

مساهمة الذكاء الاصطناعي في مواجهة التهديدات السيبرانية بالقطاع المصرفي

The contribution of artificial intelligence in countering cyber threats in the banking sector

بغداد زكرياء¹، حركاتي نبيل²¹ جامعة سطيف 1- فرحات عباس، الجزائر، مخبر تقييم رؤوس الأموال الجزائرية في ظل العولمة، baghded.zakaria@univ-setif.dz² جامعة سطيف 1- فرحات عباس، الجزائر، مخبر تقييم رؤوس الأموال الجزائرية في ظل العولمة، nharkati@univ-setif.dz

تاريخ الاستلام: 2026/01/10 تاريخ القبول: 2026/04/16 تاريخ النشر: 2026/04/30

ملخص:

تتناول هذه الورقة البحثية دور الذكاء الاصطناعي في تعزيز الأمن السيبراني بالقطاع المصرفي، عبر تحليل مفاهيم كل منهما وطبيعة العلاقة التكاملية بينهما. وقد توصلت النتائج إلى إسهام الذكاء الاصطناعي بشكل فعال في حماية الأنظمة المصرفية، حيث أكدت الإحصائيات مساعدة التقنيات المعتمدة عليه في خفض تكاليف الخروقات الأمنية وتسريع الاستجابة لها. إلا أن التطبيق لا يخلو من تحديات، أبرزها مواكبة التهديدات الإلكترونية المتسارعة وبعض القيود المرتبطة بالذكاء الاصطناعي.

بناءً على ذلك، توصي الدراسة بتعزيز الاستثمار في تطوير وتوظيف تقنيات الذكاء الاصطناعي للأمن السيبراني، مع التركيز على البنية التحتية الرقمية وتأهيل الكوادر المتخصصة. كما تشدد على أهمية تعزيز التعاون بين المؤسسات المالية لتبادل الخبرات والإنذارات المبكرة، وإقامة شراكات مع المؤسسات الأكاديمية والبحثية لابتكار حلول متقدمة والاستعداد للمخاطر المستقبلية.

كلمات مفتاحية: تحول رقمي، ذكاء اصطناعي، أمن سيبراني، قطاع مصرفي، تحديات أمنية.

تصنيفات JEL: O33، M15، L86، G21.

Abstract:

This research paper addresses the role of artificial intelligence in enhancing cybersecurity within the banking sector by analyzing the fundamental concepts of each and exploring the nature of their

المؤلف المرسل: بغداد زكرياء، الإيميل: baghded.zakaria@univ-setif.dz

complementary relationship. The findings indicate that AI contributes effectively to protecting banking systems, with statistics confirming that AI-based technologies help reduce the costs of security breaches and accelerate response times. However, the implementation is not without challenges, most notably keeping pace with rapidly evolving cyber threats and certain limitations associated with artificial intelligence itself.

Accordingly, the study recommends increasing investment in the development and deployment of AI technologies for cybersecurity, with a focus on digital infrastructure and training specialized personnel. It also emphasizes the importance of enhancing cooperation among financial institutions to exchange expertise and early warnings, and establishing partnerships with academic and research institutions to develop innovative solutions and continue research and development efforts in preparation for future risks.

Keywords: Digital transformation, artificial intelligence, cybersecurity, banking sector, security challenges

Jel Classification Codes: O33, M15, L86, G21.

1. مقدمة:

شهد القطاع المصرفي تطورا هائلا بفضل الرقمنة التي جعلت الخدمات المصرفية سهلة ومتاحة لأي عميل من أي مكان في العالم، ومع ذلك، فإن هذا التحول الرقمي السريع قد جلب معه تحديات جديدة خاصة في مجال الأمن السيبراني، حيث أصبحت الخدمات المصرفية الرقمية هدفا لمجرمي الإنترنت الذين يمكنهم تهديد أنظمتها بواسطة هجمات إلكترونية معقدة ومتطورة كبدت المؤسسات المالية خسائر طائلة، مما دعا إلى الحاجة الملحة لإعادة النظر في الضرورات الأمنية، إلى أن ظهر الذكاء الاصطناعي مؤخرا كأداة قوية جدا لدعم الأمن السيبراني الذي يؤدي دورا حاسما في مواجهة التحديات الأمنية المتزايدة في العالم الرقمي، من خلال الكشف عن التهديدات والاستجابة السريعة والتنبؤ بالمخاطر المستقبلية. ومع تطور التهديدات، سيظل الذكاء الاصطناعي عاملا رئيسيا في بناء دفاعات أكثر ذكاء وقدرة على التكيف.

الإشكالية: من خلال ما سبق يمكن طرح إشكالية البحث في التساؤل التالي:

كيف يساهم الذكاء الاصطناعي في مواجهة التهديدات السيبرانية بالقطاع المصرفي؟

للإجابة على الإشكالية المطروحة، تم صياغة الفرضية التالية:

يساهم الذكاء الاصطناعي بشكل إيجابي في خفض نسبة التهديدات السيبرانية بالقطاع المصرفي.

أهداف البحث: تسعى هذه الدراسة لتحقيق جملة من الأهداف يمكن إيجازها فيما يلي:

- توضيح مفهوم الذكاء الاصطناعي وتطبيقاته بالقطاع المصرفي؛
- استعراض أهم التهديدات السيبرانية التي تواجه القطاع المصرفي؛
- الاطلاع على آخر الإحصائيات المتعلقة بالتهديدات السيبرانية ومساهمة الذكاء الاصطناعي في التصدي لها.

منهجية البحث:

يعتمد البحث على المنهج الوصفي التحليلي، من خلال وصف شامل للذكاء الاصطناعي والأمن السيبراني استناداً إلى مراجع ودراسات سابقة حديثة، مع تحليل الواقع الحالي للذكاء الاصطناعي والأمن السيبراني بالقطاع المصرفي.

2. الذكاء الاصطناعي في القطاع المصرفي

في عالم يتسارع نحو الرقمنة، أصبح الذكاء الاصطناعي أحد أهم الأدوات التي تعيد تشكيل القطاع المصرفي، إذ لم يعد مجرد تقنية مستقبلية، بل تحول إلى جزء من العمليات اليومية للبنوك، فمن خلال تطبيقات متعددة يعمل الذكاء الاصطناعي على تبسيط العمليات المصرفية المعقدة وتقديم حلول مبتكرة تلبي توقعات العملاء.

