

تطبيقات الذكاء الاصطناعي في الأمن السيبراني: إطار مفاهيمي وتحليل للمخاطر والتحديات في المجال المالي

Artificial Intelligence Applications in Cyber security: A Conceptual Framework and Analysis of Risks and Challenges in the Financial Domain

البروفيسور جدار رياض

جامعة الجزائر 3

ملخص:

تهدف هذه الدراسة إلى استكشاف دور تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني وتحليل أبرز التحديات التي تواجه توظيفه، معتمدة على المنهج الوصفي التحليلي. كشفت النتائج أن تقنيات الذكاء الاصطناعي تحدث تحولاً جوهرياً في الكشف الاستباقي عن التهديدات والاستجابة الآلية للحوادث وبالأخص الحوادث التي تقع في القطاعات المالية. مما يمكن من الانتقال نحو نموذج حماية استباقي وذكي. غير أن ثمة تحديات تقنية وقانونية وتنظيمية تحول دون التوظيف الأمثل لهذه التقنيات، أبرزها: الإيجابيات الكاذبة، وصعوبة التفسير، وندرة الكفاءات، ومخاطر الخصوصية، والغموض القانوني. وتوصي الدراسة بتبني استراتيجيات متكاملة تجمع بين تطوير البنية التحتية والكفاءات البشرية وحوكمة الذكاء الاصطناعي وتعزيز التعاون الدولي.

كلمات مفتاحية: الذكاء الاصطناعي، الأمن السيبراني، التعلم الآلي، التهديدات السيبرانية، القطاع المالي.

Abstract:

This study explores the role of artificial intelligence applications in enhancing cyber security and analyzes the key challenges facing their deployment, using a descriptive-analytical approach. Findings reveal that AI technologies fundamentally transform proactive threat detection and automated incident response, enabling organizations to shift from reactive to intelligent, proactive protection. However, several technical, legal, and regulatory challenges persist, including false positives, decision opacity, talent shortages, privacy risks, and legal ambiguity. The study recommends integrated strategies combining infrastructure investment, human capital development, AI governance frameworks, and international cooperation.

Keywords: Artificial Intelligence, Cyber security, Machine Learning, Cyber Threats, Financial Domain.

المؤلف المرسل: البروفيسور جدار رياض

مقدمة :

أحدثت الثورة الرقمية تحولا غير مسبوق، وأسفر هذا التحول عن تحسينات ملموسة في سرعة إنجاز المعاملات وسهولة الوصول إلى الخدمات، غير أن هذا التطور الرقمي المتسارع قد أفرز في المقابل تحديا محوريا يتمثل في التصاعد المستمر لمخاطر الأمن السيبراني وتعدد أشكالها، فمع اتساع نطاق الاعتماد على البنية التحتية الرقمية، باتت الأنظمة المالية عرضة لطيف واسع من التهديدات السيبرانية المتطورة، تتراوح بين هجمات الفدية الخبيثة، وعمليات التعدين الخفي للعمليات الرقمية والتصيد الاحتيالي المدعوم بتقنيات الذكاء الاصطناعي، وصولا إلى استغلال ثغرات الحوسبة السحابية والبنى التحتية الحكومية. يستثمر المهاجمون السيبرانيون ترسانة متقدمة من الأساليب والتقنيات لاستهداف نقاط الضعف في منظومات أمن البيانات المالية، مما يفضي إلى عواقب وخيمة تشمل الاحتيال المالي، واختراقات البيانات الحساسة، وانتهاكات الامتثال التنظيمي.

لقد تجاوزت التهديدات السيبرانية كونها مخاطر محتملة لتصبح ظاهرة راسخة ومتعددة الأبعاد تهدد الأمن الاقتصادي والاستقرار المالي على المستويين الوطني والدولي. ففي عصر يتسم بتلاشي الحدود الجغرافية في الفضاء الرقمي، تستغل الجماعات الإجرامية والجهات الخبيثة هذه البيئة الافتراضية لشن هجمات عابرة للحدود تستهدف البنى التحتية المالية الحيوية، مما يولد حاجة ملحة لحماية شاملة للشبكات والأنظمة والعمليات والبيانات من هذه المخاطر المتفاقمة. في ظل هذا السياق المعقد، لم تعد أساليب الحماية التقليدية القائمة على القواعد الثابتة والتوقيعات المعرفة مسبقا كافية لمواجهة التهديدات السيبرانية المتطورة والمتغيرة باستمرار. إذ أصبحت الحاجة ماسة للانتقال نحو آليات حماية حديثة ومبتكرة تعتمد على تقنيات الذكاء الاصطناعي والتعلم الآلي، قادرة على التكيف الديناميكي مع أنماط الهجمات المستجدة.

من هنا، تبرز أهمية دراسة دور تطبيقات الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني، وفهم الآليات التي يمكن من خلالها توظيف هذه التقنيات المتطورة لبناء دفاعات ذكية ومرنة تواكب التطور المستمر للتهديدات السيبرانية.

– إشكالية الدراسة: في ضوء ما تقدم، تسعى هذه الدراسة إلى الإجابة على تساؤلين رئيسيين مترابطين:

- **التساؤل الأول:** فيم تتمثل أهم أدوار تطبيقات الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني؟
 - **التساؤل الثاني:** ماهي أهم التحديات الجوهرية التي تواجه تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي؟
- من خلال استكشاف هذه التساؤلات، تهدف الدراسة إلى تقديم إطار مفاهيمي متكامل يسهم في فهم أعمق للفرص الواعدة والتحديات المحتملة لتوظيف الذكاء الاصطناعي في حماية الأنظمة المالية الرقمية، بما يدعم عمليات صنع القرار الاستراتيجي وصانعي السياسات. بناء على ماسبق ذكره يمكن صياغة فرضيتين رئيسيتين للدراسة كالتالي:

■ **الفرضية الأولى:** هناك علاقة إيجابية بين توظيف تطبيقات الذكاء الاصطناعي وبين تعزيز فعالية منظومة الأمن السيبراني، من حيث دقة الكشف عن التهديدات، وكفاءة التحليل الأمني، وسرعة الاستجابة للهجمات داخل البيئات الرقمية المالية.

■ **الفرضية الثانية:** تؤثر التحديات المرتبطة باستخدام الذكاء الاصطناعي، مثل محدودية الشفافية، ومخاطر الخصوصية تأثيراً مباشراً في كفاءة تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي داخل البيئات الرقمية المالية.

- أهمية الدراسة:

تكتسب هذه الدراسة أهميتها المحورية من تناولها لدور تطبيقات الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني بمختلف القطاعات عبر مراحلها الحيوية، في ظل التصاعد المستمر للتهديدات السيبرانية والتحول الرقمي المتسارع. وعلى الرغم من تزايد الاهتمام البحثي بتطبيقات الذكاء الاصطناعي في المجال الأمني، إلا أن الأدبيات السابقة تظهر فجوة معرفية واضحة في تقديم رؤية تكاملية شاملة تربط بين الإمكانيات التقنية لهذه التطبيقات والتحديات متعددة الأبعاد (التقنية، القانونية، التنظيمية) التي تعيق توظيفها الفعال عبر مختلف القطاعات. كما يلاحظ ندرة الدراسات التي تقدم تقييماً منهجياً لفعالية الآليات الحالية في مواجهة التهديدات المتطورة، مما يحد من قدرة صناع القرار على بناء استراتيجيات قائمة على الأدلة. وتنبع أهمية هذه الدراسة من قدرتها على سد هذه الفجوة البحثية من خلال تزويد صناع القرار برؤية شاملة حول الإمكانيات الواعدة لتقنيات الذكاء الاصطناعي في تحصين البنية الأمنية الرقمية، وتقييم فعالية الآليات الحالية في مواجهة التهديدات المتطورة. كما تتجلى قيمتها المضافة في تحليلها المعمق للتحديات التقنية والقانونية والتنظيمية التي تواجه توظيف هذه التقنيات، مما يمكن المسؤولين من استيعاب الطبيعة الديناميكية لهذه التحديات وصياغة استراتيجيات مرنة وحلول عملية قابلة للتكيف، مما يعزز من فعالية حماية الأنظمة المالية الرقمية ويحافظ على سلامة المعاملات التجارية الإلكترونية واستقرار النظام المالي بأكمله.

- منهجية الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، بهدف استكشاف طبيعة العلاقة بين تطبيقات الذكاء الاصطناعي وتحقيق الأمن السيبراني، وذلك من خلال تحليل الأدبيات ذات الصلة واستقراء المفاهيم النظرية المرتبطة بالموضوع. ويسهم هذا المنهج في تقديم فهم معمق للفرص التي يتيحها الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني، فضلاً عن إبراز التحديات والمخاطر المالية التي قد تنجم عن توظيفه، وبالأخص في القطاعات المالية.

- مصطلحات الدراسة:

- الذكاء الاصطناعي (AI):

تعددت التعاريف الخاصة بالذكاء الاصطناعي، حيث يعرف الذكاء الاصطناعي بأنه "علم وهندسة صناعة الآلات الذكية، وخاصة برامج الحاسوب الذكية" (Top Characteristics of Artificial Intelligence, 2023). ويعرف أيضا بأنه هو فرع علم الحاسب الذي يتعامل مع محاكاة السلوك الذكي في أجهزة الكمبيوتر وقدرة الماكينة على تقليد السلوك البشري (Sadia, 2021).

