	الإجابة				
		لا أو افق بشدة	لا أو افق	محايد	أو افق	أو افق بشدة
22	تُمكن نظم الذكاء الاصطناعي من المراجعة الدورية لمخاطر الجرائم المالية.					
23	تساعد أدوات التحليل الذكية في رصد التطورات الجديدة في أنماط الجرائم المالية.					
24	تُمكن المراقبة المستمرة باستخدام التقنيات الذكية من تحديث إستراتيجيات إدارة مخاطر الجرائم المالية.					
25	تسهم تقنيات التعلم العميق في التعرف على التغيرات في أساليب ارتكاب الجرائم المالية.					
26	توفر نظم الذكاء الاصطناعي تقارير دورية دقيقة عن حالة المخاطر ذات الصلة بالجرائم المالية.					
27	تُمكن نظم الذكاء الاصطناعي من مراقبة ومراجعة المخاطر بشكل دوري مما يمكن من تعديل إجراءات إدارة مخاطر الجريمة المالية بشكل فعال.					
28	تسهل أدوات الذكاء الاصطناعي عملية تتبع الأداء في إدارة مخاطر الجرائم المالية.					

ملحق رقم (3)

ملخص الدراسات السابقة

أ. ملخص الدراسات السابقة المتعلقة بالمتغير المستقل "الذكاء الاصطناعي":

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2023	الجزائر	الأسد صالح الأسد	الذكاء الاصطناعي: الفرص والمخاطر والواقع في الدول العربية	تبني تقنيات وتطبيقات الذكاء الاصطناعي في الدول العربية	▪ هدفت الدراسة إلى التعرف على فرص ومخاطر استخدام الذكاء الاصطناعي، وواقع الدول العربية في هذا المجال. ▪ خلصت الدراسة إلى أن الذكاء الاصطناعي يوفّر فرصًا واعدة تتطلب استغلالها من خلال بناء قاعدة علمية وتقنية متينة، مع التحسّب لمخاطره ووضع حلول للحد من آثاره السلبية. وأشارت إلى تفاوت واقع الدول العربية؛ فبعضها أحرز تقدمًا عمليًا حقيقا، والبعض الآخر لا زال في مرحلة الإستراتيجيات المكتوبة فقط، بينما فريق ثالث لا يزال بعيدًا عن دخول هذا المجال.
2023	الولايات المتحدة الأمريكية	Zador et al	Catalyzing Next-Generation of Artificial Intelligence through NeuroAI	مجال الذكاء الاصطناعي العصبي	▪ هدفت الدراسة لتقديم نظرة شاملة للمفاهيم الأساسية في علم الأعصاب والذكاء الاصطناعي، والذكاء الاصطناعي العصبي، وإبراز أهمية توظيف معارف الدماغ في تطوير أنظمة ذكية، وتشجيع التفاعل بين المجالين لتطوير وكلاء ذكيين بقدرات بشرية، ونماذج اصطناعية تحاكي سلوك الحيوانات بدقة عبر أجسام افتراضية في بيئات محاكاة. ▪ توصلت الدراسة إلى أن النظم الحالية للذكاء الاصطناعي تفتقر للقدرات الحسية-الحركية؛ إذ تركز جهود التطوير حاليا على تطبيقات تعلم الآلة أكثر من تطبيقات الذكاء الاصطناعي العصبي؛ ولذا يجب الاستثمار في البحث فيما يسمى "الذكاء الاصطناعي العصبي"، حيث إن ذلك سيقربنا من تحقيق الذكاء العام الاصطناعي.
2023	المملكة المتحدة	Mona Simion & Christoph Kelp	Trustworthy Artificial Intelligence	مجال الذكاء الاصطناعي الموثوق	▪ هدفت هذه الدراسة إلى تطوير الأدبيات العلمية بتقديم تعريف واضح للذكاء الاصطناعي الموثوق باستخدام مفهوم الالتزامات الوظيفية. ▪ توصلت الدراسة إلى أن الذكاء الاصطناعي الموثوق هو الذي يحقق معايير أداء التزاماته بقوة إرادة قصوى، وإلى عدم جدوى استخدام معايير نفسية، كالإرادة الحسنة أو الصفات الشخصية، في تعريف الذكاء الاصطناعي الموثوق، كما قدمت إطارا مفاهيميًا يحدد الالتزامات المرتبطة بوظائف الأنظمة الذكية.
2022	إسبانيا	Garrido-Merch & Blanco	Do Artificial Intelligence Systems Understand?	قدرات الفهم الذاتي لنماذج الذكاء الاصطناعي وكيفية تمثيل هذه النماذج للمعرفة وتعلم الأنماط من البيانات	▪ هدفت هذه الدراسة إلى مناقشة والتحقق مما إذا كانت أنظمة الذكاء الاصطناعي الحالية قادرة على الفهم أم لا. ▪ وتوصلت الدراسة إلى أن الفهم يتطلب الحدس والمرجعية الذاتية، بينما الأنظمة الحالية من الذكاء الاصطناعي تعالج المعلومات فقط من خلال اتباع التعليمات أو الأنماط المستنتجة إحصائيًا؛ فهي لا تفهم المعاني ومن ثمَّ تفتقد المرجعية الذاتية حاليا، رغم أنها لا تستبعد أن يحمل المستقبل تطويرا لأنظمة تتمتع بالذاتية والحالات العقلية من خلال التعلم الذاتي المعقد بشكل كبير.