1.2 نبذة عن نشأة وتطور الذكاء الاصطناعي:

تطور الذكاء الاصطناعي من مجرد أفكار نظرية خلال الحرب العالمية الثانية إلى ثورة تقنية حديثة تعتمد على التعلم العميق، حيث قدم آلان تورينج (Alan Turing) عام 1950 اختباراً لتقييم ذكاء الآلات، ثم تأسس المجال رسمياً عام 1956 خلال مؤتمر دارتموث حيث ظهر مصطلح "الذكاء الاصطناعي" لأول مرة. أتى بعد ذلك العصر الذهبي (حتى 1974) الذي شهد تطبيقات مبكرة مثل برنامج المحادثة "إليزا" وروبوت "WABOT-1" الياباني، إلا أن القيود التقنية أدت إلى فترات ركود عُرفت باسم "شتاء الذكاء الاصطناعي".

عاد الاهتمام في الثمانينيات مع أنظمة الخبراء، لكن الطفرة الحقيقية حدثت في الألفية الجديدة بفضل تطور وحدات معالجة الرسومات (GPUs) التي سرّعت تدريب الشبكات العصبية العميقة،

مفسحة المجال لتطبيقات ثورية في الطب والصناعة. ومن أبرز الإنجازات: فوز "واتسون" (IBM) بمسابقة جوباردي عام 2011، ونجاح "يوجين جوستمان" في اجتياز اختبار تورينج عام 2014، وتطوير "دوبلكس" (جوجل) لنظام حوار متقدم عام 2018. وعلى الرغم من ارتباط الذكاء الاصطناعي الوثيق بعلم البيانات، إلا أنه يظل مجالا أوسع يهدف إلى محاكاة القدرات الذهنية البشرية. (Adib Bin Rashid, MD Ashfakul Karim Kausik, 2024, pp. 3-5).

2.2 تعريف الذكاء الاصطناعي:

هو تقنية نموذجية قادرة على أداء مختلف وظائف العقول البشرية مثل التفكير والتعلم والتفاعل مع البيئة وممارسة الرياضة (Vishal Dineshkumar Soni, 2020, p. 4). بمعنى أن الذكاء الاصطناعي عبارة عن أنظمة كمبيوتر قادرة على محاكاة الوظائف المعرفية البشرية، كالاستدلال والتنبؤ والتعرف على الأنماط وفهم اللغة الطبيعية وتوليدها، من تحليل كميات هائلة من البيانات واستخلاص الأنماط والعلاقات الكامنة فيها، لتصبح قادرة لاحقا على اتخاذ القرارات. وعلى الرغم من أن العديد من أنظمة الذكاء الاصطناعي تُدرَّب تحت إشراف بشري لتوجيه تعلمها، توجد نماذج أخرى مصممة لاكتساب المعرفة ذاتيا. ومع مرور الوقت، تطور هذه الأنظمة كفاءتها مما يمكنها من التكيف مع البيانات الجديدة وإصدار أحكام مستقلة دون الحاجة إلى برمجة مسبقة (Mahfujur Rahman Faraji et al, 2024, p. 4769). باختصار، الذكاء الاصطناعي هو قدرة الآلة على محاكاة الذكاء البشري لتبسيط المهام وتعزيز قدرات حل المشكلات، اعتمادا على تحليل البيانات من خلال خوارزميات رياضية ونماذج إحصائية، مما يمكنها من التطور مع مرور الوقت (Adib Bin Rashid, MD Ashfakul Karim Kausik, 2024, p. 2).

3.2 تقنيات الذكاء الاصطناعي:

تتنوع تقنيات الذكاء الاصطناعي وتتطور باستمرار، ولكن يمكن تسليط الضوء على بعض التقنيات الرئيسية التي تشكل جوهره والتي تساهم بدورها في تحسين الكفاءة والأداء في مختلف المجالات، وفتح آفاق جديدة للابتكار والإبداع وهي: التعلم الآلي والتعلم العميق ومعالجة اللغة الطبيعية والرؤية الحاسوبية.

1.3.2 التعلم الآلي (Machine Learning)

مجموعة فرعية من الذكاء الاصطناعي تعتمد على خوارزميات قادرة على استخلاص الأنماط والمعرفة من البيانات الضخمة، مما يمكنها من اتخاذ قرارات وتنبؤات ذكية دون تدخل بشري مباشر. تتعلم هذه الخوارزميات من خلال عمليات التدريب على البيانات، حيث تتحسن دقتها وكفاءتها تدريجيا مع كل معلومة جديدة. وهكذا، يفتح التعلم الآلي الباب أمام تطبيقات واسعة في مجالات متنوعة، من التعرف

على الصور وترجمة اللغات وصولاً إلى التوصيات الشخصية والقيادة الذاتية، مما يجعله أداة حيوية في العالم المتصل بالبيانات (Oluwaseun Isaac Odufisan et al, 2025, p. 1).

2.3.2 التعلم العميق (Deep Learning)

هو فرع متقدم من التعلم الآلي يهدف إلى محاكاة التفكير البشري عبر نماذج قائمة على الشبكات العصبية ذات الطبقات المتعددة، مما يمكنها من معالجة كميات هائلة من البيانات واستخلاص أنماط معقدة ودلالات خفية. ويتميز بقدرته على تحقيق هدفين رئيسيين: استخراج المعنى من المدخلات وتوليد مخرجات دقيقة وقيمة، وذلك بكفاءة وسرعة تفوق القدرة البشرية (Karan Aggarwal et al, 2022, p. 119).

3.3.2 معالجة اللغة الطبيعية (Natural Language Processing – NLP)