- الأمن السيبراني (Cyber Security):

عرف التقرير الصادر عن الاتحاد الدولي للاتصالات (2011) الأمن السيبراني بأنه: مجموعة من المهمات مثل تجميع الوسائل، والسياسات والإجراءات الأمنية، والمبادئ التوجيهية والمقاربات لإدارة المخاطر وبالأخص المخاطر المالية التي تتعرض لها أغلب القطاعات المالية، والتدريبات والممارسات الفضلى والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

- الخطر السيبراني:

يعرف الخطر السيبراني بأنه "آثار انتهاك البيانات بدون الهجوم على نظام المعلومات المالية، أو آثار الهجوم على نظام المعلومات أي الدخول غير المشروع لنظام المعلومات (Tibah, 2018).

- الإطار النظري:

أولا: الذكاء الاصطناعي:

1. مفهوم الذكاء الاصطناعي:

يعد الذكاء الاصطناعي فرع علم الحاسوب الذي يتعامل مع محاكاة السلوك الذكي في أجهزة الكمبيوتر وقدرة الماكينة على تقليد السلوك البشري. ولا يوجد تعريف واحد متفق عليه لمصطلح الذكاء الاصطناعي، وذلك بالرغم من كثرة تداول هذا المصطلح خلال العقود الأخيرة (Grosz et al., 2016) وبشكل عام، يمكن تعريف الذكاء الاصطناعي بأنه البرمجيات القادرة على التعلم والتكيف والابداع وحل المشكلات (Rosa et al., 2016)، ووفقا للمجلس الوطني للعلوم والتقنية التابع للبيت الأبيض فإن جذور الذكاء الاصطناعي ترجع للأربعينات من القرن الماضي. لكن البعض يعتقد أن فكرة الذكاء الاصطناعي بدأت في التبلور عام 1950 بواسطة الباحث (Alan Turing)، وذلك من خلال دراسته حيث كان السؤال الرئيسي المطروح في هذه الدراسة: هل تستطيع الآلات التفكير؟ (Luger & Chakrabarti, 2017).

2. تقنيات الذكاء الاصطناعي:

أشارت الباحثة بخوش (2025) إلى مجموعة من التقنيات الخاصة بالذكاء الاصطناعي والتي يمكن ذكرها في النقاط التالية:

- **التعلم الآلي (Machine Learning):** هو مجموعة فرعية من الذكاء الاصطناعي الذي يمكن الأنظمة من التعلم والتحسين من التجربة دون أن تتم برمجتها بشكل صريح، وفي مجال الأمن السيبراني، يتم استخدام التعلم الآلي لتحديد الأنماط والحالات الشاذة أي التمييز بين حركة مرور الشبكة العادية والأنشطة الضارة المحتملة.

- **معالجة اللغات الطبيعية (Natural Language Processing):** تتضمن البرمجة اللغوية العصبية قدرة أجهزة الكمبيوتر على فهم اللغة البشرية وتفسيرها وتوليدها.

- **الشبكات العصبية (Neural Network):** عبارة عن نماذج متقدمة للتعلم الآلي مستوحاة من بنية الدماغ البشري ووظيفته، تركز على تحديد الأنماط المعقدة في البيانات بسبب بنيتها العميقة ذات الطبقات وقدرتها على تعلم العلاقات غير الخطية، على عكس نماذج التعلم الآلي التقليدية التي غالبا ما تقتصر على التفسيرات الخطية أو البسيطة القائمة على قواعد القرار.

- **كشف الشذوذ:** أسلوب يستخدم لتحديد الأنماط غير العادية التي لا تتوافق مع السلوك المتوقع، وهو مفيد بشكل خاص في تحديد التهديدات السيبرانية الجديدة التي لم يسبق لها مثيل.

- **التحليلات التنبؤية:** تستخدم التحليلات التنبؤية التقنيات الإحصائية ونماذج التعلم الآلي لتحديد احتمالية النتائج المستقبلية بناءً على البيانات التاريخية. فالذكاء الاصطناعي هو أكثر من مجرد تقنية فهو ظاهرة معرفية واجتماعية مركبة تتطلب رؤية متعددة التخصصات تجمع بين الحوسبة، الفلسفة، والسياسة، وتعتبر تقنية أدوات حيوية تساهم في تحسين الكفاءة والقدرة على اتخاذ القرارات في مجموعة متنوعة من المجالات.

ثانيا: الأمن السيبراني:

يعتبر أمن المعلومات والأمن السيبراني وبالأخص في جانب القطاع المالي من أهم قضايا الفضاء السيبراني في العصر الحالي (Wu et al., 2018). تطرق العديد من الباحثين والدارسين في الآونة الأخيرة إلى مفهوم الأمن السيبراني، محاولين الوصول إلى صيغة موحدة، وقد تعددت مجموعة من التعريفات شأنًا شأن العديد من تعريفات تقنيات المعلومات. فحسب (Schatz et al., 2017) الأمن السيبراني يقصد به مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والتوجيهات ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة والأصول.

1. أهمية الأمن السيبراني:

تكتسي قضية الأمن السيبراني حسب (Ali et al. (2025 أهمية بالغة في سياق التحول الرقمي المتسارع الذي تشهده القطاعات المالية ومختلف القطاعات المعاصرة، إذ أضحت ركيزة أساسية لضمان استدامة العمليات المصرفية والمالية وحماية البنى التحتية الرقمية من التهديدات المتزايدة. وتتجلى هذه الأهمية في عدة أبعاد استراتيجية، يأتي في مقدمتها مكافحة الجريمة السيبرانية والحد من المخاطر والتهديدات الرقمية التي باتت تستهدف البيانات الحساسة للدول والمؤسسات والشركات، مما يستوجب حماية فعالة من الاختراقات والهجمات الإلكترونية التي قد تعصف بالاستقرار المؤسسي. كما يسهم الأمن السيبراني في دعم تنمية تكنولوجيا المعلومات وتعزيز حماية البنى التحتية الرقمية، الأمر الذي ينعكس إيجاباً على تحقيق الرفاه الاقتصادي وتعزيز الاستقرار المالي للدول من خلال توفير بيئة رقمية آمنة ومستقرة.

ومن جهة أخرى، يلعب الأمن السيبراني دوراً محورياً في حماية المستهلكين وتأمين المعلومات المتداولة عبر شبكات الإنترنت، وذلك عبر ردع الجرائم المرتبطة بالمعاملات التجارية الإلكترونية وضمان سلامتها القانونية، فضلاً عن تأمين بيانات العملاء والمنتجين من السرقة أو التعطيل أو التشفير غير المشروع. وتمتد هذه الحماية لتشمل تعزيز الثقة في البيئة الرقمية، مما يسهم بشكل مباشر في زيادة حجم المعاملات الإلكترونية وتطور الاقتصاد الوطني، خاصة في ظل التوسع المتنامي في تطبيقات الذكاء الاصطناعي والتقنيات المالية الحديثة. وعلى الصعيد المؤسسي، يساهم الأمن السيبراني في تقليل الخسائر المالية الجسيمة الناتجة عن الهجمات السيبرانية، والتي أثبتت الدراسات أن آثارها قد تضاهي أو تفوق في بعض الأحيان آثار الكوارث الطبيعية من حيث الأضرار الاقتصادية والتشغيلية. كما يعمل على حماية الموارد المالية والبشرية والتقنية والتنظيمية والمعلوماتية للمؤسسات المالية، مما يضمن استمرارية الأعمال وتقليل مخاطر التوقف التشغيلي. ويتطلب ذلك توفير أطر قانونية وآليات تقنية وإجرائية فعالة لمواجهة التهديدات السيبرانية، بالإضافة إلى تعزيز التعاون الدولي لمجابهة الطابع العابر للحدود للجريمة السيبرانية، نظراً لتعقيد وتشابك الفضاء الإلكتروني العالمي وصعوبة مكافحة هذه الجرائم بجهود وطنية منفردة.