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2022	أيرلندا	Abeba Birhane	Automating Ambiguity: Challenges and Pitfalls of Artificial Intelligence	مجال أنظمة تعلم الآلة (ML)	▪ هدفت الدراسة لتعزيز العدالة والمساواة في مجال أنظمة تعلم الآلة عبر تحليل منهجي لأبحاثها لمعالجة مشكلاتها وتحديد اتجاهاتها المستقبلية. ▪ أثبتت الدراسة صعوبة التنبؤ الدقيق بالسلوك البشري لتعقيده وعدم قابلية البشر للتحديد، وأن افتراضات أنظمة تعلم الآلة تمثل "ظلمًا خوارزميًا" يكرّس الصور النمطية ويضر بالفئات المهمشة، وكشفت عدم دقة بعض تطبيقات رؤية الحاسب، مثل التعرف على الوجوه، مما يشكل خطرًا على المستخدمين، واقترحت إطارا أخلاقيًا يراعي الأبعاد الاجتماعية والبيئية، لضمان ذكاء اصطناعي عادل ومفيد.
2022	الهند، العراق، الأردن، تركيا، الولايات المتحدة الأمريكية	Aggarwal et al.	Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning	استخدام الذكاء الاصطناعي وتطبيقاته المختلفة في تحليل البيانات و اتخاذ القرارات في القطاعات الصحية	▪ هدفت هذه الدراسة إلى تبسيط مفاهيم الذكاء الاصطناعي، وشرح آلية عمل تقنياته وتطبيقاته المختلفة، وتحليل مجالاته البحثية وتطبيقاته، مع مناقشة مزاياه وتحدياته واستشراف مستقبله، بهدف تعزيز الفهم وتشجيع اعتماده في مختلف المجالات، وتقديم مرجع شامل حوله. ▪ وخلصت الدراسة إلى أن الذكاء الاصطناعي سيواصل التطور والتقدم، وأوصت الدراسة بالاعتماد على نماذج تعلم الآلة والتعلم العميق لتعزيز التنبؤ وصنع القرار، وتحليل البيانات الضخمة لتقليل التدخل البشري.
2021	الصين الولايات المتحدة الأمريكية	Zhang and Lu	Study on Artificial Intelligence: The State of the Art and Future Prospects	الآفاق المستقبلية للذكاء الاصطناعي(AI) واحتمالات تطوره	▪ هدفت هذه الدراسة إلى تقديم مراجعة منهجية عن الذكاء الاصطناعي تعتمد على تكامل المعلومات الصناعية، مع عرض شامل للذكاء الاصطناعي وخلفيته ودوافعه، وتقنياته، وتطبيقاته المختلفة. ▪ وخلصت الدراسة إلى أن الذكاء الاصطناعي لا يتطلب فقط التفكير المنطقي والتقليد، بل يتطلب أيضًا العاطفة، حيث إنها جزء لا غنى عنه، وأن الذكاء الاصطناعي - مع استمرار تطوره - قد يتجاوز قريبا قدرات الاستدلال المنطقي للحواسيب من خلال منحه هذه الحواسيب والأنظمة الذكية قدرات عاطفية، ومن ثمَّ فقد يتجاوز ذكاء الآلة قريبًا ذكاء الإنسان.
2018	فرنسا الجزائر	قمورة ومحمد وكروش	الذكاء الاصطناعي بين الو اقع والمأمول، دراسة تقنية وميدانية	أسس الذكاء الاصطناعي وخصائصه ودراسة بعض نماذجه	▪ هدفت هذه الدراسة إلى رسم صورة واضحة للتطورات الحالية في التقنيات الذكية ومستقبلها، خاصة في مجالات الوسط الأكاديمي، مما يتيح للباحثين متابعة دراسات دقيقة حولها. ▪ وتوصلت الدراسة إلى أن المجتمعات البشرية ستتجه نحو التعايش مع الآلات، كما يتضح في المدن الذكية والمنازل الذكية وإنترنت الأشياء، واستبعدت الدراسة المخاوف من تدمير البشرية بسبب الآلات أو استقلاليتها الكامل؛ وذلك لقاعدتين مهمتين، الأولى: استحالة وضع خوارزمية مطلقة نظرًا لأن مصممها غير مطلق، والثانية: هي ذلك الفارق الجوهري بين الأداء والخلق، إذ يستطيع الروبوت التفوق في مجال ما لكنه لا يستطيع ابتكار القواعد لهذا المجال.

ب. ملخص الدراسات السابقة المتعلقة بالمتغير التابع "إدارة مخاطر الجريمة المالية":

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2023	الولايات المتحدة الأمريكية	Karina Kasztelnik	The Observational Study Financial Fraud Offense Themes and Financial Fraud Risk of Money Laundering to Increase Financial Global Sustainability Compliance	المؤسسات المصرفية الأمريكية والنظام المصرفي الأمريكي مكافحة غسل الأموال ومكافحة تمويل الإرهاب	▪ هدفت الدراسة إلى تحديد أنماط الجرائم المالية المرتبطة بغسل الأموال، ودراسة كيفية تعرف مديري الالتزام ومحققي غسل الأموال على هذه الأنماط في النظام المصرفي الأمريكي؛ وذلك للحد من المخاطر وتعزيز الامتثال والاستدامة المالية في المؤسسات المصرفية والمالية. ▪ توصلت الدراسة إلى ضرورة تحديث مجالات الجرائم المالية ضمن ثماني مجالات ناشئة لتعزيز برامج الامتثال ومؤشرات الإنذار، وأوصت بتعديل الإجراءات التشغيلية لجمع بيانات محدثة عن العملاء ذوي المخاطر العالية لتعزيز الشفافية وتقليل المخاطر، كما أسهمت في سد فجوة معرفية في إدارة مخاطر الجرائم المالية، داعية لمزيد من الأبحاث، وأخيرًا شددت على أهمية رفع الوعي العام عبر تثقيف العملاء وتنفيذ مبادرات توعية مجتمعية.
2023	الهند إيران كندا	Afjal et al.	Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability.	القطاع المصرفي العلاقة بين الاحتيال المالي، ومخاطر الائتمان، واستقرار المؤسسات المصرفية	▪ هدفت الدراسة إلى استكشاف كيفية تفاعل الاحتيال المالي ومخاطر الائتمان وتحديد طبيعة العلاقة بينهما وتأثيرها على الاستقرار المصرفي من خلال تقييم الأثر التراكمي لهذه العلاقة على المستوى الجزئي (البنوك الفردية) والكلي (القطاع المصرفي والاقتصاد الأوسع). ▪ وقدّمت الدراسة تحليلاً معمقًا للعلاقة بين الاحتيال المالي ومخاطر الائتمان والاستقرار المصرفي، وخلصت إلى الدعوة إلى اتباع نهج تكاملي يسد الفجوات البحثية ويسهم في فهم أعمق لهذه العلاقة المعقدة، كما أكدت على ضرورة تطوير أطر تنظيمية وإستراتيجيات فعالة لإدارة المخاطر، بما يعزز المرونة أمام الأزمات، وتُعد نتائجها مرجعًا لتوجيه إستراتيجيات إدارة المخاطر في القطاع المصرفي، بهدف الحد من المخاطر وتعزيز الاستقرار المالي.
2022	نيجيريا	KASIE and AKUJINMA	FRAUD AND ITS EFFECT ON BANKING INDUSTRY: A STUDY OF SELECTED BANKS IN NIGERIA	تأثير جرائم الاحتيال والجرائم المالية على القطاع المصرفي النيجيري	▪ هدفت هذه الدراسة إلى تحديد تأثير الاحتيال على ربحية الصناعة المصرفية، وتقييم تأثير هذه الجرائم على ثقة العملاء، وكذا استكشاف طبيعة وطرق وقوع جرائم الاحتيال. ▪ وتوصلت الدراسة إلى أن جرائم الاحتيال في القطاع المصرفي تتنوع بين الرشوة، والاختلاس، والفساد، والتزوير، وسرقة الهوية، واحتيال القروض، والبطاقات الائتمانية، والاحتيال الإلكتروني، وتؤثر هذه الجرائم سلبًا على ربحية البنوك وثقة العملاء والمستثمرين، وأوصت الدراسة بضرورة الإبلاغ عن المعاملات المشبوهة، وتعزيز الشفافية بين البنوك والجهات التنظيمية، وتنفيذ برامج فعالة لمكافحة الاحتيال.
2022	المملكة المتحدة	John Mahony	Best Practices in Combating Fraud in	إدارة مخاطر الاحتيال والامتثال في	▪ هدفت الدراسة إلى تحديد الخطوات العملية لإنشاء إطار لمكافحة جرائم الاحتيال المالي، وتقديم التوصيات