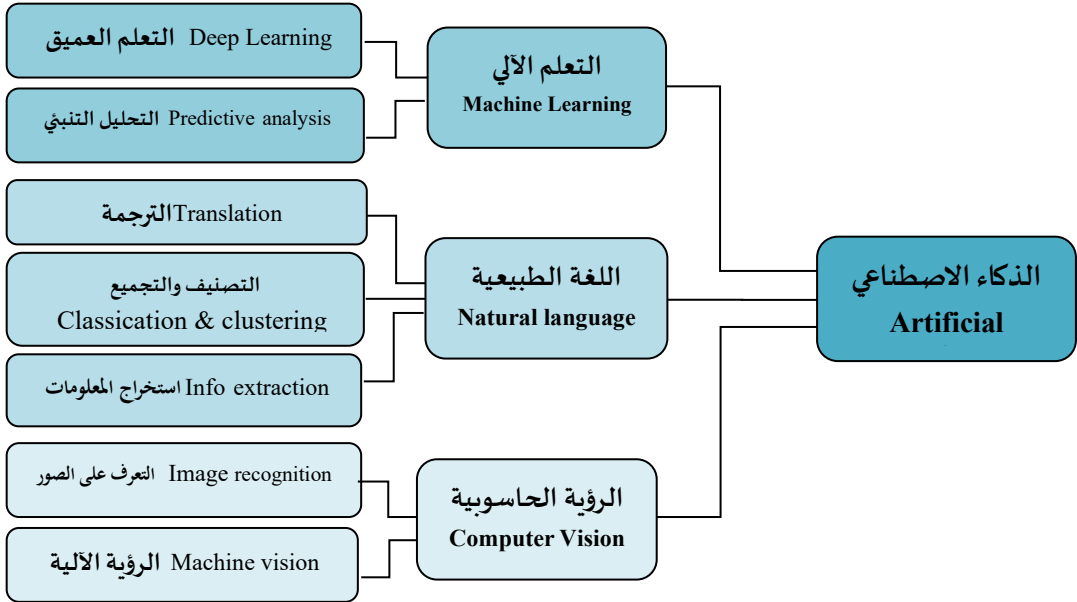
هي مجال متخصص داخل الذكاء الاصطناعي يركز على تمكين الآلات من فهم اللغة البشرية وتحليلها وإنتاجها. وتعتمد في أساسها على تقنيات التعلم الآلي والتعلم العميق لمعالجة البيانات اللغوية الضخمة واستخراج الأنماط والدلالات المعقدة، حيث تتجلى تطبيقاتها في مجالات حيوية مثل الترجمة الآلية، وتحليل المشاعر، وتلخيص النصوص، والرد الذكي، مما يجعلها عنصراً أساسياً في تعزيز التفاعل بين الإنسان والآلة (Yanhan Chen et al, 2024, p. 546).

4.3.2 الرؤية الحاسوبية (Computer Vision)

هي تقنية متطورة في مجال معالجة المعلومات تسعى إلى محاكاة قدرة الإنسان على الرؤية والفهم البصري، حيث تعمل على تفسير وتحليل الصور والفيديو باستخدام أسس نظرية كالتعلم العميق والتعرف على الأنماط وتتبع الأجسام. تتيح هذه العناصر للأجهزة معالجة المحتوى المرئي وتصنيفه بذكاء، وتظهر تطبيقاتها الواسعة في مجالات حيوية مثل التشخيص الطبي، العلوم الحياتية، البحث العلمي، والتطبيقات العسكرية، مما يحقق إنجازات نوعية ويفتح آفاقاً للابتكار (Yizhi Chen et al, 2024, p. 46).

استناداً إلى ما سبق، يمكن تلخيص تقنيات الذكاء الاصطناعي في الشكل الموالي:

الشكل 1: تقنيات الذكاء الاصطناعي



المصدر: إعداد الباحثين بالاعتماد على Péter Bagó, Cyber Security and Artificial Intelligence, Economy and Finance, Vol. 10. Iss. 2, 2023, p191

4.2 استخدامات الذكاء الاصطناعي بالقطاع المصرفي:

يمكن دمج الذكاء الاصطناعي في القطاع المصرفي بشكل فعال في العديد من المجالات، مثل تحسين تجربة العملاء من خلال التفاعل الذكي، وزيادة الكفاءة التشغيلية، وتعزيز استراتيجيات التسويق، وتحسين إدارة المخاطر، ومكافحة الاحتيال وتعزيز تدابير الأمن السيبراني.

1.4.2 التفاعل مع العملاء (Interact with customers)

إن التفاعل مع العملاء عامل حاسم لنجاح المؤسسات المالية، حيث أصبحوا يبحثون عن تجارب سلسلة وشخصية ودعم على مدار الساعة، وهو ما أتاحتها تقنيات الذكاء الاصطناعي كالمستشارين الآليين وروبوتات الدردشة. وتقدم المؤسسات هذه الخدمات بما يضمن الامتثال للتشريعات الأفقية والقطاعية*، كما توفر الاستشارة الآلية معلومات تدعم قدرة العملاء على اتخاذ قرارات استثمارية (Vishal Dineshkumar Soni, 2020, p. 4).

* التشريعات الأفقية هي قوانين عامة تنطبق على جميع القطاعات مثل قوانين حماية البيانات الشخصية، بينما التشريعات القطاعية خاصة بقطاع معين كقوانين تنظيم الخدمات المالية.

وتعد روبوتات الدردشة الآلية والمساعدون الافتراضيون أدوات مبتكرة تعتمد على الذكاء الاصطناعي لتعزيز التفاعل بين العملاء وأجهزة الكمبيوتر، وقد أصبحت بديلاً واسع الانتشار للتواصل التقليدي في فروع البنوك (Stephanie Ness et al, 2024, p. 1066)، حيث تحل محل موظفي الاستقبال، كما توفر تجارب رقمية مخصصة ومتطورة مصممة خصيصاً لتلبية الاحتياجات الفريدة للعملاء (Mohit Kumar et al, 2024, p. 98). فعلى سبيل المثال، أطلق أحد البنوك برنامج دردشة آلية لمساعدة العملاء في تلبية احتياجاتهم المصرفية اليومية، حيث يعمل كممثل افتراضي للبنك يعالج استفسارات العملاء ويوفر لهم حلولاً سريعة ومباشرة عبر واجهة الدردشة على المنصة الرقمية للبنك (Stephanie Ness et al, 2024, p. 1066).

2.4.2 كشف الاحتيال (Fraud Detection)

يساهم الذكاء الاصطناعي بشكل كبير في مكافحة الاحتيال المالي باختلاف أنواعه (الخارجي والداخلي)، حيث تعتمد الأنظمة الحديثة على تقنيات متقدمة كالتعلم التكراري وهندسة الخصائص لتحليل البيانات وكشف الأنماط غير الطبيعية، وتتكامل هذه الأنظمة مع أنظمة إدارة الاحتيال لمراقبة العمليات المشبوهة وحظرها، كما تعزز كفاءة إنشاء ملفات العملاء وتخفيض التكاليف التشغيلية. ويمتد دور الذكاء الاصطناعي ليشمل مكافحة غسل الأموال وتمويل الإرهاب، حيث يعد اكتشاف الشذوذ عاملاً أساسياً في منع الهجمات الإلكترونية والحد من المخاطر المالية (Vishal Dineshkumar Soni, 2020, p. 4).