2. أهم التحديات القانونية التي تواجه الأمن السيبراني:

تواجه منظومة الأمن السيبراني في مختلف القطاعات حسب (Ali et al. (2025 مجموعة معقدة من التحديات القانونية التي تنقسم إلى بعدين رئيسيين: داخلي وخارجي، تتشابك فيهما الإشكاليات التقنية بالثغرات التشريعية والإجرائية. فعلى المستوى الداخلي، تبرز إشكالية المساءلة القانونية للأطراف الداخلية كأحد أبرز التحديات، خاصة في ظل ارتفاع نسبة التهديدات الصادرة من داخل المؤسسات المالية. وتتفاقم هذه الإشكالية بفعل صعوبات الإثبات القانوني للتسريبات والاختراقات الداخلية، إذ تعاني الأطر القانونية القائمة من قصور في توفير آليات فعالة لتتبع المسارات الرقمية وإسناد المسؤولية الجنائية أو المدنية للأطراف المخلة. كما تضاف إلى ذلك ثغرات تنظيم حماية البيانات المحذوفة، حيث تفتقر التشريعات إلى معايير ملزمة بشأن الحذف النهائي والأمن للمعلومات الحساسة، مما يتيح إمكانية

استرجاعها واستغلالها بطرق غير مشروعة، وهو ما يهدد ثلاثية أمن المعلومات الأساسية: السرية والسلامة والإتاحة. أما على المستوى الخارجي، فتتصدر الطبيعة العابرة للحدود للجرائم السيبرانية قائمة التحديات القانونية الأكثر تعقيدا، إذ تفتقر المنظومة القانونية الدولية إلى إطار موحد وفعال ينظم الاختصاص القضائي ويسهل الملاحقة القانونية عبر الحدود. وتزداد هذه الإشكالية تعقيدا بفعل صعوبة تحديد هوية المهاجمين نتيجة لتقنيات الإخفاء والتشفير المتقدمة، مما يعيق جمع الأدلة الرقمية وفق المعايير القانونية المقبولة في الإجراءات القضائية. تواجه الأنظمة القانونية تحديا متصاعدا يتمثل في عدم مواكبة التشريعات لسرعة التطور التكنولوجي، حيث أن القواعد القانونية التقليدية المصممة للجرائم التقليدية تعجز عن استيعاب خصوصية الجرائم الرقمية المتطورة، مما يخلق فراغا تشريعا يستغله المجرمون السيبرانيون. وأخيرا، يشكل غياب آليات قانونية لتقدير التعويضات عن الأضرار السيبرانية تحديا جوهريا، نظرا لصعوبة تقييم الخسائر غير المادية كالأضرار بالسمعة وفقدان الثقة. توجد هناك علاقة بين الأمن السيبراني وأمن المعلومات، حيث تتضمن هذه الأخيرة حسب (Alalwan (2022 مجموعة من العمليات هي:

3. عمليات أمن المعلومات:

مراحل عمليات أمن المعلومات: إطار منهجي متكامل:

تتكون منظومة أمن المعلومات من ثلاث مراحل استراتيجية متكاملة تشكل دورة حياة شاملة للحماية الأمنية، وهي مرحلة الوقاية ومرحلة الاكتشاف ومرحلة الاستجابة، وتتكامل هذه المراحل لتوفير حماية متعددة الطبقات للأصول المعلوماتية.

المرحلة الأولى: الوقاية:

تمثل مرحلة الوقاية خط الدفاع الأول وتهدف إلى الحماية الشاملة للأصول المعلوماتية قبل حدوث الهجمات الأمنية. وتقوم هذه المرحلة على ثلاثة أركان رئيسية: أولاها وضع سياسات أمن المعلومات الواضحة التي تتضمن أهداف أمن المعلومات وأسس توجيه جميع الأنشطة ذات العلاقة، مع تحديد المسؤوليات العامة والخاصة للمنظمة والموظفين والإدارة بشكل دقيق. وثانيها تثقيف الموظفين وتعزيز وعيهم بأهمية أمن المعلومات من خلال برامج توعوية دورية تضمن إدراكهم الكامل لمسؤولياتهم الأمنية. أما الركن الثالث فيتمثل في التحكم في الوصول، والذي يهدف لتقييد الوصول للمعلومات وضمان دخول المستخدمين المصرح لهم فقط إلى النظام والخدمات الإلكترونية، مع منع أي وصول غير مصرح به.

المرحلة الثانية: الاكتشاف:

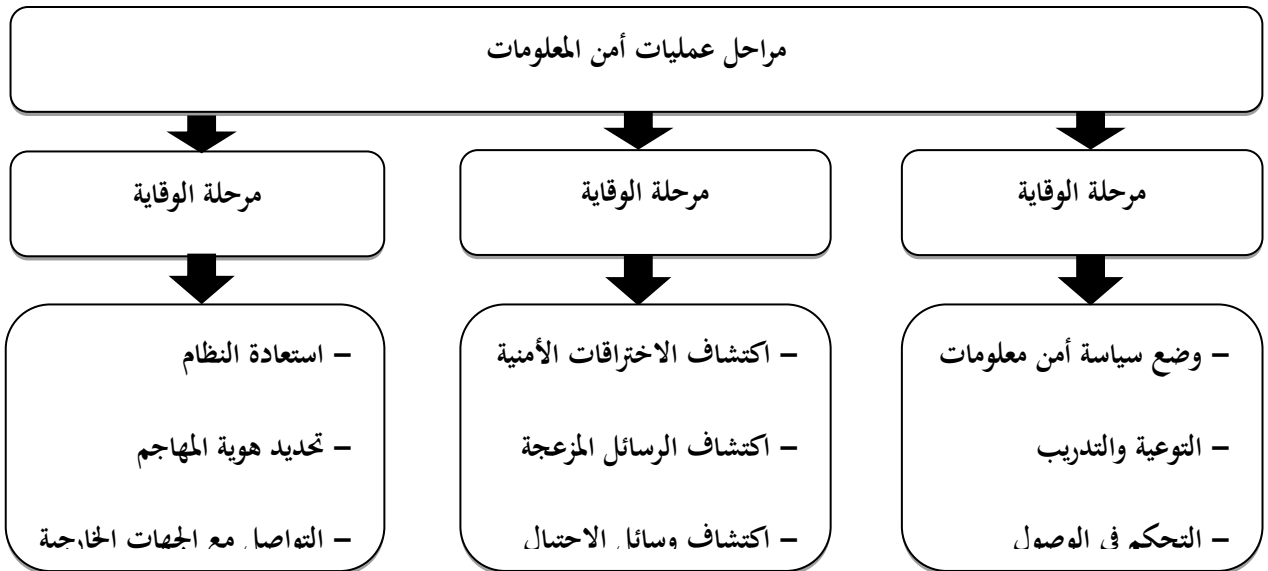
تؤكد أدبيات أمن المعلومات على استحالة تحقيق حماية كاملة بنسبة 100% لأي نظام إلكتروني، مما يجعل مرحلة الاكتشاف ضرورة استراتيجية لا غنى عنها. وترتكز هذه المرحلة على عنصرين حرجين: الاكتشاف السريع للاختراقات من جهة، وإشعار مسؤولي أمن المعلومات الفوري بحدوث هذه الاختراقات من جهة أخرى. ولتحقيق ذلك، يتم توظيف

أنظمة كشف التسلل كبرمجيات أو أجهزة ترافق النظام أو الشبكة بحثاً عن أية خروقات أو أنشطة مشبوهة. وتصنف هذه الأنظمة إلى ثلاث فئات رئيسية: أنظمة كشف التسلل المعتمدة على التوقعات التي تقارن توقيع البيانات الواردة بقاعدة بيانات التهديدات المعروفة والبرمجيات الخبيثة المحددة سابقاً، وأنظمة كشف التسلل المعتمدة على الانحرافات التي ترافق سلوك الشبكة الطبيعي وتحدد الاختلافات عن السلوك المعتاد كانهزافات مشبوهة، بالإضافة إلى الأنظمة الهجينة التي تجمع بين كلا النهجين.

المرحلة الثالثة: الاستجابة:

تمثل مرحلة الاستجابة خط الدفاع الأخير وتؤكد على ضرورة وجود خطة محكمة للاستجابة لحوادث أمن المعلومات، مع تشكيل فريق متخصص له أدوار ومسؤوليات واضحة ومحددة. وتهدف هذه المرحلة إلى القضاء على سبب الحادث واستعادة النظام إلى حالته الطبيعية، مع اتخاذ إجراءات تحقيق معقولة لتحديد المهاجم أو الجهة التي عرضت الأنظمة للخطر من خلال جمع الأدلة الجنائية الرقمية واحتواء الهجوم واستعادة الأنظمة المخترقة. كما تتطلب هذه المرحلة إقامة علاقات استباقية مع الأطراف الخارجية الرئيسية مثل منظمات إنفاذ القانون ووكالات النيابة العامة ووسائل الإعلام خلال مرحلة التخطيط للعمليات الأمنية. وتختتم هذه المرحلة بتقييم شامل للأضرار، واحتواء كامل للحادث، وإجراء تحليل ما بعد الحادث لتوثيق الدروس المستفادة وتعزيز قدرات أمن المعلومات في مواجهة الحوادث الأمنية المستقبلية. يمكن تلخيص المراحل السابقة في الشكل الموالي:

الشكل (1): مراحل عمليات أمن المعلومات وأدوارها



المصدر: من إعداد الباحثين

ثالثا: المخاطر والهجمات السيبرانية:

1. تعريف الخطر السيبراني:

ويعرف (Andress (2014) المخاطر السيبرانية بأنها مجموعة التهديدات التي من شأنها أن تؤثر سلبا على الفضاء السيبراني، مما يؤدي إلى خسائر مادية ومالية ومعنوية على حد سواء. إن عملية الحماية من المخاطر السيبرانية ليست باليسيرة، وإنما هي عملية صعبة ومعقدة تتكون من ثلاث عناصر رئيسة هي: السرية، السلامة، والتوافر، ذلك ما يجعل كل إجراءات الحماية من التهديدات والمخاطر السيبرانية تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات والخدمات الإلكترونية إلى الأشخاص المناسبين وفي الوقت المناسب، والمحافظة على سريتها وسلامتها وهذا لا يعني شيئا ما لم يستطع الأشخاص المخولون الوصول إليها.

2. أنواع الهجمات السيبرانية:

تتنوع الهجمات السيبرانية التي تستهدف مختلف القطاعات الحيوية في تقنياتها وآلياتها ومستويات تعقيدها، مما يفرض على المؤسسات ضرورة الفهم العميق لطبيعتها وخصائصها التقنية لتطوير استراتيجيات دفاعية فعالة. ويمكن تصنيف هذه الهجمات إلى عدة فئات رئيسية تتباين في أساليبها ومخاطرها المحتملة.