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
			Financial Institutions	المؤسسات المصرفية والمالية	لتعزيز القدرات في منع واكتشاف الجرائم المالية في المؤسسات المصرفية والمالية. ▪ خلصت الدراسة إلى مجموعة من النتائج والتوصيات التي تعزز دفاعات المؤسسات المالية وتحمي سمعتها، أبرزها: ضرورة ترسيخ الحوكمة وثقافة المساءلة من خلال هياكل المسؤولية وإجراءات المساءلة التفصيلية، واعتماد تدابير موحدة للكشف عن الاحتيال، واتباع أفضل ممارسات التحقيق مع مراعاة سرية البيانات والامتثال لقوانين الخصوصية، كما شددت على مواءمة برامج مكافحة الاحتيال مع المتطلبات التنظيمية، وأهمية التقييم المستمر للإستراتيجيات لمواكبة المخاطر المتغيرة.
2021	إندونيسيا	Pradesyah et al	Fraud in Financial Institutions	الاحتيال في المؤسسات المالية التقليدية والمؤسسات المالية الإسلامية في إندونيسيا.	▪ هدفت الدراسة إلى تحليل اتجاهات جرائم الاحتيال، مبيّنة تباين معدلاتها بين المؤسسات، مع تصاعد القلق من الاحتيال السيبراني. ▪ وأكدت الدراسة على أهمية فهم مخاطر الاحتيال الداخلي باستخدام نظرية مثلث الاحتيال، داعية إلى تطوير أنظمة متخصصة للرصد والمنع، وتعزيز التعاون بين الباحثين وصنّاع السياسات، إضافة إلى المراقبة المستمرة للموارد البشرية وتطبيق إجراءات قانونية عند الضرورة لتعزيز مصداقية المؤسسات المالية وثقة الجمهور.
2021	صربيا	Haris Muminovic	Typologies of Financial Crimes	أنماط الجرائم المالية وتصنيفاتها، مع تحليل شامل لأنواعها	▪ هدفت الدراسة إلى تحديد أنواع الجرائم المالية وتصنيفاتها، وتحليل خصائص الجرائم المالية وتأثيرها على المجتمع والاقتصاد. ▪ خلصت الدراسة إلى أن الجرائم المالية تُشكّل تهديدًا خطيرًا للنظام المالي العالمي، وتشمل: الفساد، والاحتيال، والسرقة، والتلاعب، وغسل الأموال، موضحة أن العولمة زادت من تعقيد هذه الجرائم وانتشار الشبكات الإجرامية المنظمة، مما صعّب على الجهات الرقابية تعقّبها، وأوصت الدراسة بضرورة التوصل الى حلول شاملة تشمل القطاعات الأكاديمية، القانونية، والرقابية، وتعزيز التعاون الدولي وتحسين الإجراءات التنظيمية لمواجهة التحديات المرتبطة بالجرائم المالية العابرة للحدود.
2020	الولايات المتحدة الأمريكية	Gao et al.	Dirty Money: How Banks Influence	مجال التمويل والاقتصاد المالي، مع تركيز خاص	▪ هدفت هذه الدراسة إلى تحليل حوافز البنوك في الإبلاغ عن الأنشطة المشبوهة من خلال تقارير النشاط المشبوه، واستكشاف مدى فاعلية هذه السياسات في

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
			Financial Crime	على الجريمة المالية، الامتثال المصرفي، وسلوك البنوك في الإبلاغ عن الأنشطة المشبوهة.	مكافحة الجريمة المالية، مع التعرف على كيفية استغلال المجرمين للثغرات التنظيمية، وتحديد تأثير المنافسة وتراجع الربحية على سياسات الإبلاغ، وجذب العملاء المشبوهين، وقياس العلاقة السببية بين ضغوط الربحية وسلوك البنوك باستخدام صدمات خارجية مثل طفرة الغاز الصخري. ▪ توصلت الدراسة إلى أن ضغوط الربحية قد تدفع بعض المؤسسات المصرفية إلى اتباع سياسات إبلاغ ضعيفة، مما يجعلها عرضة لجذب العملاء من ذوي الأنشطة الإجرامية، كما أثبتت وجود علاقة سببية بين حوافز قبول المخاطر، مثل: التنافس، وزيادة أو انخفاض تقارير النشاط المشبوه، وأن ضعف معايير الإبلاغ يسهم في تفاقم الجرائم المالية، وبناءً عليه أوصت الدراسة بتعزيز الرقابة التنظيمية، وتحسين التشريعات، وضبط ضغوط الربحية، وتبني معايير إبلاغ صارمة، وتنفيذ ممارسات فعّالة لإدارة المخاطر، إلى جانب تعزيز التعاون بين البنوك والجهات الرقابية، وإجراء تقييمات دورية لسياسات مكافحة الجرائم المالية.
2020	كينيا	Nyakarimi et al	Risk Assessment and Fraud Prevention in Banking Sector	إدارة المخاطر، الرقابة الداخلية، ومنع الاحتيال في القطاع المصرفي في كينيا	▪ هدفت هذه الدراسة إلى التعرف على تأثير تقييم المخاطر على منع جرائم الاحتيال في القطاع المصرفي في كينيا، وسد الفجوة البحثية حول العلاقة بين تقييم المخاطر وجرائم الاحتيال. ▪ وأثبتت نتائج الدراسة أن الاحتيال المصرفي والمالي أصبح أكثر تعقيدًا وسهولة في ارتكابه بفضل التقدم التكنولوجي، وأن هناك حاجة كبرى لتحسين الضوابط الأمنية وآليات تحديد مخاطر الاحتيال المصرفي والمالي، وأوصت الدراسة بضرورة إشراك محللي المخاطر بشكل منتظم لتحديد علامات ومؤشرات الاحتيال مبكرًا، وكذا بضرورة تدريب الموظفين بشكل دوري لتعزيز قدراتهم في مجالات اكتشاف وتحديد مخاطر الاحتيال المصرفي والمالي والتعامل معها، مما يساعد في كشف ومنع جرائم الاحتيال المصرفي والمالي.