3.4.2 تحسين إدارة المخاطر (Improve risk management)

يعد تقييم مخاطر الائتمان مجالاً آخر يتفوق فيه الذكاء الاصطناعي على النماذج التقليدية التي تعتمد على بيانات محدودة، إذ تستخدم خوارزمياته مجموعة أوسع من المصادر بما في ذلك وسائل التواصل الاجتماعي وسجلات الدفع والمؤشرات الاقتصادية، لتقييم أكثر شمولاً للجدارة الائتمانية. يعزز هذا النهج المتقدم دقة القياس ويساهم في بناء محفظة ائتمانية مرنة، مما يخفف معدلات التخلف عن السداد ويعزز الاستقرار المالي (Clark J. Lion et al, 2024, p. 90). كما يمكن أن يسمح للبنوك بإنشاء استراتيجيات إدارة مخاطر أكثر فعالية من خلال التنبؤ بالتقلبات والمخاطر في الأسواق المالية (Serkan Demirel and Murat Topcu, 2024, p. 2). علاوة على ذلك، يمكن للذكاء الاصطناعي تعزيز إدارة المخاطر التشغيلية من خلال التنبؤ بالمشاكل المحتملة وتمكين التدابير الاستباقية، مما يسمح للبنوك بمعالجة نقاط الضعف قبل تفاقمها (Clark J. Lion et al, 2024, p. 90).

4.4.2 تعزيز استراتيجيات التسويق (Enhance marketing strategies)

يعد التسويق المدعوم بالذكاء الاصطناعي أداة استراتيجية فاعلة تمنح البنوك ميزة تنافسية من خلال معالجة كميات هائلة من البيانات بذكاء وسرعة، مما يتيح تحليل سلوك العملاء بدقة والتنبؤ باحتياجاتهم المستقبلية. وتُحدث هذه القدرات تحولا جذريا في استراتيجيات التسويق المصرفي، خاصة في البيئات الاقتصادية الصعبة، حيث لا يقتصر اعتماد التسويق الذكي على جذب عملاء جدد والاحتفاظ بال الحاليين فقط، بل يعزز الإيرادات ويضمن النمو المستدام (Elnaz Mehran et al, 2024, p. 64).

5.4.2 تحسين الكفاءة التشغيلية (Improve operational efficiency)

تعتبر الكفاءة التشغيلية عنصرا حيويا في استراتيجيات البنوك لتأثيرها المباشر في الربحية ورضا العملاء، حيث يمكن لأي تحسين فيها أن يحدث فرقا كبيرا في الأرباح. ورغم فعالية الطرق التقليدية كإعادة هندسة العمليات، إلا أن تأثيرها محدود، بينما يقدم الذكاء الاصطناعي إمكانيات متطورة لتحسين الكفاءة عبر التحليلات المتقدمة والأتمتة وأنظمة دعم القرار، مما يساهم في أتمتة العمليات الروتينية وخفض التكاليف وتعزيز الإنتاجية (Idha Kristiana, 2024, p. 271).

6.4.2 الأمن السيبراني (Cybersecurity)

تتضح العلاقة المتينة بين الذكاء الاصطناعي والأمن السيبراني مع تطور التقنية، فبقدراته التحليلية الفائقة أصبح يرفع من كفاءة الأمن السيبراني عبر تمكين المؤسسات من اكتشاف الهجمات الإلكترونية والتصدي لها بذكاء وسرعة. وتزداد أهميته مع تنوع التهديدات وتعقيدها، حيث يقدم الذكاء الاصطناعي حلولاً مبتكرة تشمل تحليل الأنماط الأمنية واستخراج رؤى عميقة من البيانات وتطوير أنظمة أمنية ذاتية التعلم والتكيف، مما يجعل الدفاع الرقمي أكثر متانة ومرونة (Dendy Jonas et al, 2023, p. 83).

3. الأمن السيبراني بالقطاع المصرفي (Cybersecurity in the banking sector)

مع تزايد الاعتماد على الخدمات المصرفية الرقمية، تتضاعف المخاطر الأمنية حيث تصبح البيانات الحساسة عرضة لهجمات إلكترونية متطورة ومتزايدة التعقيد، مما يستلزم استراتيجيات متطورة لحمايتها من التهديدات السيبرانية وضمان استمرارية العمليات.

1.3 تعريف الأمن السيبراني

هو تطبيق يشمل التدابير الوقائية للدفاع عن الأنظمة والشبكات والبرامج من التهديدات الإلكترونية التي تهدف عادة إلى الحصول على إمكانية الوصول غير القانوني أو تعديل أو تدمير المعلومات الحساسة أو ابتزاز الأموال عبر عدوى برامج الفدية أو إلحاق الضرر بالأنشطة التجارية العادية

(Mahfujur Rahman Faraji et al, 2024, p. 4766). فهو يحمي الأجهزة والخدمات من المتسللين ومرسلي البريد العشوائي ومجرمي الانترنت الذين يريدون الوصول إلى البيانات الحساسة أو تغييرها أو حذفها أو تعطيل أنشطة المؤسسات (Takudzwa Fadziso et al, 2023, p. 1).

2.3 تطور مخاطر الأمن السيبراني

تتطور التهديدات السيبرانية باستمرار، حيث تظهر أجيال جديدة من هذه التهديدات بشكل دوري كنتيجة مباشرة للتطورات التكنولوجية. حتى الآن، تطورت خمسة أجيال من المخاطر السيبرانية، إلى جانب الحلول المصممة لمكافحتها، والتي يمكن تلخيصها في الجدول التالي:

الجدول 1: تطور أجيال المخاطر السيبرانية

الجيل	اسم الجيل	التهديدات الرئيسية	الحلول الأمنية الرئيسية
الأول	الفيروسات (Virus)	هجمات الفيروسات على أجهزة الكمبيوتر المستقلة	أنظمة مكافحة الفيروسات
الثاني	الشبكة (Network)	هجمات سيبرانية تنتقل عبر الإنترنت	جدران الحماية (Firewalls)
الثالث	التطبيقات (Applications)	استغلال الثغرات الأمنية في برامج التطبيقات	أنظمة منع التطفل IPS (Intrusion Prevention Systems)
الرابع	الحمولة (Payload)	برامج ضارة متطورة تتجاوز أنظمة الحماية التقليدية	أدوات مكافحة الروبوتات (Anti-Bot)، صناديق الحماية (Sandboxes)
الخامس	ميغا (Mega)	هجمات واسعة النطاق ومتعددة الاتجاهات	حلول أمنية متطورة من الجيل الخامس

المصدر: إعداد الباحثين بالاعتماد على (Takudzwa Fadziso et al (2023), Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat, Digitalization & Sustainability Review, Vol 3, N° 1, p4