أ. البرمجيات الخبيثة (Malware):

تشكل البرمجيات الخبيثة إحدى أخطر فئات التهديدات السيبرانية وأكثرها انتشاراً، وتشمل مجموعة واسعة من البرامج الضارة المصممة لاختراق الأنظمة وإلحاق الضرر بها أو سرقة البيانات الحساسة. وتتضمن هذه الفئة الفيروسات (Viruses) التي تعد أقدم أشكال البرمجيات الخبيثة، والتي تتميز بقدرتها على التكاثر الذاتي وإصابة الملفات والبرامج الأخرى، حيث ظهرت أولى فيروسات الحاسوب منذ سبعينيات القرن الماضي وتطورت بشكل متسارع (Pramanick et al., 2025). كما تشمل برامج الفدية (Ransomware) التي باتت من أكثر التهديدات تدميراً للمؤسسات المالية، إذ تعمل على تشفير بيانات الضحية ومنع الوصول إليها حتى دفع الفدية المطلوبة، وقد شهدت هذه الهجمات تزايداً ملحوظاً خلال السنوات الأخيرة مما أدى إلى خسائر اقتصادية فادحة (Darem et al., 2023; Olech & Štručl, 2025). وتضم هذه الفئة أيضاً أحصنة طروادة (Trojans) التي تتنكر في صورة برامج شرعية لخداع المستخدمين وتمكين المهاجمين من الوصول غير المصرح به إلى النظام، بالإضافة إلى برامج التجسس (Spyware) التي تراقب أنشطة المستخدم وتجمع المعلومات الحساسة كبيانات تسجيل الدخول والمعلومات المالية دون علم الضحية. (Umoga et al., 2024).

ب. التصيد الاحتيالي والهندسة الاجتماعية (Phishing and Social Engineering):

تمثل هجمات الهندسة الاجتماعية استغلالاً منهجياً للعامل البشري، الذي يعتبر الحلقة الأضعف في منظومة الأمن السيبراني، وتستهدف هذه الهجمات التلاعب النفسي بالأفراد لحملهم على الإفصاح عن معلومات سرية أو القيام بإجراءات تعرض الأنظمة للاختراق (Momoh et al., 2023). ويأتي التصيد الاحتيالي (Phishing) في صدارة هذه الهجمات، حيث يتم إرسال رسائل إلكترونية مزيفة تحاكي مصادر موثوقة كالبنوك أو المؤسسات الحكومية لإغراء المستلمين بالنقر على روابط ضارة أو تقديم بيانات اعتماد حساسة (Ayoola et al., 2024).

وتشمل تقنيات الهندسة الاجتماعية الأخرى هجمات التستر التي يتقمص فيها المهاجم شخصية مزيفة لبناء علاقة ثقة مع الضحية واستخلاص المعلومات تدريجياً، وهجمات الإغراء (Baiting) التي تعتمد على تقديم مغريات كهدايا أو عروض وهمية لحث الضحايا على تحميل برمجيات خبيثة أو الإفصاح عن بيانات شخصية (Hijji & Alam, 2021).

3. أنواع أخرى من الهجمات السيبرانية المتطورة:

تتضمن منظومة التهديدات السيبرانية مجموعة من الهجمات التقنية المتقدمة التي تستهدف الثغرات في البنى التحتية الشبكية وتطبيقات الويب. ومن أبرزها هجمات رفض الخدمة ورفض الخدمة الموزع التي تهدف إلى إغراق الخوادم بحجم هائل من الطلبات الوهمية لتعطيل الخدمات وجعلها غير متاحة للمستخدمين الشرعيين، وهي من الهجمات الأكثر شيوعاً ضد المؤسسات المالية لما تسببه من خسائر تشغيلية ومالية جسيمة (Signor, 2023; Kļaviņš, 2025). كما تشمل هجمات الرجل في المنتصف التي يقوم فيها المهاجم باعتراض الاتصالات بين طرفين دون علمهما، مما يمكنه من سرقة البيانات الحساسة أو التلاعب بها، وهي تشكل تهديداً خطيراً لمعاملات الدفع عبر الإنترنت (Fereidouni et al., 2025; Muzammil et al., 2024).

وعلى مستوى تطبيقات الويب، تبرز هجمات البرمجة النصية عبر المواقع التي تستغل ثغرات في التطبيقات لحقن أكواد برمجية ضارة في صفحات الويب المعروضة للمستخدمين (Khazal et al., 2025; Johns, 2009). وتأتي أيضاً هجمات الحقن (Injection Attacks) وأبرزها حقن SQL الذي يستهدف قواعد البيانات من خلال إدخال أوامر SQL ضارة عبر حقول الإدخال، مما قد يؤدي إلى الوصول غير المصرح به لقواعد البيانات وسرقة أو تعديل أو حذف المعلومات الحساسة (Muzammil et al., 2024).

وأخيراً، تتصاعد المخاوف بشأن هجمات إنترنت الأشياء (IoT Attacks) مع التوسع المتزايد في استخدام الأجهزة الذكية المتصلة، حيث تستغل هذه الهجمات ضعف بروتوكولات الأمان في أجهزة IoT لتحويلها إلى بوابات للاختراق أو استخدامها في هجمات DDoS الموزعة، مما يضاعف من سطح الهجوم المحتمل على المؤسسات المالية (Fereidouni et al., 2025).

4. أشهر أطر الأمن السيبراني:

اجتهد الكثير من المؤلفين المبادرين والمهتمين بالنشر في المجال في إيجاد جملة من الأطر التي تهدف بالأساس في مضمونها إلى التحكم في المخاطر السيبرانية . أشهر هذه الأطر المستشهد بها في العديد من الدراسات COBIT و ITIL و ISO 27001 و ISO 17799 و ISO 38500 و Davaridolatabadi et al., 2019; (Smits & Hillegersberg, 2013).

- المنظمة الدولية للمعايير (ISO 27002/ISO 27001):

تعد شهادة ISO 27001 بمثابة بيان عام لقدرة المؤسسة على إدارة أمن المعلومات، وكضمان لقدرة على التطور والتكيف مع مختلف المخاطر المتعلقة بتكنولوجيا المعلومات (Mataracioglu & Ozkan, 2011).

- المنظمة الدولية للمعايير (ISO 38500):

هو معيار دولي لا يختلف عن سابقه من الأطر، يتضمن مجموعة من المبادئ التوجيهية الخاصة بحوكمة تكنولوجيا المعلومات كالمساءلة والشفافية والمحاذاة الإستراتيجية وإدارة المخاطر، كل هذه المبادئ تهدف إلى ضمان الاستخدام الفعال لتكنولوجيا المعلومات وتحقيق التوافق بين أهداف تكنولوجيا المعلومات وأهداف المؤسسة (ISO/IEC, 2008).

- المنظمة الدولية للمعايير (ISO 17799):

يشكل معيار ISO 17799 إطارا مرجعيا هاما في مجال أمن المعلومات وحوكمة تكنولوجيا المعلومات، حيث يضع مجموعة من الإرشادات والممارسات المثلى لإدارة أمن المعلومات بطريقة منهجية داخل المؤسسات، كما يعني هذا الإطار كذلك بتحديد متطلبات حماية المعلومات من التهديدات المتنوعة وضمان الحفاظ على سرية وسلامة وتوافر البيانات، مما يساهم في تقليل المخاطر التشغيلية والتقنية، ويعزز من قدرة المؤسسات على الامتثال للمتطلبات التنظيمية والقانونية.

- أهداف السيطرة على تكنولوجيا المعلومات والتكنولوجيا ذات الصلة (COBIT):

هو إطار عمل أنشئ من طرف جمعية تدقيق نظم المعلومات (ISACA) لإدارة وحوكمة تكنولوجيا المعلومات، حسب (Andry and Hartono, 2017) تعد هذه الجمعية من أهم المؤسسات الرائدة في مجال حوكمة تكنولوجيا المعلومات على المستوى العالمي. يهتم إطار COBIT بالرقابة الداخلية على أنظمة المعلومات الإلكترونية والتكنولوجيا المتعلقة بهذه الأنظمة وحماية أمن المعلومات (Almusawi, 2022)، كما يهتم بتحسين أدائها المالي وتقليل حجم المخاطر المرتبطة بالمؤسسة وتمكين المؤسسة من قياس إجراءات تنفيذ تكنولوجيا المعلومات (Alkhalidi et al., 2017).

- مكتبة البنية التحتية لحوكمة تكنولوجيا المعلومات (ITIL):

تم تطوير هذا الإطار من قبل مكتب التجارة الحكومية بالمملكة المتحدة (OGC)، يعد بمثابة نهج يحظى بالقبول العالمي من ناحية توفير أفضل الممارسات المتعلقة بإدارة تكنولوجيا المعلومات، واستخدام أنظمة المعلومات في بيئة الأعمال بأكثر فعالية (Rusman et al., 2022). يتضمن هذا الإطار حسب Almeida et al. (2020) ثلاثة إصدارات آخرها الإصدار ITILv3 الذي يتألف من خمسة كتب: استراتيجية الخدمة، تصميم الخدمة، الخدمة الانتقال وتشغيل الخدمة والتحسين المستمر.