ج. ملخص الدراسات السابقة التي تناولت العلاقة بين المتغير المستقل والمتغير التابع:

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2024	الولايات المتحدة الأمريكية المملكة المتحدة	Sina Ahmadi	Open AI and its Impact on Fraud Detection in Financial Industry	تأثير الذكاء الاصطناعي المفتوح (Open AI) في كشف الاحتيال في القطاع المالي	▪ هدفت الدراسة لتحليل دور الذكاء الاصطناعي في تحسين الكشف عن جرائم الاحتيال المالي مقارنة بالأنظمة التقليدية القائمة على القواعد، واستعراض تقنيات تعلم الآلة المستخدمة كالنماذج التنبؤية ومناقشة التحديات، مثل البيانات غير المتوازنة والانذارات الكاذبة، واستغلال المحتالين لتقنيات الذكاء الاصطناعي، وقدمت نماذج لجهود شركات مالية مثل Mastercard في تطبيق الذكاء الاصطناعي لمكافحة الاحتيال. ▪ وتوصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي قللت الاحتيال بنسبة 99.6% في بعض الحالات كغسل الأموال، وخفضت الإنذارات الكاذبة من 30% إلى 1.%، كما حسنت تجربة العملاء من خلال تقليل الرفض الخاطئ للمعاملات؛ مما يقلل انتقال العملاء إلى المنافسين (25% منهم يتركون البنك إذا تعرضوا لرفض خاطئ)، وأوضحت الدراسة وجود تحديات جديدة مثل استغلال المحتالين للذكاء الاصطناعي في تزيف الأصوات وانتحال الشخصية أو إنشاء مستندات مزيفة، وأوصت بضرورة تحديث أنظمة الأمان باستمرار لمواكبة تطور أساليب الاحتيال.
2023	الدنمارك	سمية بن علي	مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي	دور الذكاء الاصطناعي في كشف الاحتيال وتعزيز الأمن السيبراني في القطاع المصرفي مع دراسة تطبيقية على بنك Danske الدنماركي	▪ هدفت الدراسة لتحليل دور الذكاء الاصطناعي في تحسين كشف الاحتيال المالي عبر تطبيقات الأمن السيبراني، ودراسة فاعليته في معالجة البيانات الضخمة وتحديد الأنماط الاحتيالية التي يصعب اكتشافها يدويًا، وتقييم تجربة بنك Danske في استخدام الذكاء الاصطناعي لتقليل الاحتيال وتحسين الأمن الرقمي، وتحديد تحديات تبني الذكاء الاصطناعي في القطاع المصرفي. ▪ خلصت الدراسة إلى أن الذكاء الاصطناعي أسهم في كشف 95% من حالات الاحتيال، مما عزز كفاءة إدارة المخاطر، وأسهم في تبسيط العمليات المصرفية وتحسين تجربة العملاء، إضافةً إلى معالجة قضايا كالبطالة والتحيز، كما أكدت على ضرورة التصدي للتحديات القانونية المرتبطة باستخدامه، وأهمية التعاون بين المؤسسات المالية والحكومات لضمان حماية الفئات الضعيفة، وأوصت بتبني إستراتيجيات متكاملة لتعزيز الأمان الرقمي وتحسين الخدمات المصرفية.

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2023	أوكرانيا	Mytnyk et al	Application of Artificial Intelligence for Fraudulent Banking Operations Recognition	استكشاف وتحليل إمكانات الذكاء الاصطناعي في تحسين اكتشاف جرائم الاحتيال في المؤسسات المصرفية	▪ هدفت الدراسة إلى فهم كيفية استخدام تطبيقات الذكاء الاصطناعي في التعرف على المعاملات المصرفية والمالية الاحتيالية، مع التركيز على تطوير خوارزميات آلية موثوقة. ▪ وتوصلت الدراسة إلى أن خوارزميات تعلم الآلة، خاصة الشبكات العصبية الاصطناعية وخوارزميات التصنيف، أثبتت فاعليتها في تحسين دقة كشف الاحتيال، كما أظهرت خوارزمية التعميم المكدس أداء أفضل من الخوارزميات الفردية، مؤكدة أهمية توافر بيانات تاريخية شاملة وعالية الجودة لتدريب النماذج بدقة، وتفادي النتائج الإيجابية الكاذبة، وأشارت إلى تحديات مثل عدم الشفافية، وضعف تفسير مخرجات الخوارزميات، ومخاوف الخصوصية، والتحيز في البيانات، داعية إلى معالجتها لضمان عمل الأنظمة بكفاءة وأمان، وأوصت الدراسة باعتماد تقنيات الذكاء الاصطناعي مع التركيز على معالجة هذه التحديات لتحقيق نتائج دقيقة في كشف الاحتيال المصرفي.
2022	الصين	Piao and Xiao	Risk Management Analysis of Modern Commercial Using "Banks Behavioral Finance Theory and Artificial Neural Networks	إدارة مخاطر الائتمان في البنوك التجارية الحديثة باستخدام نظرية التمويل السلوكي والشبكات العصبية الاصطناعية	▪ هدفت الدراسة إلى تحليل تحديات إدارة مخاطر الائتمان في البنوك التجارية الصينية في ظل العولمة المالية وتحرير أسعار الفائدة، وتقديم نموذج كمي جديد يعتمد على الذكاء الاصطناعي لتحسين دقة تقييم المخاطر الائتمانية، ومعالجة قيود النماذج التقليدية التي تعتمد على التحليل النسبي البسيط، والتي لا تلبي احتياجات البنوك الحديثة وتعزيز قدرة البنوك على التنبؤ بالمخاطر وتقليل نسبة القروض المتعثرة. ▪ وخلصت الدراسة إلى أن طبيعة مخاطر الائتمان غير المتماثلة وغير الخطية تتطلب تقييمًا دقيقًا، وأن العواطف والتحيزات قد تؤثر سلبًا على إدارة المخاطر، كما بينت عدم كفاية النماذج التقليدية، داعية إلى استخدام تقنيات متقدمة مثل التمويل السلوكي والشبكات العصبية الاصطناعية، وأثبتت فاعلية خوارزميات مثل الشبكات العصبية ذات الانتشار المرتد وآلة المتجهات في تحسين دقة تصنيف البيانات ودعم قرارات القروض، وفي الختام أوصت الدراسة باعتماد نماذج تقييم متقدمة لتعزيز ربحية البنوك وتقليل القروض المتعثرة وتحسين إدارة المخاطر.