3.3 مخاطر الأمن السيبراني بالقطاع المصرفي

يعد القطاع المصرفي هدفا رئيسيا للهجمات السيبرانية نظرا لكميات المعلومات الحساسة التي يتعامل معها، وفقا لتقرير الاستقرار المالي العالمي الصادر عن صندوق النقد الدولي في 2024. حيث تشير الإحصائيات إلى أن ما يقرب من 20% من الهجمات السيبرانية تستهدف المؤسسات المالية، وتأتي البنوك في مقدمة القطاعات الأكثر تضرراً حسب ما يوضحه الشكل التالي:

الشكل 2: الحوادث السيبرانية وخسائر القطاع المالي خلال 20 سنة

الحوادث السيبرانية في القطاع المالي (العدد، 2004-2023)

خسائر القطاع المالي (العدد، 2004-2023)



المصدر: إعداد الباحثين بالاعتماد على Mahfujur Rahman Faraji, Examining the Role of

Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions, International Journal of Religion, Vol5, N° 10, 2024

يتضح من الشكل أعلاه أن القطاع المالي قد عانى من أكثر من 20.000 هجوم إلكتروني مما تسبب في خسائر بلغت 12 مليار دولار على مدى عشرين سنة، تتضمن هذه الإحصائيات القطاع المصرفي الذي تعرض وحده لما يقارب 10.000 هجوم إلكتروني بخسائر قدرت بـ 03 مليار دولار.

ولفهم طبيعة التهديدات السيبرانية التي تواجه القطاع المصرفي، سيتم التطرق إلى أنواعها التي تتلخص في التصيد الاحتيالي والهندسة الاجتماعية، البرمجيات الخبيثة وبرامج الفدية، هجمات الحرمان من الخدمة الموزعة، حقن SQL والتهديدات المستمرة المتقدمة.

1.3.3 التصيد الاحتيالي والهندسة الاجتماعية (Phishing and Social Engineering)

تعد هجمات التصيد الاحتيالي والهندسة الاجتماعية من أكثر التهديدات السيبرانية انتشارا في القطاع المصرفي، حيث تستغل نقاط الضعف البشرية للوصول غير المصرح به إلى المعلومات الحساسة. وقد ازدادت خطورة هذه الهجمات بسبب الرقمنة الواسعة في القطاع المالي، كما أن تعقيدها المتزايد يجعل الدفاع ضدها أمرا صعبا بشكل خاص (Suri babu Nuthalapati, 2023, p. 361).

في عام 2025، استهدف 88.5% من هجمات التصيد الاحتيالي بيانات تسجيل الدخول لحسابات البنوك والخدمات المالية، بينما شكلت 9.5% بيانات شخصية و2% تفاصيل بطاقات ائتمانية، وفقا لتحليل كاسبرسكي للفترة التي امتدت من شهر جانفي إلى غاية شهر سبتمبر 2025. كما سجلت 6.7 مليون محاولة تصيد تستهدف التجارة الإلكترونية وأنظمة الدفع (kaspersky, 2026).

2.3.3 البرمجيات الخبيثة وبرامج الفدية (Malware and Ransomware)

تشكل البرمجيات الخبيثة، بما في ذلك برامج الفدية، تهديدا كبيرا للخدمات المصرفية الرقمية، حيث يمكنها تعطيل العمليات وسرقة البيانات الحساسة والمطالبة بمدفوعات الفدية. وقد شهد القطاع المصرفي زيادة كبيرة في هذه الهجمات، مما يستدعي الحاجة الملحة إلى تدابير قوية للأمن السيبراني (Suri babu Nuthalapati, 2023, p. 361).

لقد تجاوز إجمالي هجمات البرمجيات الخبيثة البنكية عالميا 1.338 مليون هجمة في عام 2025، فيما تأثرت 12.8% من المؤسسات المالية من نوع B2B بهجمات برامج الفدية خلال العام نفسه، كما تم تسجيل زيادة بنسبة 35.7% في عدد المستخدمين الماليين الذين واجهوا برامج الفدية مقارنة بالسابق في حين تعرض 15.81% من مستخدمي القطاع المالي لتهديدات محلية (newagebd, 2025).

3.3.3 هجمات الحرمان من الخدمة الموزعة (Distributed Denial of Service attacks)

تهدف هجمات الحرمان من الخدمة الموزعة (DDoS) إلى إغراق الأنظمة المصرفية بحركة مرور مكثفة، مما يجعلها غير متاحة للمستخدمين الشرعيين. يمكن أن تسبب هذه الهجمات أضرارا مالية وتؤثر سلبا على سمعة البنك (Suri babu Nuthalapati, 2023, p. 361).

شهدت هجمات DDoS ارتفاعا عالميا بنسبة 82% في الربع الثالث من عام 2025 مقارنة بالفترة نفسها من العام السابق. واستحوذ القطاع المالي على 22% من إجمالي هذه الهجمات عالميا، مسجلا زيادة قدرها 91% عن العام السابق. وتستخدم 63% من الهجمات الموجهة للقطاع المالي متجهات هجوم متعددة، فيما تجمع 37% منها بين ثلاثة أنواع أو أكثر في وقت واحد (uktechnews, 2026).

4.3.3 حقن SQL (SQL INJECTION)

في هجمات حقن SQL*، يتم إدخال تعليمات برمجية ضارة في قواعد البيانات لسرقة بيانات الاعتماد مثل أسماء المستخدمين وكلمات المرور. يمكن استخدام هذه البيانات للوصول غير المصرح به إلى حسابات العملاء (Olha Shulha et al, 2022, p. 6).

خلال عام 2025، تم رصد 10 ثغرات أمنية حرجة في نظام PHPGurukul Bank Locker Management System 1.0**، وتصنف جميعها ضمن ثغرات حقن SQL، بمتوسط درجة خطورة بلغ 9.8 من أصل 10 (stack.watch, 2025).

5.3.3 التهديدات المستمرة المتقدمة (Advanced Persistent Threats)

تمثل التهديدات المستمرة المتقدمة (APTs) شكلا خطيرا ومعقدا من الهجمات الإلكترونية، حيث تقوم جهات خبيثة عالية التنظيم باختراق شبكات المؤسسات المالية والبقاء خفية لفترات طويلة لسرقة الأصول المالية الحساسة أو بيانات العملاء. وتتميز هذه الهجمات بدعم مالي وتقني كبير ودافع استراتيجي قوي، مما يجعلها من أخطر التحديات الأمنية التي تواجه القطاع المصرفي، خاصة مع تفاقم المخاطر بوجود تهديدات داخلية محتملة من موظفين أو شركاء موثوقين، مما قد يؤدي إلى وصول غير مصرح به وانتهاكات بيانات وخسائر مالية جسيمة (Samuel Onimisi Dawodu et al, 2023, p. 239).