- أطر أخرى:

مثل إطار عمل اللائحة العامة لحماية البيانات (GDPR)؛ قانون إدارة أمن المعلومات الفيدرالي (FISMA)؛ قانون نقل التأمين الصحي والمساءلة (HIPAA)؛ الإمتثال لمعايير SOC؛ معيار تحالف ثقة المعلومات الصحية (HITRUST)؛ شهادة نضج الأمن السيبراني (CMMC)؛ حماية البنية التحتية الحيوية لشركة موثوقية الكهرباء في أمريكا الشمالية (NERC CIP)؛ مصفوفة التحكم السحابي (CLOUD CONTROL MATRIX)؛ إطار العمل السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST - CSF).

الجانب التطبيقي:

في هذا الجزء من الدراسة سنتطرق إلى دور الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني وأهم التحديات الجوهرية التي تواجه تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي إلى جانب حالات واقعية للتطبيقات العملية للذكاء الاصطناعي في الأمن السيبراني.

أولاً: دور تطبيقات الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني:

يمثل الذكاء الاصطناعي ركيزة استراتيجية محورية في تعزيز منظومة الأمن السيبراني للمؤسسات المالية المعاصرة، إذ أحدث تحولاً جذرياً في قدرات الكشف والاستجابة والحماية من التهديدات الرقمية المتطورة. وتتجلى إسهامات الذكاء الاصطناعي في عدة أبعاد جوهرية، يأتي في مقدمتها الكشف الاستباقي عن التهديدات، حيث تمكن خوارزميات التعلم الآلي والتعلم العميق من تحليل ملايين المعاملات والأحداث الأمنية في الوقت الفعلي، وبناء نماذج تنبؤية قادرة على رصد الأنماط الشاذة والسلوكيات الاستثنائية التي قد تنذر بمجمعات وشبكة قبل تحققها، مما يقلص زمن الاستجابة للحوادث من ساعات إلى ثوان معدودة (Ekundayo et al., 2024; Paramesha et al., 2024). وعلى صعيد مكافحة الاحتيال المالي أحدثت أنظمة كشف الشذوذ المدفوعة بالذكاء الاصطناعي نقلة نوعية من خلال استخدام تقنيات التعلم غير الموجه لبناء ملفات سلوكية ديناميكية لكل عميل، تأخذ في الاعتبار أنماط الإنفاق والمواقع الجغرافية وتوقيت المعاملات، مما يحقق دقة في الكشف، متفوقة بذلك على الأنظمة التقليدية القائمة على القواعد الثابتة (Ejiofor, 2023; Ajayi et al., 2024; Chukwu, 2024).

ومن جهة أخرى، يعالج الذكاء الاصطناعي تحدي التهديدات الداخلية التي تشكل 60% من إجمالي الهجمات السيبرانية، وذلك من خلال أنظمة مراقبة السلوك المستخدم وتحليل الكيانات التي تبني خطوطاً أساسية سلوكية لكل موظف وترصد الانحرافات المشبوهة كمحاولات الوصول غير المألوف للبيانات الحساسة أو نقل كميات استثنائية من المعلومات (Ajayi et al., 2024). كما تسهم تقنيات معالجة اللغة الطبيعية في تحليل الاتصالات الإلكترونية للكشف عن مؤشرات محتملة على نوايا ضارة. وفي مجال الاستجابة الآلية للحوادث، تتيح أنظمة التنسيق الأمني والاستجابة الآلية المدعومة بالذكاء الاصطناعي اتخاذ قرارات فورية عند اكتشاف التهديدات، كعزل الأجهزة المصابة أو حظر عناوين IP المشبوهة أو إيقاف المعاملات الاحتمالية دون تدخل بشري، مما يقلل الأضرار المحتملة بشكل جوهري (Udayakumar et al., 2023; Asmar & Tuqan, 2024). علاوة على ذلك، تمكن التحليلات التنبؤية واستخبارات تهديدات المؤسسات من تحويل البيانات الأمنية الضخمة إلى رؤى استراتيجية قابلة للتنفيذ، إذ تحلل خوارزميات التعلم الآلي البيانات من مصادر متعددة كسجلات الأحداث الأمنية وتقارير التهديدات العالمية لتحديد مؤشرات الاختراق والتنبؤ بالهجمات المستقبلية (Ekundayo et al., 2024; Ayeola, 2025).

ثانياً: أهم التحديات الجوهرية التي تواجه تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي:

على الرغم من الإمكانيات الواعدة للذكاء الاصطناعي في تعزيز الأمن السيبراني، تواجه مختلف القطاعات مجموعة معقدة من التحديات الجوهرية التي تعيق التطبيق الأمثل لهذه التقنيات وتستوجب معالجات استراتيجية متكاملة. ويتصدر هذه التحديات إشكالية الإيجابيات الكاذبة التي تمثل معضلة تقنية وتشغيلية كبيرة، إذ تصدر أنظمة الذكاء الاصطناعي أحياناً تنبيهات خاطئة عن تهديدات غير حقيقية، مما يرهق فرق الأمن السيبراني بالتحقيق في آلاف الحالات الوهمية ويقلل من كفاءتها التشغيلية، بل قد يؤدي إلى إرهاق التنبيهات الذي يجعل المحللين يتجاهلون التنبيهات الحقيقية وسط الضجيج الكبير من الإنذارات الكاذبة (Gonaygunta, 2023; Asmar & Tuqan, 2024).

وترتبط بهذه الإشكالية صعوبة تفسير قرارات الذكاء الاصطناعي، حيث تعمل العديد من نماذج التعلم العميق كـ"صناديق سوداء" يصعب فهم آلية عملها الداخلية، مما يعقد عملية التحقق من دقة القرارات الأمنية والامتثال للمتطلبات التنظيمية التي تفرض الشفافية والمساءلة في الأنظمة المالية (Paramesha et al., 2024; Soldatova, 2026).

وعلى المستوى التقني، تواجه المؤسسات المالية تحدياً كبيراً يتمثل في متطلبات البنية التحتية التقنية الضخمة، إذ تتطلب أنظمة الذكاء الاصطناعي المتقدمة قدرات حوسبية هائلة ومساحات تخزينية ضخمة لمعالجة وتحليل البيانات الضخمة، فضلاً عن الحاجة إلى بنية شبكية عالية السرعة والموثوقية، وهو ما يفرض استثمارات رأسمالية باهظة قد تفوق إمكانيات المؤسسات المالية الصغيرة والمتوسطة (Metibemu, 2025; Yussuf et al., 2020).

ومن التحديات الحرجة أيضا مخاطر الخصوصية وحماية البيانات، إذ تتطلب أنظمة الذكاء الاصطناعي جمع وتحليل كميات هائلة من البيانات الشخصية والسلوكية للعملاء والموظفين، مما يثير مخاوف جدية بشأن انتهاك الخصوصية وإمكانية إساءة استخدام هذه المعلومات الحساسة، خاصة في ظل التشريعات الصارمة كاللائحة العامة لحماية البيانات الأوروبية التي تفرض قيودا صارمة على معالجة البيانات الشخصية (Soldatova, 2026; Ahmad, 2023). ويضاف إلى ذلك تحدي جودة البيانات وتحيزاتها، حيث أن أنظمة الذكاء الاصطناعي تعتمد بشكل جوهري على البيانات التدريبية، وأي تحيزات أو عيوب في هذه البيانات قد تنتقل إلى النماذج المدربة، مما ينتج عنه قرارات أمنية منحازة أو غير دقيقة قد تميز ضد فئات معينة من العملاء أو تخفق في اكتشاف أنماط تهديدات جديدة لم تكن موجودة في البيانات التاريخية (Ejiofor, 2023; Zainal, 2023).

وتبرز كذلك مخاطر التسليح المضاد للذكاء الاصطناعي، إذ يمكن للمهاجمين السيبرانيين استخدام تقنيات الذكاء الاصطناعي لتطوير هجمات خصومية مصممة خصيصا لخداع أنظمة الذكاء الاصطناعي الدفاعية، من خلال توليد برمجيات خبيثة أو رسائل تصيد احتيالي مخصصة تتجاوز آليات الكشف الآلي (Chukwu, 2024; Clement, 2024). علاوة على ذلك، يشكل التكامل مع الأنظمة القديمة تحديا تقنيا معقدا، حيث تعمل العديد من المؤسسات المالية على بنى تحتية تقنية قديمة يصعب دمجها سلسا مع تطبيقات الذكاء الاصطناعي الحديثة، مما يتطلب جهودا كبيرة في التحديث والتوافقية والانتقال التدريجي (Asmar & Tuqan, 2024). وأخيرا، تواجه المؤسسات تحديات الامتثال التنظيمي، إذ أن الأطر القانونية والتنظيمية الحالية في العديد من الدول لم تواكب بعد التطورات السريعة في تقنيات الذكاء الاصطناعي، مما يخلق حالة من الغموض القانوني بشأن المسؤولية عن قرارات الأنظمة الذكية، وكيفية إثبات الامتثال للمعايير الأمنية، والإجراءات الواجب اتباعها عند حدوث فشل في الأنظمة المدعومة بالذكاء الاصطناعي (Soldatova, 2026; Ayeola, 2025). وتتطلب هذه التحديات المتشابكة استراتيجيات متكاملة تجمع بين الاستثمار التقني المستدام، وتطوير الكفاءات البشرية، وبناء أطر حوكمة رشيدة، وتعزيز التعاون بين القطاعين العام والخاص لضمان تسخير الإمكانيات الكاملة للذكاء الاصطناعي في تأمين المنظومة المالية الرقمية.