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
2022	الهند وبلجيكا	Apoorv Awasthi	Using Artificial Intelligence to Prevent Banking Fraud	استخدام الذكاء الاصطناعي وتعلم الآلة في منع الاحتيال المصرفي	▪ هدفت هذه الدراسة إلى استكشاف كيفية استخدام الذكاء الاصطناعي وتطبيقاته لمنع الاحتيال المصرفي، مع التركيز على نمطين شائعين من الجرائم المالية هما: سرقة الهوية، والتصيد الاحتيالي عبر البريد الإلكتروني. ▪ خلصت الدراسة إلى أن الذكاء الاصطناعي وتعلم الآلة يسهمان في حماية أموال البنوك وبيانات العملاء من خلال حلول متقدمة تشمل مصادقة العملاء وفحوصات أمنية متعددة، وفي مكافحة التصيد، تُحلَّل البيانات التعريفية وسلوك المستخدم لرصد التهديدات، بينما تشمل مكافحة سرقة الهوية تقنيات التحقق من الوثائق والتعرف على الوجه، وأكدت الدراسة على أهمية الابتكار والبحث المستمر لمواكبة تطور أساليب الاحتيال وضمان أمن الأنظمة المالية.
2022	كندا	Hilal et al.	Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances	كشف الاحتيال المالي باستخدام تقنيات تعلم الآلة والذكاء الاصطناعي، مع تركيز خاص على الأنظمة الخبيرة وتقنيات اكتشاف الشذوذ	▪ هدفت الدراسة إلى تحديد عمليات الاحتيال الشائعة في الصناعة المصرفية وكيفية ارتكابها، ومناقشة تأثير الاحتيال على الشركات والأفراد والاقتصادات، ورصد التقنيات المستخدمة في اكتشاف الاحتيال، وتحديد تحديات تلك التقنيات وقياس فاعليتها. ▪ توصلت الدراسة إلى نتائج مؤثرة بشأن تقنيات الكشف عن الاحتيال المالي، حيث أكدت تطور أساليب المحتالين واستغلالهم لنقاط الضعف، مما يتطلب أنظمة متقدمة للكشف، وأوضحت أن احتيالات الشيكات والمدفوعات الإلكترونية من أكثر الأنواع شيوعًا، بينما يحظى احتيال بطاقات الائتمان والتأمين بأكبر اهتمام بحثي، إلى جانب تزايد الأبحاث حول غسل الأموال، في حين تظل الدراسات حول احتيال الرهن العقاري والأوراق المالية محدودة، كما بينت أن اكتشاف احتيال البطاقات يعتمد على تحليل الملفات والسلوكيات، بينما يعتمد التأمين على تحليل المطالبات، وأشارت إلى أن الأساليب الموجهة والشبكات العصبية وأشجار القرار كانت الأكثر استخدامًا، لكن هناك توجه متزايد نحو الأساليب غير الموجهة، كالتجميع والغابات المعزولة لمعالجة قيود النماذج الموجهة، كما نبهت إلى وجود فجوات بحثية في نماذج الاحتيال

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
					الأخرى، والنماذج القابلة للتفسير، واكتشاف الاحتيال عبر الإنترنت.
2021	الصين	Zhu et al.	Intelligent Financial Fraud Detection Practices in Post-Pandemic	الاحتيال المالي الذكي، مع تركيز خاص على كشف الاحتيال المالي في العصر ما بعد الجائحة (كوفيد-19)	▪ هدفت الدراسة إلى تحليل تأثير جائحة كوفيد-19 على أنماط الاحتيال المالي، واستعرضت تطور البيانات المستخدمة في كشف الاحتيال، سواء المنظمة أو غير المنظمة، إلى جانب مراجعة الأساليب الحالية، كالأنظمة الخبيرة، وتعلم الآلة، والتعلم العميق، مع التركيز على الشبكات العصبونية البيانية لقدرتها على تحليل البيانات غير المتجانسة، كما سلطت الضوء على التحديات المستقبلية، مثل سرية الاحتيال، وتشتت البيانات، والحاجة لتحسين قابلية تفسير النماذج. ▪ توصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي، كتعلم الآلة والنظم المعرفية، لها قدرة عالية على دمج المعلومات حول الكيانات المتورطة في الاحتيال، مما يسهّل أتمتة الكشف وتحديد الأنماط المشبوهة باستخدام البيانات المنظمة وغير المنظمة لتحليل الحالات الشاذة والعلاقات السرية، كما أكدت الحاجة إلى نماذج قابلة للتفسير لمواجهة تحديات التحيز، حيث إن عدم توازن الفئات يفاقم مشكلة التحيز، مما يتطلب تطوير نماذج أكثر عدالة. وأكدت على البحث المستمر لتطوير أنظمة كشف احتيال فعالة وموثوقة تدعم ممارسات مرنة.
2021	أستراليا	Rouhollahi et al.	Towards Artificial Intelligence Enabled Financial Crime Detection	دور الذكاء الاصطناعي في كشف الجرائم المالية، مع تركيز خاص على كشف عمليات غسل الأموال باستخدام تقنيات تعلم الآلة وتحليل البيانات.	▪ هدفت الدراسة لتعزيز فاعلية كشف غسل الأموال من خلال تطوير نموذج هجيني يجمع بين تقنيات التعلم الموجه وغير الموجه لتحسين دقة التعرف على المعاملات المشبوهة، كما هدفت إلى تقليل الاعتماد على التدخل البشري عبر خفض معدلات الإنذارات الكاذبة التي تستلزم تحقيقات يدوية مكلفة، إضافة لتطوير آليات تصنيف تلقائي للبيانات بالاستناد إلى قواعد معرفية يحددها خبراء مكافحة غسل الأموال. ▪ خلصت الدراسة إلى أن نموذج الشبكة العصبية المتصلة بالكامل قدّم أعلى دقة بين نماذج التصنيف، بينما أظهرت طريقة غابة العزل أفضل أداء في كشف الحالات الشاذة، واقترحت منهجية هجينة بين التصنيف الموجه والكشف غير الموجه عن الشذوذ، مما حسن دقة الكشف عن المعاملات المشبوهة وقلل الحاجة للتدخل البشري وخفض الإنذارات الكاذبة، وأوصت بتوسيع البحث من خلال دمج خصائص العملاء، وتطوير تقنيات هندسة السمات الذكية، واعتماد النمذجة الشبكية وتقنيات التجميع، بهدف تزويد المحللين بلوحات تحكم ديناميكية تدعم اتخاذ القرار، كما شددت على أهمية تعزيز الامتثال

السنة	البلد	الباحث	عنوان الدراسة	مجال التطبيق	ملخص الدراسة
					التنظيمي ورفع مستوى اليقظة في رصد الأنشطة المالية المشبوهة.

ملحق رقم (4) مصطلحات الدراسة

أولاً: المصطلحات ذات الصلة بالمتغير المستقل (الذكاء الاصطناعي):