في إحدى الحالات الشهيرة، استطاعت عصابة سرقة ما يقارب مليار دولار على مدار عامين من بنوك عالمية متعددة، وذلك باستخدام برنامج ضار يُدعى "Carbanak" لاستهداف موظفي البنوك عبر رسائل البريد الإلكتروني المخترقة. وبعد إصابة أجهزة الحواسيب، تمكنوا من محاكاة نشاط الموظفين المصرح لهم، ونقل الأموال إلى حساباتهم الخاصة، والتحكم في أجهزة الصراف الآلي لتوزيع النقود تلقائيا في أوقات محددة، بالإضافة إلى استغلال أنظمة الدفع الإلكترونية لسحب الأموال (kaspersky, 2024).

* SQL هي اختصار لـ Structured Query Language، وتعني لغة الاستعلام الهيكلية. وهي لغة برمجية قياسية تُستخدم لإدارة قواعد البيانات العلائقية (Relational Databases) والتفاعل معها. تُستخدم SQL لإنشاء قواعد البيانات، تعديلها، استخراج البيانات منها، وإجراء عمليات أخرى مثل إضافة أو حذف أو تحديث السجلات.

** PHPGurukul Bank Locker Management System (BLMS) هو نظام صُمم لإدارة الخزائن البنكية التي يحتفظ فيها العملاء بالأشياء الثمينة، حيث يتم حفظ جميع تفاصيل الخزائن في قاعدة البيانات.

4. الذكاء الاصطناعي لتعزيز الأمن السيبراني بالقطاع المصرفي

إن الكشف عن التهديدات الإلكترونية والتخفيف من حدتها أمر حاسم لضمان أمن المعاملات المالية في القطاع المصرفي، وتواجه البنوك تحديات تنظيمية معقدة جراء تعدد إرشادات الهيئات المحلية والدولية لإدارة المخاطر السيبرانية، غير أن سرعة تطور التهديدات تجعل الامتثال تحدياً دائماً. ولجابهة ذلك، تستثمر البنوك في تدابير تقنية وتنظيمية في مقدمتها توظيف تقنيات الذكاء الاصطناعي لتعزيز قدراتها الدفاعية وضمان التوافق مع المعايير الأمنية المتطورة (Suri babu Nuthalapati, 2023, p. 361)

1.4 دور الذكاء الاصطناعي في الأمن السيبراني

أصبح التحالف بين الذكاء الاصطناعي والأمن السيبراني ضرورة استراتيجية في مواجهة التهديدات الإلكترونية، ومع تنامي حجم وتعقيد البيانات الأمنية، برزت الحاجة الملحة إلى تحليلها بدقة وفورية، وهو ما يلبيه الذكاء الاصطناعي عبر أدواته كالتعلم الآلي والتحليل العميق، حيث يمكن الأنظمة من الكشف الاستباقي عن التهديدات الناشئة قبل تحولها إلى اختراقات فعلية (Dendy Jonas et al, 2023, p. 83).

1.1.4 الكشف عن التهديدات (Threat detection)

يسهل الذكاء الاصطناعي تنفيذ الكشف المتقدم عن التهديدات السيبرانية وتحديد حجمها في الوقت الفعلي، حيث تمكن هذه الاستراتيجية الاستباقية من التعرف في الوقت المناسب على المخاطر الناشئة والمعقدة (Mahfujur Rahman Faraji et al, 2024, p. 4769).

تعد هجمات التصيد الاحتيالي من أبرز التهديدات انتشاراً التي يستخدمها مجرمو الإنترنت للوصول غير المصرح به إلى البيانات، وقد ساهم تكامل الذكاء الاصطناعي مع الأمن السيبراني في رفع كفاءة اكتشاف هذه الهجمات والتعامل معها، فمن خلال التحليل الذكي تتمكن الأنظمة المدعومة بالذكاء الاصطناعي من تمييز الرسائل الاحتيالية بدقة حتى مع محاولات التموه المتقدمة، مما يساعد المؤسسات على تجنب الخداع ويقلل من مخاطر الاختراقات باهظة التكلفة (Dendy Jonas et al, 2023, p. 83).

2.1.4 الاستجابة الآلية (Automated Incident)

لقد أحدث دمج الذكاء الاصطناعي مع الأمن السيبراني تحولاً جذرياً في مواجهة التهديدات، حيث انتقلت الحماية من النمط التفاعلي بعد الهجوم إلى النهج الاستباقي القائم على التوقع والتحليل المسبق. فعند رصد أي مؤشر خطر، يمكن للنظام تنفيذ رد فعل آلي فوري كتحديد التهديد قبل تفاقم

الأضرار. هذه السرعة والدقة تمنح فرق الأمن السيبراني القدرة على احتواء التهديدات بفعالية، مما يخفف احتمالية نجاح الهجمات ويقلل حجم الخسائر المحتملة (Dendy Jonas et al, 2023, p. 83).

3.1.4 تحليل السلوك (Behavior Analysis)

يُظهر الذكاء الاصطناعي كفاءة استثنائية في التحليلات السلوكية، والتي تشمل فحص أنماط سلوك المستخدم ونشاط الشبكة. يمكن لأنظمة الذكاء الاصطناعي تحديد التهديدات الأمنية من خلال مقارنة النشاط الحالي بخط الأساس القياسي واكتشاف أي إجراء أمني غير طبيعي قد يتم تجاهله (Mahfujur Rahman Faraji et al, 2024, p. 4769).

يعتبر التحليل السلوكي الأساس في ممارسات الأمن السيبراني المعاصرة، فهو يمكن أنظمة الأمان مراقبة وتحديد الانحرافات عن الأنماط الراسخة بشكل مستمر، وتحديد التهديدات المحتملة بشكل استباقي قبل أن تتجسد في شكل خروقات أمنية (Dendy Jonas et al, 2023, p. 83).

2.4 تحديات استخدام الذكاء الاصطناعي في الأمن السيبراني

يمثل استخدام الذكاء الاصطناعي في مجال الأمن السيبراني تطوراً واعداً، ولكنه لا يزال يواجه العديد من التحديات التي يجب معالجتها وتجاوزها لتحقيق الأهداف المرجوة من هذه التقنية، أهمها: (Ravi Sen et al, 2022, pp. 189-191)

1.2.4 بيانات التدريب: تعتبر جودة بيانات التدريب المستخدمة في تطوير أنظمة الذكاء الاصطناعي حاسمة لتحقيق الفعالية المطلوبة. ومع ذلك، يواجه توفير بيانات تدريب مناسبة صعوبات، مثل عدم التوازن في توزيع البيانات بين الفئات المختلفة، والقيود المفروضة على مشاركة بعض أنواع البيانات، بالإضافة إلى التكلفة العالية لعملية وضع العلامات على البيانات وتصنيفها.