ثالثا: حالات واقعية للتطبيقات العملية للذكاء الاصطناعي في الأمن السيبراني:

تظهر التطبيقات المعاصرة للذكاء الاصطناعي في مجال الأمن السيبراني أن هذا التحول لم يعد مجرد تطوير تقني محدود، بل أصبح جزءا من البنية التشغيلية للمؤسسات في الكشف عن التهديدات وتحليلها والاستجابة لها. ومن أبرز الأمثلة على ذلك حالة Microsoft Defender، حيث يستخدم الذكاء الاصطناعي في فرز الرسائل التي يشتبه في كونها محاولات تصيد إلكتروني، وذلك من خلال تحليل محتوى الرسائل وروابطها ومرفقاتها وسياقها العام. وتبدو أهمية هذه الحالة في كونها تعكس الدور العملي للذكاء الاصطناعي في تقليل العبء المتزايد على محلي الأمن، خاصة في البيئات التي تشهد حجما كبيرا من التنبيهات اليومية. غير أن هذه الحالة تكشف أيضا أن فعالية الذكاء الاصطناعي تظل مرتبطة

بوجود إشراف بشري يراجع المخرجات ويضبط حدود الاعتماد عليها، لأن الخطأ في التصنيف قد يؤدي إلى تجاهل تهديد حقيقي أو تضخيم إنذار غير مهم .

وفي مثال آخر، توضح حالة Google Security Operations كيف تطور دور الذكاء الاصطناعي من مجرد دعم التحليل إلى المساهمة في أتمتة الاستجابة للحوادث الأمنية. فالمنصة تتيح التعامل مع سيناريوهات متكررة مثل التصيد أو برمجيات الفدية عبر إجراءات جاهزة تنفذ بطريقة أكثر سرعة وتنظيمًا. وتبرز أهمية هذه الحالة في أنها تقدم صورة عملية عن كيفية الاستفادة من الذكاء الاصطناعي في توحيد الاستجابة وتقليل الوقت المستغرق في التنسيق بين الفرق الأمنية. ومع ذلك، فإن هذه الفاعلية لا تعني غياب المخاطر، إذ إن الاعتماد على الأتمتة قد يصبح مشكلة بحد ذاته إذا كانت قواعد التنفيذ غير دقيقة أو إذا بنيت القرارات على بيانات ناقصة أو منحازة. لذلك فإن هذه الحالة تؤكد أن إدماج الذكاء الاصطناعي في العمل الأمني ينبغي أن يتم في إطار حوكمة واضحة، تضمن سلامة القرار الآلي وتحد من آثاره غير المقصودة.

أما حالة Darktrace المرتبطة بمجموع Wasted Locke، فهي تمثل مثالاً مهماً على قدرة الذكاء الاصطناعي على كشف السلوك الشاذ داخل الشبكات حتى عندما يستخدم المهاجم أدوات وأساليب يصعب تمييزها بالوسائل التقليدية. فالهجوم لم يعتمد على برمجيات مكشوفة بسهولة، بل على تحركات بدت في ظاهرها قريبة من النشاط المعتاد داخل البيئة الرقمية للمؤسسة. وهنا برزت فائدة التحليل السلوكي الذي يعتمد على فهم النمط الطبيعي للشبكة، ثم رصد أي انحراف عنه في الوقت المناسب. وتعد هذه الحالة من أكثر النماذج إقناعاً في إظهار القيمة الفعلية للذكاء الاصطناعي في البيئات المعقدة والمتغيرة، لكنها في الوقت نفسه تثير مسألة تفسير قرارات الأنظمة الذكية، إذ قد يصعب على المسؤولين الأمنيين أحياناً فهم الكيفية التي توصل بها النظام إلى تصنيف سلوك معين بوصفه خطراً. ومن ثم، فإن نجاح هذا النوع من الحلول لا يرتبط بالدقة التقنية وحدها، بل أيضاً بقدرتها على تقديم نتائج قابلة للفهم والمراجعة.

وعلى الجانب المقابل، تكشف حالة Trend Micro الخاصة بانتحال شخصية المدير المالي عبر التزييف العميق عن أن الذكاء الاصطناعي لا يخدم الدفاع فقط، بل يمكن أن يتحول إلى أداة فعالة بيد المهاجمين. وتنبع خطورة هذه الحالة من أنها تظهر تطور أساليب الهندسة الاجتماعية من الرسائل والنصوص المزيفة إلى محاكاة الصوت والصورة بصورة يصعب على الموظف العادي اكتشافها بسهولة. وبهذا المعنى، فإن التهديد هنا لا يتعلق بخلل تقني في النظام بقدر ما يتعلق باستغلال الثقة البشرية والإجراءات التنظيمية. ولهذا تقدم هذه الحالة دليلاً واضحاً على أن مواجهة مخاطر الذكاء الاصطناعي في الأمن السيبراني لا يمكن أن تعتمد على الحلول التقنية فقط، بل يجب أن تشمل أيضاً مراجعة مسارات التحقق، وفرض آليات اعتماد متعددة، ورفع مستوى الوعي المؤسسي بمخاطر الخداع المدعوم بالتقنيات الذكية.

ويمكن القول في ضوء هذه الحالات الأربع إن الذكاء الاصطناعي في الأمن السيبراني يحمل طبيعة مزدوجة، فهو من ناحية يعزز قدرات الرصد والتحليل وسرعة الاستجابة، ومن ناحية أخرى يمنح المهاجمين أدوات أكثر تطوراً في الإخفاء والخداع والتأثير. لذلك فإن النقاش حول الذكاء الاصطناعي في هذا المجال لا ينبغي أن يقتصر على إبراز مزاياه التقنية، بل يجب أن يمتد إلى مساءلة مخاطره وحدود الاعتماد عليه، وآليات ضبطه داخل المؤسسة. ومن هنا تكتسب هذه الحالات أهميتها في الجانب التطبيقي للمقال، لأنها تنقل الموضوع من المستوى النظري إلى مستوى الممارسة الفعلية، وتبين أن نجاح المؤسسات في الاستفادة من الذكاء الاصطناعي سيظل رهيناً بقدرتها على تحقيق توازن دقيق بين التوظيف الفعال لهذه التقنيات وبين التحكم فيما تفرضه من مخاطر وتحديات جديدة.

الخاتمة:

في ختام هذه الدراسة التي استهدفت استكشاف دور تطبيقات الذكاء الاصطناعي في تعزيز منظومة الأمن السيبراني بمختلف القطاعات، وتحليل التحديات الجوهرية التي تواجه هذا التوظيف، يمكن التأكيد على أن الذكاء الاصطناعي لم يعد خياراً تقنياً تكميلياً، بل أصبح ضرورة استراتيجية لرفع كفاءة الحماية السيبرانية، لا سيما في البيئات المالية الرقمية التي تتسم بارتفاع حساسية البيانات وتسارع وتيرة التهديدات وتعاضم الآثار المترتبة على الاختراقات الأمنية. وقد أظهر التحليل المفاهيمي والتطبيقي أن تقنيات الذكاء الاصطناعي، بما تتضمنه من تعلم آلي وتعلم عميق ومعالجة اللغة الطبيعية، أسهمت في إحداث تحول نوعي في آليات الكشف الاستباقي عن التهديدات، وتحليل الأنماط الشاذة، ومكافحة الاحتيال المالي، ومعالجة التهديدات الداخلية، والاستجابة السريعة والآلية للحوادث الأمنية، بما يدعم انتقال المؤسسات من منطق الدفاع التفاعلي إلى منطق الحماية التنبؤية الذكية. وفي المقابل، كشفت الدراسة أن هذا التحول، رغم أهميته، لا يخلو من تحديات معقدة تحد من فعالية توظيف الذكاء الاصطناعي في الأمن السيبراني، من أبرزها محدودية الشفافية وقابلية التفسير، ومخاطر الخصوصية وحماية البيانات، والتحيزات المرتبطة ببيانات التدريب، وإشكالية الإيجابيات الكاذبة وإرهاق التنبيهات، فضلاً عن ارتفاع متطلبات البنية التحتية التقنية، وندرة الكفاءات المتخصصة، والتعرض للهجمات الخصومية، والغموض التنظيمي والقانوني المتعلق بالمسؤولية والامتثال. وعليه، فإن فعالية الأمن السيبراني المدعوم بالذكاء الاصطناعي لا تتحدد فقط بمدى تطور الخوارزميات، بل أيضاً بمدى نضج البيئة المؤسسية والقانونية والتنظيمية التي تحتضن هذه التقنيات.

أولاً: اختبار الفرضيات:

1. الفرضية الأولى: هناك علاقة إيجابية بين توظيف تطبيقات الذكاء الاصطناعي وبين تعزيز فعالية منظومة الأمن السيبراني، من حيث دقة الكشف عن التهديدات، وكفاءة التحليل الأمني، وسرعة الاستجابة للهجمات داخل البيئات الرقمية المالية.