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
الشبكات العصبية الترشيحية	Convolutional Neural Network-CNN	الدقة	Accuracy
مؤشر تأثير التكلفة	Cost Impact Index	مؤشر قياس الدقة	Accuracy Measuring Index
الأمن السيبراني	Cyber Security	دالة تنشيط	Activation Function
لوحة تحكم	Dashboard	كشف الاحتيال القائم على الذكاء الاصطناعي	AI-based Fraud Detection
قواعد البيانات	Databases	مؤشرات قياس أداء الذكاء الاصطناعي	AI Performance Metrics
دقة تصنيف البيانات	Data Classification Accuracy	خوارزمية	Algorithm
تسمية البيانات	Data Labeling	الظلم الخوارزمي	Algorithmic Injustice
التنقيب عن البيانات	Data Mining	تقنيات الكشف عن الحالات الشاذة	Anomaly Detection Techniques
اختبارات صحة البيانات	Data Validity Tests	تطبيقات	Applications
أشجار القرار	Decision Trees	الذكاء الاصطناعي	Artificial Intelligence (AI)
التعلم العميق	Deep Learning	الذكاء الاصطناعي العام	Artificial General Intelligence -AGI
شبكة عصبية اصطناعية متعددة الطبقات	Deep Neural Network	الذكاء الاصطناعي العصبي	Artificial Neural Intelligence -NeuroAI
شبكة المحولات العصبية العميقة	Deep Neural Network Transformers	شبكة عصبية اصطناعية	Artificial Neural Network -ANN
الالتزامات التصميمية	Design-sourced Commitments	ذات طبيعة غير متماثلة	Asymmetric Nature
المميز	Discriminator	الواقع المعزز	Augmented Reality
الدوافع	Drivers	معايير مصادقة الهوية	Authentication Parameters Identity
القوى المحركة	Dynamics	المرمزات التلقائية	Autoencoders
اختبار تورينج المجسد	Embodied Turing Test	الأتمتة (التشغيل الآلي)	Automization
تحيز عاطفي	Emotional Biases	شبكات عصبية اصطناعية ذات انتشار مرتد	Backpropagation – Artificial Neural Network (BP-ANN)
التعرف على المشاعر	Emotion Recognition	التحيزات في تحليل البيانات	Bias in Data Analysis
المدفوعات الإلكترونية	E-Payments	البيانات الضخمة	Big Data
مؤشر قياس معدل الخطأ	Error Rate Measuring Index	القياسات الحيوية	Biometrics
إطار أخلاقي	Ethical Framework	التكنولوجيا الحيوية	Biotechnology
القابلية للتفسير	Explainability	الروبوتات البرمجية	Bots
النماذج القابلة للتفسير	Explainable Models	القدرات	Capabilities
النظم الخبيرة	Expert Systems	خوارزميات التصنيف	Classification Algorithms
التعرف على الوجه	Facial/Face Recognition	نماذج التصنيف	Classifiers
ذكاء اصطناعي عادل ومفيد	Fair and Useful AI	عدم توازن الفئات	Class Imbalance
نتائج إيجابية كاذبة	False Positive Results	التجميع	Clustering
استخراج الخصائص	Feature Extraction	النظام الزميل	Colleague System
التكنولوجيا المالية	FinTech	قدرات الحوسبة	Computational Power
نماذج الكشف عن الاحتيال	Fraud Detection Models	رؤية الحاسب	Computer Vision
تواتر / تكرار	Frequency	مصفوفة الالتباس	Confusion Matrix
الالتزامات الوظيفية	Functional Commitments	نموذج شبكة عصبية متصلة	Connected Neural Network Model

Convolutional Neural Network-CNN	الشبكات العصبية الترشيحية	Functionalities	الوظائف
Customer Authentication	مصادقة العميل	Fundamental Qualitative Data	البيانات النوعية الأساسية
Customer Features Incorporation	دمج خصائص العملاء	Generative Adversarial Network - GANs	الشبكات التوليدية التنافسية

المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية
Generative AI	الذكاء الاصطناعي التوليدي	Loss Functions	دوال الخسارة
Geometric Transformations	التحويلات الهندسية	Machine Learning	تعلم الآلة
Ghost Workers	عمالة غير مرئية	Machine Vision	الرؤية الآلية / رؤية الآلة
Global Navigation Satellite System - GNSS	النظام العالمي للملاحة عبر الأقمار الصناعية	Mental States	الحالات العقلية
Graph Modeling	تطبيق النمذجة الشبكية	Metadata	البيانات التعريفية
High-Level Processing	تحليل المشهد ومعالجة الصور عالية المستوى	Model Bias	تحيز النموذج
Hybrid	هجين / مختلط	Model Performance	أداء النموذج
Hyperparameter Tuning	توجيه عملية ضبط المعاملات	Morphological Analysis	التحليل الصرفي
Identity Authentication	التحقق من الهوية	Multi-Agent Systems	النظم متعددة المواهب
Image Acquisition	التقاط الصورة	Naive Bayes	مصنف بايز البسيط
Image Processing	معالجة الصورة	Narrow AI or Weak AI	الذكاء الاصطناعي الضيق/ الضعيف
Image Segmentation	تجزئة الصورة	Natural Language Processing	معالجة اللغات الطبيعية
Incorporating Customer Features	دمج خصائص العملاء	Neural Networks	الشبكات العصبية
Information Integration	تكامل المعلومات	NeuroAI	مجال الذكاء الاصطناعي العصبي
Integrating Data	القيام بدمج البيانات	Neuromorphic Computing	الحوسبة العصبية
Integrative Approach	منهج / نهج تكاملي	Neurons	الخلايا العصبية
Intelligent Agent	وكيل ذكي	Neuroscience	علم الأعصاب
Intelligent Feature Engineering	التقنيات الذكية لهندسة الخصائص	Nonlinear Characteristics	الخصائص غير الخطية
Intensity	شدة	OCR and Barcodes	التعرف الضوئي على الحروف والباركود
Internal Assimilation	فهم أو استيعاب داخلي	Optimization Algorithms	خوارزميات التحسين
Internet of Things	إنترنت الأشياء	Personal Biases	التحيزات الشخصية
Interpretability	القابلية للتفسير	Potential Anomalies	الحالات الشاذة المحتملة
Intuition	الحدس	Pragmatic (Context) Analysis	تحليل السياق / التحليل التداولي
Invisible Labors	عمالة غير مرئية	Predicting	التنبؤ
Isolation Forests	غابات العزل	Predictive Analytics Index	مؤشر التحليل التنبؤي
K-nearest Neighbor	خوارزمية الجار الأقرب	Preprocessing	المعالجة المسبقة للصور
Knowledge-based Systems	نظم قائمة على قاعدة معرفية	Privacy Concerns	المخاوف المتعلقة بالخصوصية
Knowledge Gap	الفجوة المعرفية	Probabilistic Graphical Models - PGMs	النماذج الشبكية الاحتمالية
Knowledge Graphs	الشبكات المعرفية	Profile-based Fraud Detection	كشف الاحتيال القائم على تحليل الملفات الشخصية
Labeled Data	البيانات المسماة أي المعلومة	Quantitative Tabular Data	البيانات الكمية التقليدية
Large Language Models – LLM	نماذج اللغة الكبيرة	Random Forest	خوارزمية الغابة العشوائية
Learning Model	نموذج التعلم	Reactive AI	الذكاء الاصطناعي التفاعلي
Limited Memory AI	الذكاء الاصطناعي ذو الذاكرة المحدودة	Rectify Inconsistencies	تصحيح التناقضات
Logical Consistency Analysis	تحليل الاتساق المنطقي	Recall Measuring Index	مؤشر قياس الاستدعاء

Logical Reasoning Capabilities	قدرات الاستدلال المنطقي	Recurrent Neural Network-RNN	الشبكة العصبية التكرارية
Logistic Regression	خوارزميات الانحدار اللوجستي	Regression Algorithms	خوارزميات الانحدار
Long-Short Term Memory- LSTM	الشّبكة العصبية ذات الذّاكرة الطّويلة قصيرة المدى	Reinforcement Learning	التعلم المعزز / القائم على التعزيز

المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية
Reliable Automated Algorithms	خوارزميات آلية موثوقة	Supervised Models	النماذج الموجهة
Reliability	المصداقية	Support Vector Machine - SVM	آلة المتجهات الداعمة
Resilience	المرونة	Syntactic Analysis	التحليل النحوي
Robotics Process Automation – RBA	أتمتة العمليات الروبوتية	Synthetic Data	البيانات المصطنعة
Robots	الروبوتات – شخص آلي	Taxonomizing	التصنيف
Robustness	قوة	Temporal Models	النماذج الزمنية
Rule-based Methods / Systems	طرق / أنظمة قائمة على القواعد التقليدية	Test Data	بيانات الاختبار
Self-Aware AI	الذكاء الاصطناعي القائم على الوعي الذاتي	Text Generation	توليد النصوص
Self-Awareness	الوعي الذاتي	Text Processing	معالجة النصوص
Self-driving Cars	السيارات الذكية ذاتية القيادة/ التوجيه	Theory- of-Mind AI	الذكاء الاصطناعي القائم نظرية العقل
Self-referential	المرجعية الذاتية	Training Algorithms	خوارزميات التدريب
Semantic Analysis	التحليل الدلالي	Training Data	بيانات التدريب
Semi-supervised Learning Algorithms	خوارزميات التعلم شبه الموجه	Transfer Learning	نقل التعلم
Semi-supervised Models	النماذج شبه الموجهة	Transitive Effects	التأثيرات الانتقالية
Smart Cities	المدن الذكية	Transparency	الشفافية
Smart Drones	الطائرات الذكية ذاتية التوجيه	Trust	الثقة
Smart Homes	المنازل الذكية	Trustworthiness	الجدارة بالثقة / الموثوقية
Smart Marketing	التسويق الذكي	Trustworthy	جدير بالثقة/ موثوق
Smart Phones	الهواتف الذكية	Trustworthy Artificial Intelligence	الذكاء الاصطناعي الموثوق
Smart Watches	الساعات الذكية	Unlabeled Data	بيانات غير معلومة / غير مسماة
Social Change	التغيير الاجتماعي	Unsupervised Anomaly Detection	الكشف غير الموجه عن الحالات الشاذة
Sorting	التصنيف	Unsupervised Learning	التعلم غير الموجه
Speech Recognition	التعرف الآلي على الكلام	Unstructured Data	البيانات غير المنظمة
Stacked Autoencoders	المرمزات التلقائية المكدسة	User Behavior	سلوك المستخدم
Stacked Generalization	خوارزمية التعميم المكدس	User Interfaces	واجهات المستخدم
Stochastic Gradient Descent	خوارزمية النزول الاشتقاقي العشوائي	Validation Data	بيانات تحقق
Strong AI	الذكاء العام أو القوي	Video Manipulation	التلاعب بالفيديو
Structured Data	البيانات المنظمة	Virtual Agents	الوكلاء الافتراضيين
Subjectivity	الذاتية	Voice and Image Cloning	استنساخ الأصوات والصور
Super Artificial Intelligence	الذكاء الاصطناعي الفائق أو الخارق	Word Embedding	تمثيل الكلمات
Supervised Classification	التصنيف الموجه		

ثانيًا: المصطلحات ذات الصلة بالمتغير التابع (إدارة مخاطر الجرائم المالية):

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
احتيالات بطاقات الائتمان	Credit Card Fraud	المساءلة	Accountability
مخاطر الائتمان	Credit Risks	جرائم مالية في مرحلة فتح الحسابات	Account Opening Stages
ثقافة المساءلة	Culture of Accountability	الاستيلاء على الحسابات المصرفية	Account Takeover
ثقافة الامتثال / الالتزام	Culture of Compliance	احتيالات معاملات المقاصة	ACH Fraud
تدابير العناية الواجبة بالعملاء	Customer Due Diligence - CDD	مكافحة غسل الأموال	Anti-Money Laundering
مخاطر العملاء	Customer Risk	تجميد الأصول	Asset Freezing
الهجمات السيبرانية	Cyber Attacks	اختلاس الأصول	Asset Misappropriation
الجرائم السيبرانية	Cyber Crimes	هجمات اختراق أجهزة الصراف الآلي	ATM Skimming
الاحتيال السيبراني	Cyber Fraud	هجمات البرمجيات الخبيثة	Attacks Malware
الضوابط الكشفية	Detective Controls	الصناعة المصرفية	Banking Industry
الخدمات المصرفية الرقمية	Digital Banking	الاستقرار المصرفي	Banking Stability
جرائم ترتكب بالوسائل الرقمية	Digital Crimes	الرشوة	Bribery
عملة رقمية	Digital Currency	مخاطر الأعمال	Business Risks
العناية الواجبة الرقمية	Digital Due Diligences	صفات الشخصية	Character Traits
الضوابط التوجيهية	Directive Controls	احتيالات الشيكات	Checks Fraud
هجمات حجب الخدمة الموزعة	Distributed Denial-of-Service - DDoS	تحليل المطالبات	Claims Analysis
الابتزاز الاقتصادي	Economic Extortion	المستفيد الحقيقي أو النهائي	Beneficial Owner
الاختلاس	Embezzlement	مخططات الفوترة	Billing Schemes
إجراءات الإنفاذ	Enforcement Actions	سلاسل الكتل -البلوك تشين	Blockchain Technology
المراقبة المستمرة المشددة	Enhanced Ongoing Monitoring	الرشوة	Bribery
خرق قرارات الجزاءات المالية	Evasion of Financial Sanctions	هجمات اختراق البريد الإلكتروني المؤسسي	Business Email Compromise
الاحتيال في استرداد النفقات والمصروفات	Expense Reimbursement Schemes	الاحتيال في السلع	Commodities Fraud
التقييم القائم على رأي الخبراء	Expert Judgment	الامتثال / الالتزام	Compliance
مخاطر الانكشاف	Exposure Risk	الالتزامات والمصروفات الخفية	Concealed Liabilities and Expenses
المحسوبية	Favoritism	مخاطر التركز	Concentration Risk
الإيرادات الوهمية	Fictious Revenue	السرية	Confidentiality
مجموعة العمل المالي	- Financial Action Task Force FATF	تضارب المصالح	Conflict of Interest
مجالات الجرائم المالية	Financial Crimes Themes	تحليل السياق	Context Analysis
وحدة الاستخبارات / المعلومات المالية	Financial Investigation Unit	الضوابط التصحيحية	Corrective Controls
العقوبات المالية	Financial Penalties	علاقات المراسلة المصرفية	Correspondent Banking
المخاطر المالية	Financial Risks	الفساد	Corruption
الاحتيال في البيانات المالية	Financial Statements Fraud	التزييف	Counterfeiting
الاستدامة المالية	Financial Sustainability	مكافحة تمويل الإرهاب	Counter Terrorism Financing - CFT
التزوير	Forgery	مخاطر الدولة	Country Risks