2.2.4 التحديث المستمر: تتطور البرامج الضارة باستمرار، مما يستدعي تحديث نماذج الذكاء الاصطناعي بشكل دوري لمواكبة هذه التغيرات. يعرف ذلك بمشكلة "انحراف المفهوم"، حيث يصبح النموذج قديماً وغير قادر على التعرف على التهديدات الجديدة إذا لم يتم تحديثه بانتظام.

3.2.4 التعلم الآلي العدائي: يمكن للمخترقين خداع نماذج الذكاء الاصطناعي من خلال "تسميم" بيانات التدريب بمعلومات مضللة، أو استخدام "مدخلات معادية" مصممة خصيصاً لخداع النموذج.

4.2.4 استخدام الذكاء الاصطناعي لأغراض ضارة: يمكن للمخترقين استخدام الذكاء الاصطناعي لتطوير فيروسات وبرامج ضارة أكثر ذكاءً وقدرة على التكيف، مما يجعل مهمة الحماية أكثر صعوبة.

5.2.4 صعوبة الفهم: تتسم بعض أنظمة الذكاء الاصطناعي بالتعقيد الشديد، مما يجعل من الصعب فهم كيفية عملها، ويصعب بالتالي تقييم فعاليتها وإصلاحها عند الحاجة.

3.4 أهم الإحصائيات حول مساهمة الذكاء الاصطناعي في الوقاية من التهديدات الأمن السيبراني

في عصر يتسم بهجمات سيبرانية متكررة وضارة بشكل متزايد، يمثل الذكاء الاصطناعي سلاحاً ذا حدين في مجال الأمن السيبراني. فبالإضافة إلى المخاوف والتحديات الأمنية التي يطرحها استخدامه، يوفر أيضاً حلولاً مبتكرة وفعالة للدفاع ضد التهديدات وهجمات الجهات المعادية، ونتيجة لذلك، استخدام هذه التقنية في تزايد مستمر وهو ما تؤكدته الإحصائيات التالية:

1.3.4 نمو سوق الذكاء الاصطناعي في الأمن السيبراني

يشهد سوق الذكاء الاصطناعي في الأمن السيبراني نمواً متسارعاً بشكل غير مسبوق، فوفقاً لتقرير صادر عن Statistics MRC، بلغ حجم السوق العالمي 31.53 مليار دولار في عام 2025، مع توقعات بارتفاعه إلى 145.39 مليار دولار بحلول عام 2032، بمعدل نمو سنوي مركب يبلغ 24.4% (marketresearch, 2025).

2.3.4 اعتماد الذكاء الاصطناعي وتأثيره

وفقاً لاستطلاع ISC2 الذي شمل 436 متخصصاً في الأمن السيبراني على مستوى العالم، فإن 30% من فرق الأمن السيبراني قد دججت بالفعل أدوات الذكاء الاصطناعي في عملياتها، بينما يوجد 42% إضافية في مرحلة الاستكشاف والاختبار، ومن بين المستخدمين الحاليين، أفاد 70% بأن للذكاء الاصطناعي تأثيراً إيجابياً على الفعالية الشاملة لفريقهم. ويُسجل القطاع المالي والمصرفي نسبة اعتماد تبلغ 21% مقارنة بقطاعات أخرى (isc2, 2025).

3.3.4 الذكاء الاصطناعي وكشف التهديدات والاستجابة

كشفت مايكروسوفت في مؤتمر Ignite 2025 عن نتائج مذهلة لأدواتها الأمنية المدعومة بالذكاء الاصطناعي، حيث أظهر وكيل تصنيف التصيد الاحتمالي (Phishing Triage Agent) قدرة على تحليل رسائل التصيد المحتملة بشكل أسرع 6.5 مرات في الدقيقة، محققاً تحسناً في الكفاءة بلغ 550%. كما سجل الوكيل تحسناً في دقة الكشف بنسبة تصل إلى 77% (computerweekly, 2025).

4.3.4 الذكاء الاصطناعي كسلاح ذو حدين

تشير الإحصائيات إلى تنامي دور الذكاء الاصطناعي في الصراع السيبراني من الجانبين، حيث تعرضت 87% من المؤسسات لهجمات مدعومة بالذكاء الاصطناعي خلال عام 2025، شملت تقنيات الديب فيك (Deepfakes) وحملات التصيد المولدة بالذكاء الاصطناعي. وفي المقابل، تستخدم 78% من المؤسسات الذكاء الاصطناعي بشكل دفاعي لمواجهة هذه التهديدات (neuraking, 2025).

5.3.4 توفير التكاليف باستخدام الذكاء الاصطناعي

حقق الذكاء الاصطناعي توفيراً بـ 94 مليون دولار في تكاليف الاستجابة للهجمات للشركات الكبرى في 2025، مع تقليل تكلفة الحادثة الواحدة بنسبة 28% (من 4.88 مليون دولار في 2024 إلى 3.52 مليون دولار)، وأتمتة 72% من المهام الأمنية الروتينية (kaspersky, 2025). وفيما يلي، جدول يتضمن أحدث الإحصائيات على الصعيد العالمي، التي تبرز تأثير استخدام الذكاء الاصطناعي على الأمن السيبراني بالقطاع المصرفي:

الجدول 2: تأثير استخدام الذكاء الاصطناعي على الأمن السيبراني المصرفي

المقياس	قبل استخدام الذكاء الاصطناعي (2020-2022)	بعد استخدام الذكاء الاصطناعي (2024-2025)	نسبة التحسن
متوسط وقت اكتشاف الاختراق	200 ساعة (08 أيام)	22 ساعة	89%
متوسط وقت احتواء الاختراق	70 ساعة	28 ساعة	60%
متوسط تكلفة الاختراق (مليون دولار)	4.45	3.69 (مع AI مكثف) 1.88	29% 61%
دقة كشف هجمات التصيد الاحتيالي	75%	96%	28%
معدل كشف برامج الفدية بالقطاع المالي	64%	92%	44%

المصدر: إعداد الباحثين بالاعتماد على <https://www.kaspersky.com>

<https://www.ibm.com>

يُظهر الجدول أعلاه تحولا كبيرا في كفاءة الدفاعات الرقمية، حيث أحدث الذكاء الاصطناعي طفرة ملموسة في تقليص زمن اكتشاف التهديدات بنسبة 89%، محولاً مدة الرصد من أيام إلى ساعات معدودة. ولم يقتصر هذا التأثير على السرعة الزمنية فحسب، بل امتد ليشمل الجانب الاقتصادي عبر خفض تكاليف الاختراقات بنسبة تصل إلى 61% عند الاستخدام المكثف للتقنية، مع رفع دقة كشف هجمات التصيد وبرامج الفدية إلى مستويات قياسية تتجاوز 92% وتؤكد هذه النسب أن الذكاء

الاصطناعي بات المحرك الأساسي لتقليل الخسائر السنوية العالمية وتعزيز مرونة القطاعات الحساسة، خاصة القطاع المالي والمصرفي، في مواجهة الهجمات السيبرانية المتطورة.