الإجابة عن الفرضية الأولى: أظهرت الدراسة صحة هذه الفرضية، حيث تبين من خلال التحليل أن تطبيقات الذكاء الاصطناعي تسهم بصورة مباشرة في رفع كفاءة الأمن السيبراني داخل البيئات الرقمية المالية، وذلك عبر تحسين القدرة على اكتشاف السلوكيات الشاذة والتهديدات المعقدة في وقت مبكر، وتعزيز دقة التحليل الأمني للبيانات الضخمة والمتدفقة، وتسريع الاستجابة للحوادث والهجمات المتطورة. كما ثبت أن النظم الذكية تمكن المؤسسات المالية من الانتقال من الاستجابة اللاحقة إلى الرصد الاستباقي والوقاية المبكرة، بما يحد من الخسائر المحتملة ويعزز مرونة المنظومة الأمنية. وبناء عليه، تقبل **الفرضية الأولى** لما توفره الأدلة النظرية والتطبيقية من دعم واضح للعلاقة الإيجابية بين توظيف الذكاء الاصطناعي وفعالية الأمن السيبراني.

2. الفرضية الثانية: تؤثر التحديات المرتبطة باستخدام الذكاء الاصطناعي، مثل محدودية الشفافية، ومخاطر الخصوصية، تأثيراً مباشراً في كفاءة تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي داخل البيئات الرقمية المالية.

الإجابة عن الفرضية الثانية: أكدت الدراسة كذلك صحة هذه الفرضية، إذ كشفت أن التحديات المصاحبة لتوظيف الذكاء الاصطناعي تؤثر تأثيراً مباشراً ولمموساً في كفاءة تطبيقه الأمني. فمحدودية الشفافية وصعوبة تفسير مخرجات بعض النماذج الذكية تقللان من الثقة المؤسسية في قراراتها، كما أن مخاطر الخصوصية والتعامل مع البيانات الحساسة تفرض قيوداً تنظيمية وأخلاقية تحد من التوسع الآمن في استخدامها. ويضاف إلى ذلك أن التحيزات الخوارزمية، والإيجابيات الكاذبة، والهجمات العدائية الموجهة ضد النماذج، كلها عوامل تضعف موثوقية الحلول الذكية وتؤثر في جودة الأداء الأمني. وبناء على ذلك، تقبل **الفرضية الثانية**، لأن الدراسة أثبتت أن التحديات التقنية والتنظيمية والقانونية ليست عناصر هامشية، بل محددات جوهرية لنجاح أو تعثر تطبيق الأمن السيبراني المدعوم بالذكاء الاصطناعي.

ثانياً: نتائج الدراسة توصلت الدراسة إلى مجموعة من النتائج الرئيسة التي يمكن إجمالها فيما يأتي:

- إن الذكاء الاصطناعي يمثل أداة استراتيجية فعالة في تطوير منظومة الأمن السيبراني، خاصة في البيئات المالية الرقمية التي تتطلب قدرة عالية على الرصد والتحليل الفوري والتعامل مع التهديدات المتغيرة.
- أسهمت تطبيقات الذكاء الاصطناعي في تعزيز دقة الكشف عن الهجمات والأنشطة غير الطبيعية، وفي تقليص الزمن اللازم لتحليل الحوادث واتخاذ القرار الأمني المناسب.
- أتاح الذكاء الاصطناعي إمكانات متقدمة في مكافحة الاحتيال المالي، ورصد التهديدات الداخلية، وتحليل الأنماط السلوكية للمستخدمين والأنظمة، بما يرفع من مستوى الحماية ويحد من الخسائر.
- تبين أن فعالية هذه التطبيقات تبقى مرهونة بجودة البيانات المستخدمة في تدريب النماذج، وبمدى تكاملها مع البنية التقنية للمؤسسة، وبقدرة الموارد البشرية على فهمها وإدارتها.

- كشفت الدراسة أن أبرز معوقات التوظيف الفعال للذكاء الاصطناعي في الأمن السيبراني تتمثل في ضعف الشفافية وقابلية التفسير، ومخاطر الخصوصية، والتحيز الخوارزمي، وارتفاع كلفة البنية التحتية، وندرة الخبرات المتخصصة.
- أوضحت الدراسة أن المخاطر القانونية والتنظيمية المرتبطة باستخدام الذكاء الاصطناعي، خصوصا في المجال المالي، تمثل تحديا حقيقيا في ظل غياب أطر تشريعية موحدة تحدد المسؤوليات وتضبط آليات المساءلة والامتثال.
- خلصت الدراسة إلى أن الذكاء الاصطناعي في الأمن السيبراني يحمل طابعا مزدوجا، فهو من جهة أداة لتعزيز الدفاع الرقمي، ومن جهة أخرى قد يتحول إلى مصدر للمخاطر إذا غابت الحوكمة، أو استخدم ضمن بيئة تنظيمية وتقنية غير ناضجة.

ثالثا: توصيات الدراسة:

- في ضوء ما أسفرت عنه الدراسة من نتائج، يمكن تقديم التوصيات الآتية:
- ضرورة تبني المؤسسات المالية لاستراتيجيات متكاملة لتوظيف الذكاء الاصطناعي في الأمن السيبراني، تقوم على الجمع بين التطوير التقني، والتأهيل البشري، والحوكمة المؤسسية.
 - الاستثمار المستدام في البنية التحتية التقنية القادرة على استيعاب تطبيقات الذكاء الاصطناعي، بما يشمل منصات تحليل البيانات، وأنظمة الرصد الذكي، وأدوات الاستجابة الآلية للحوادث.
 - تطوير الكفاءات البشرية المتخصصة من خلال برامج تدريبية تجمع بين الأمن السيبراني وعلوم البيانات والذكاء الاصطناعي، بما يضمن الاستخدام الواعي والفعال لهذه الأدوات.
 - إرساء أطر حوكمة واضحة للذكاء الاصطناعي داخل المؤسسات، تقوم على مبادئ الشفافية، والمساءلة، وحماية الخصوصية، وإدارة المخاطر، وتقليل التحيز الخوارزمي.
 - اعتماد نماذج ذكاء اصطناعي قابلة للتفسير كلما أمكن، خاصة في المجالات الحساسة ذات الارتباط بالقرارات الأمنية والمالية، وذلك لتعزيز الثقة وتحسين قابلية المراجعة والتدقيق.
 - تعزيز آليات حماية البيانات الشخصية والمالية، ووضع سياسات صارمة لتنظيم جمع البيانات ومعالجتها وتخزينها، بما ينسجم مع متطلبات الأمن والامتثال القانوني.
 - توسيع التعاون بين المؤسسات المالية والجهات التنظيمية ومراكز البحث، بهدف تبادل الخبرات وتطوير معايير موحدة لاستخدام الذكاء الاصطناعي في الأمن السيبراني.

- تشجيع التنسيق الإقليمي والدولي في مواجهة الجرائم السيبرانية العابرة للحدود، خاصة تلك التي تستفيد من تقنيات الذكاء الاصطناعي في تطوير أساليب التخفي والهجوم.

رابعاً: الآفاق البحثية المستقبلية:

تفتح هذه الدراسة المجال أمام عدد من المسارات البحثية المستقبلية التي يمكن أن تعمق فهم العلاقة بين الذكاء الاصطناعي والأمن السيبراني، ومن أبرزها:

- إجراء دراسات ميدانية وقياسية لقياس أثر تطبيقات الذكاء الاصطناعي في تحسين الأداء الأمني داخل المؤسسات المالية، اعتماداً على مؤشرات كمية دقيقة.

- دراسة فعالية النماذج القابلة للتفسير في تقليل فجوة الثقة بين الأنظمة الذكية وصناع القرار الأمني، خاصة في البيئات شديدة الحساسية.

- بحث أثر الهجمات الخصومية على نماذج الذكاء الاصطناعي الأمنية، وتطوير آليات دفاعية تجعل هذه النماذج أكثر صلابة وموثوقية.

- تحليل الأبعاد القانونية والأخلاقية لتوظيف الذكاء الاصطناعي في الأمن السيبراني، لا سيما فيما يتعلق بالمسؤولية عن القرارات الآلية وحماية البيانات والامتثال التنظيمي.

- التوسع في الدراسات المقارنة بين القطاعات المختلفة، مثل القطاع المالي، والصحي، والحكومي، والصناعي، لمعرفة مدى اختلاف متطلبات الأمن السيبراني المدعوم بالذكاء الاصطناعي من قطاع إلى آخر.

- تطوير نماذج بحثية تركز على التوازن بين الكفاءة الأمنية والضمانات الحقوقية، بما يضمن عدم التضحية بالخصوصية والعدالة والشفافية في سبيل رفع الكفاءة التقنية.

يمكن القول في المحصلة إن الذكاء الاصطناعي يشكل ركيزة واعدة في تطوير الأمن السيبراني داخل البيئات الرقمية المالية، لما يوفره من قدرات متقدمة في الكشف والتحليل والاستجابة، غير أن نجاح هذا التوظيف يظل رهيناً بوجود منظومة متكاملة من الحوكمة، والتشريع، والجاهزية التقنية، والكفاءة البشرية. وعليه، فإن المستقبل الفعلي للأمن السيبراني المدعوم بالذكاء الاصطناعي لن يتحدد فقط بمستوى التقدم الخوارزمي، بل بمدى قدرة المؤسسات والدول على إدارة مخاطره، وضبط استخدامه، وتوجيهه نحو حماية أكثر ذكاء وعدالة وموثوقية.