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
المخاطر القانونية	Legal Risk	الاحتيال	Fraud
الاحتمالية	Likelihood	مثلث الاحتيال	Fraud Triangle
احتيالات القروض	Loan Fraud	الصرف الاحتيالي	Fraudulent Disbursements
التلاعب	Manipulation	شركات واجهة	Front Companies
وسيلة ارتكاب الجريمة	Method of Crime	جمع الأموال	Fund Raising
غسل الأموال	Money Laundering	نقل وتحويل الأموال	Fund Transferring
احتيالات الرهن العقاري	Mortgage Fraud	استخدام الأموال	Fund Using
الجرائم المشتركة	Mutual Crimes	تحليل الثغرات	Gap Analysis
الاحتيال الداخلي (المهني / الوظيفي)	Occupational Fraud	الحوكمة الرشيدة	Good Corporate Governance
جرائم مالية في المعاملات دون اتصال	Offline Transactions Crimes	الإرادة / النية الحسنة	Goodwill
جرائم مالية في المعاملات أثناء الاتصال	Online Transactions	الحوكمة	Governance
المخاطر التشغيلية	Operational Risk	الإجراءات التفصيلية للمساءلة	Granular Accountability Measures
الاحتيال في الرواتب	Payroll Schemes	الخرائط الحرارية	Heat Maps
المقارنة المعيارية مع الأقران	Peer Benchmarking	الاتجار بالبشر	Human Trafficking
التسويات الدورية للمعاملات	Periodic Reconciliations for Transactions	سرقة بيانات الهوية	Identity Theft
التصيد عبر البريد الإلكتروني	Phishing	الإكراميات غير القانونية	Illegal Gratuities
مرحلة الإيداع أو الإحلال	Placement Stage	الاتجار غير المشروع بالأسلحة	Illicit Arms Trafficking
المخاطر السياسية	Political Risks	الاتجار غير المشروع بالمخدرات	Illicit Drug Trafficking
الآثار / العواقب المحتملة	Possible Consequences	الأموال غير المشروعة	Illicit Funds
الضوابط الوقائية	Preventive Controls	التقييمات الخاطئة للأصول	Improper Asset Valuation
مخاطر المنتجات	Product Risk	الإفصاح غير السليم	Improper Disclosure.
ضغوط تحقيق الربح	Profit-seeking Pressures	التعاون وتبادل المعلومات	Information Exchange
تمويل انتشار أسلحة الدمار الشامل	Proliferation Financing	المخاطر الكامنة	Inherent Risk
هجمات برامج الفدية	Ransomware Attacks	التهديدات الداخلية	Insider Threats
غسل الأموال في العقارات	Real Estate Money Laundering	الاحتيال في التأمين	Insurance Fraud
التصنيف والتعرف على الأنماط	Recognition	مرحلة الدمج أو الادماج	Integration Stage
مؤشرات الإنذار أو الاشتباه	Red Flags	الاحتيال المالي الذكي	Intelligent Financial Fraud
تشريعات/ أنظمة	Regulations	أنظمة الرقابة الداخلية	Internal Controls Systems
الجهات الإشرافية والتنظيمية	Regulators	الاحتيال الداخلي	Internal (In-house) Fraud
الاعتبارات التنظيمية	Regulatory Considerations	تمويل التجارة الدولية	International Trade Finance
التوقعات التنظيمية	Regulatory Expectations	الخدمات المصرفية عبر الإنترنت	Internet Banking
أطر تنظيمية	Regulatory frameworks	سرقة / اختلاس المخزون	Inventory Theft
العقوبات التنظيمية	Regulatory Penalties	مؤشرات المخاطر الرئيسية	Key Risk Indicators - KRIs
مخاطر السمعة	Reputation Risk	اعرف عميلك	Know Your Customer - KYC
المخاطر المتبقية	Residual Risk	ملف تعريف العميل	KYC Profile
زمن الاستجابة للحالات المشبوهة	Response Time	مرحلة التغطية أو التمويه	Layering Stage

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
تحليل سلوكيات الإنفاق	Spending Behaviors Analysis	هياكل المسؤولية	Responsibility Structures
معايير الإبلاغ الصارمة	Stringent Reporting Standards	قبول المخاطر	Risk Acceptance
الهيكلة	Structuring	تحليل المخاطر	Risk Analysis
الضوابط الإضافية أو التعزيزية	Supporting or Reinforcing Controls	تقييم المخاطر	Risk Assessment
الإبلاغ عن المعاملات المشبوهة	Suspicious Transaction Reporting	تجنب المخاطر	Risk Avoidance
الجزاءات المالية المستهدفة	Targeted Financial Sanctions	تقييم مستوى المخاطر	Risk Evaluation
جريمة تمويل الإرهاب	Terrorism Financing	تحديد المخاطر	Risk Identification
السرقة	Theft	إدارة المخاطر	Risk Management
استخدام أطراف وسيطة	Third Parties	تخفيف/ معالجة المخاطر	Risk Mitigation
تهديدات	Threats	مراقبة / متابعة المخاطر	Risk Monitoring
اختلاف التوقيت	Timing Differences	ملف المخاطر	Risk Profile
غسل الأموال القائم على التجارة	Trade-based Money Laundering	مراجعة المخاطر	Risk Review
جرائم ترتكب بالوسائل التقليدية	Traditional Crimes	نماذج تصنيف المخاطر	Risk Scoring Models
سياسات مراقبة المعاملات	Transaction Monitoring Policies	نقل الخطر	Risk Transfer
جرائم مالية في مرحلة تنفيذ المعاملات	Transactions Conducting Stages	المنهج / النهج القائم على المخاطر	RBA-Risk-based Approach
الجرائم العابرة للحدود الوطنية	Transnational Crime	حوافز قبول المخاطر	Risk-taking Incentives
الوسائل والأساليب	Typologies	تقارير النشاط المشبوه	Suspicious Activity Report - SAR
ضحايا	Victims	تحليل السيناريوهات	Scenario Analysis
العملات الافتراضية	Virtual Currencies	الاحتيال في الأوراق المالية	Securities Fraud
مكامن الخطر	Vulnerability	شركات وهمية	Shell Companies
أسلحة الدمار الشامل	Weapons of Mass Destruction	نسخ بيانات البطاقة البنكية	Skimming

ثالثًا: مصطلحات أخرى:

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية	المصطلح باللغة الإنجليزية
الممارسة	Practice	نظرية التمويل السلوكي	Behavioral Finance Theory
الخطاب الأكاديمي	Scholarly Discourse	الجوانب التجريبية	Empirical
الجوانب النظرية	Theoretical Aspects	المساواة	Equality
النظرية	Theory	الاقتصاد الكلي	Macroeconomics
		الجوانب المنهجية	Methodological