قائمة المراجع:

- 1- بخوش، س. (2025). الذكاء الاصطناعي والأمن السيبراني: الوظائف والتحديات. المجلة الجزائرية للعلوم الإنسانية والإجتماعية، 9 (1)، 136 – 151.
- 2-Ahmad, A. S. (2023). Application of big data and artificial intelligence in strengthening fraud analytics and cybersecurity resilience in global financial markets. *International Journal of Advanced Cybersecurity Science and Technology Analysis*, 3(12), 45-67.
- 3-Ajayi, A. M., Omokanye, A. O., Olowu, O., & Wada, I. (2024). Detecting insider threats in banking using AI-driven anomaly detection with a data science approach to cybersecurity. *International Journal of Cybersecurity Intelligence & Cybercrime*, 7(2), 102-128.
- 4-Alalwan, J. A. A. (2022). Roles and challenges of AI-based cybersecurity: A case study. *Jordan Journal of Business Administration*, 18(3).
- 5-Ali, A. H., Mohameed, W. K., & Alaloosh, M. S. (2025). Legal challenges of cyber risk on commercial transactions. *Malaysian J. Syariah & L.*, 13, 456.
- 6-Alkhalidi, F. M., Hammami, S. M., & Ahmar Uddin, M. (2017). Understanding value characteristics toward a robust IT governance application in private organizations using COBIT framework. *International Journal of Engineering Business Management*, 9, 184797901770377.
- 7-Almeida, R., Gonçalves, P. A., Percheiro, I., Mira Da Silva, M., & Pardo, C. (2020). Integrating COBIT 5 PAM and TIPA for ITIL using an ontology matching system. *International Journal of Human Capital and Information Technology Professionals*, 11(3), 74–93.
- 8-Almusawi, I. G. (2022). Using COBIT framework for reducing the audit risks of accounting information systems. *Akkad Journal of Contemporary Accounting Studies*, 1(1), 52–74.
- 9-Andress, J. (2014). *The basics of information security - Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). DC, USA.
- 10-Andry, J. F., & Hartono, H. (2017). Performance measurement of IT based on COBIT assessment: A case study. *Jurnal Sistem Informasi Indonesia (JSII)*, 2(1), 1-13.
- 11-Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon*, 10(19), e37571.

- 12-Ayeola, F. (2025). AI-driven anomaly detection and data governance: Securing financial systems, cybersecurity networks, and regulatory compliance in multicultural digital ecosystems. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.5439102>
- 13-Ayoola, V. B., Ugoaghalam, U. J., Idoko, P. I., & Amana, D. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *International Journal of Engineering and Applied Sciences*, 6(4), 145-162.
- 14-Baur-Yazbeck, S., Frickenstein, J., & Leclerc, S. (2019). Cyber security in financial sector development: Challenges and potential solutions for financial inclusion (CGAP Background Paper). World Bank Group.
- 15-Chukwu, B. (2024). A critical intersection of cybersecurity, AI and fraud detection in the United States financial market. *International Journal of Science and Research Archive*, 13(2), 1145-1168.
- 16-Clement, O. (2024). AI in cybersecurity for financial institutions: Threat detection and prevention. *Journal of Information Security and Cybersecurity Research*, 7(3), 215-234.
- 17-Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alawad, M. A., Aloufi, K. S., & Alahmadi, A. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, 11, 119066-119092.
- 18-Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: Integrating machine learning and AI in fraud detection systems. *European Journal of Computer Science and Information Technology*, 11(4), 32-56.
- 19-Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive analytics for cyber threat intelligence in fintech using big data and machine learning. *International Journal of Research Publication and Reviews*, 5(10), 2847-2871.
- 20-Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, 8(1), e70016.
- 21-Gonaygunta, H. (2023). Factors influencing the adoption of machine learning algorithms to detect cyber threats in the banking industry [Doctoral dissertation, Capitol Technology University]. ProQuest Dissertations Publishing.
- 22-Grosz, B. J., Mackworth, A., Altman, R., Horvitz, E., Mitchell, T., Mulligan, D., & Shoham, Y. (2016). Artificial intelligence and life in 2030: One Hundred Years Study on Artificial Intelligence. Stanford University.

- 23-Hammour, R. A., Gharaibeh, Y. A., Qasaimeh, M., & Al-Qadi, Z. (2019). The status of information security systems in banking sector from social engineering perspective. *Proceedings of the 2019 2nd International Conference on Information Science and Systems*, 109-113.
- 24-Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access*, 9, 7152-7169.
- 25-InterviewBit. (2023, February 26). Top 10 characteristics of artificial intelligence. <https://www.interviewbit.com/blog/characteristics-of-artificial-intelligence/>
- 26-ISO/IEC Standard for Corporate Governance of Information Technology. (2008, June 5). ISO. <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2008/06/ref1135.html>
- 27-Johns, M. (2009). Code injection vulnerabilities in web applications: Exemplified at cross-site scripting [Doctoral dissertation, University of Passau]. OPUS.
- 28-Khazal, I. F., Ghaib, A. A., Shareef, A., Abduljabbar, Z. A., Nyangaresi, V., & Al-Juboori, A. M. (2025). Cross site scripting attacks (XSS): A review. In *Computer Science On-line Conference* (pp. 339-349). Springer.
- 29-Kļaviņš, D. (2025). Cyber diplomacy: Latvia's voice in the world. In *Cybersecurity in Latvia* (pp. 145-168). Routledge.
- 30-Luger, G. F., & Chakrabarti, C. (2017). From Alan Turing to modern AI: Practical solutions and an implicit epistemic stance. *AI & Society*, 32(3), 321-338.
- 31-Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 2700.
- 32-Metibemu, O. C. (2025). Financial risk management in digital-only banks: Addressing fraud and cybersecurity threats in a cashless economy. *SSRN Electronic Journal*.
- 33-Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the human factor in cybersecurity: Identifying and preventing social engineering attacks in financial institution. *IEEE Xplore*, 1-8.
- 34-Muzammil, M. B., Bilal, M., Ajmal, S., Shongwe, S. C., & Bhutta, M. N. M. (2024). Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking. *IEEE Access*, 12, 1825-1842.
- 35-Olech, A., & Štrucl, D. (2025). The evolution of cyber forces in NATO countries. NATO Cooperative Cyber Defence Centre of Excellence.

- 36-Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: A comprehensive review. SSRN Electronic Journal.
- 37-Pramanick, N., Mathew, J., Selvarajan, S., & Agarwal, M. (2025). Leveraging stacking machine learning models and optimization for improved cyberattack detection. Scientific Reports, 15, 1052.
- 38-Rosa, A., Feyereisl, J., & Team, T. G. (2016). A framework for searching for general artificial intelligence. CoRR abs./1611.00685, 1-54.
- 39-Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022). Information system audit using COBIT and ITIL framework: Literature review. Sinkron, 7(3), 799–810.
- 40-Sadia, S. (2021). Tabani al-dhaka' al-istina'i fi sharikat al-tamin ka-al-iya li-ta'aziz al-shumul al-mali: Dirasat halat sharikat AXA [Adoption of AI in insurance companies as a mechanism to enhance financial inclusion: A case study of AXA]. Majallat al-Jaza'iriyah li-Iqtisad al-Idarah, 15(1), 45–62.
- 41-Sadoughi, F., Davaridolatabadi, N., Ahmadi, M., & Shahi, M. (2019). Principles, domains and processes of HIT governance frameworks: A systematic review. Gazi Medical Journal, 30(4).
- 42-Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 53–74.
- 43-Schmidt, R. H., & Tyrell, M. (2003). What constitutes a financial system in general and the German financial system in particular? (No. 111). Working Paper Series: Finance & Accounting.
- 44-Signor, S. (2023). Cyber warning intelligence: Enhancing predictive capabilities in cyberspace. A comparative study of the American and Italian cases [Master's thesis, Charles University]. Digital Repository of Charles University.
- 45-Smits, D., & Hillegersberg, J. Van. (2013). The continuing mismatch between IT governance theory and practice: Results from a Delphi study with CIOs.
- 46-Soldatova, J. (2026). Using artificial intelligence technologies in compliance processes in the banking sector in Lithuania: Challenges and opportunities from corporate digital responsibility perspective [Master's thesis, ISM University of Management and Economics]. eLABa.
- 47-Tibah, S. (2018). Présentation cyber risques. Compagnie centrale de réassurance (CCR).

- 48-Udayakumar, R., Joshi, A., Boomiga, S. S., & Bharanidharan, N. (2023). Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. *Journal of Internet Services and Information Security*, 13(4), 140-159. <https://jisis.org/wp-content/uploads/2023/12/2023.I4.010.pdf>
- 49-Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Omidiora, J. O. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive*, 12(1), 1823-1841.
- 50-Wu, J., Dong, M. X., Ota, K., et al. (2018). Big data analysis based secure cluster management for optimized control plane in software-defined networks. *IEEE Trans. Netw. Serv. Manag.*, 15(1), 27-38.
- 51-Yussuf, M. F., Oladokun, P., & Williams, M. (2020). Enhancing cybersecurity risk assessment in digital finance through advanced machine learning algorithms. *International Journal of Computer Applications Technology and Research*, 9(11), 445-464.
- 52-Zainal, A. (2023). Role of artificial intelligence and big data technologies in enhancing anomaly detection and fraud prevention in digital banking systems. *International Journal of Advanced Cybersecurity Science and Technology Analysis*, 3(12), 23-44.