5. الخلاصة:

يؤدي الذكاء الاصطناعي دورا مهما في تعزيز الأمن السيبراني للقطاع المصرفي، حيث يوفر تقنيات متقدمة لرصد التهديدات والاستجابة السريعة لها بكفاءة عالية. ورغم التحديات التي تواجهه، يبقى الاستثمار في الذكاء الاصطناعي وتطوير استراتيجيات شاملة هو السبيل لضمان أمن مالي رقمي آمن وموثوق بها.

تم التوصل من خلال هذا البحث إلى مجموعة من النتائج يمكن ذكرها كالتالي:

- تتزايد التهديدات السيبرانية بالقطاع المصرفي باستمرار وتتطور جنبا إلى جنب مع التطور التكنولوجي؛
- قُدر حجم سوق الذكاء الاصطناعي العالمي في الأمن السيبراني بأزيد من 31 مليار دولار أمريكي في عام 2025، ومن المتوقع أن يشهد نموا كبيرا في السنوات القادمة؛
- تُظهر الإحصائيات أن المؤسسات التي تعتمد على الذكاء الاصطناعي في مجال الأمن السيبراني تتمكن من تقليل تكاليف الخروقات الأمنية والاستجابة لها بشكل أسرع؛
- يواجه استخدام الذكاء الاصطناعي في الأمن السيبراني بعض التحديات، مثل الحاجة إلى بيانات تدريب عالية الجودة والتحديث المستمر للنماذج لمواكبة التهديدات المتطورة وفي مقدمتها استخدام الذكاء الاصطناعي من قبل المخترقين أنفسهم.
- من خلال عرض نتائج البحث يمكن تقديم الاقتراحات التالية:
- تخصيص ميزانية هامة لزيادة الاستثمار في تطوير وتطبيق تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني من خلال الاستثمار في البنية التحتية اللازمة؛
- التعاون المستمر بين البنوك والمؤسسات المالية لتبادل المعلومات حول التهديدات السيبرانية وأفضل الممارسات في مجال الأمن السيبراني، مع إبرام اتفاقيات مع المؤسسات البحثية لتطوير حلول مبتكرة لمواجهة التحديات الأمنية؛
- تدريب إطارات وموظفي القطاع المصرفي على استخدام تقنيات الذكاء الاصطناعي في مجال الأمن السيبراني، مع توفير برامج تدريبية متخصصة وتنظيم ورشات عمل ومؤتمرات؛

- مواصلة البحث والتطوير في مجال الذكاء الاصطناعي والأمن السيبراني، والاستعداد لتبني تقنيات جديدة استعدادا للتكيف مع التهديدات المستقبلية.

5. قائمة المراجع:

● المقالات:

1. Adib Bin Rashid, MD Ashfakul Karim Kausik. AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances* (7), 2024
2. Clark j. Lion et al. Risk control and management in banking sector: investigating the work of artificial intelligence in mitigating risks. *International journal of advancement in education, management, science and technology* , 7 (1), 2024.
3. Dendy Jonas et al. Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity. *International Transactions on Education Technology (ITEE)* , 2 (1), 2023.
4. Elnaz Mehran et al. Intelligent Marketing Model with a Focus on Artificial Intelligence in the Banking Industry. *Business, Marketing, and Finance Open* , 1 (6), 2024.
5. Idha Kristiana. Review of Improving Banking Operational Efficiency through AI and ML: Strategy, Implementation and Impact. *Jurnal Komunikasi Sains dan Teknologi* , 3 (1), 2024.
6. Karan Aggarwal et al. Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning. *Iraqi Journal for Computer Science and Mathematics* , 3 (1), 2022.
7. Mahfujur Rahman Faraji et al .Examining the Role of Artificial Intelligence in Cyber Security (CS): A Systematic Review for Preventing Prospective Solutions in Financial Transactions .*International Journal of Religion* 5 (10), 2024.
8. MD Ashfakul Karim Kausik Adib Bin Rashid .AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications .*Hybrid Advances*(7) , 2024.
9. MD Ashfakul Karim Kausik Adib Bin Rashid .AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications .*Hybrid Advances*(7) ,2024 .
10. Mohit Kumar et al. The Impact Of Artificial Intelligence On The Banking Sector. *Afr. J. Biomed. Res* , 27 (5), 2024.
11. Olha Shulha et al. Banking Information Resource Cybersecurity System Modeling, , 8, 80, , p 6. *J. Open Innov. Technol. Mark. Complex* , 8 (80), 2022.
12. Oluwaseun Isaac Odufisan et al. Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. *Journal of Economic Criminology* (7), 2025.

13. Ravi Sen et al. Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics, Communications of the Association for Information Systems, Volume 51, 2022.
14. Samuel Onimisi Dawodu et al. Cybersecurity risk assessment in banking: methodologies and best practices. *Computer Science & IT Research Journal* , 4 (3), 2023.
15. Serkan Demirel and Murat Topcu. The Impact of Artificial Intelligence Applications on Digital Banking in Turkish Banking Industry. *Wiley Advances in Human-Computer Interaction* , 2024.
16. Stephanie Ness et al. Banking 4.0: The Impact of Artificial Intelligence on the Banking Sector and its Transformation of Modern Banks. *International Journal of Innovative Science and Research Technology* , 9 (2), 2024.
17. Suri babu Nuthalapati. AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. *Educational Administration: Theory and Practice* , 29 (1), 2023.
18. Takudzwa Fadziso et al. Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. *Digitalization & Sustainability Review*, 3(1), 2023
19. Vishal Dineshkumar Soni. Role of artificial intelligence in combating cyber threats in banking, *International Engineering Journal For Research & Development*. 4 (1), 2020.
20. Yanhan Chen et al. Artificial Intelligence Methods in Natural Language Processing: A Comprehensive Review. *Highlights in Science, Engineering and Technology* , 85, 2024.
21. Yizhi Chen et al. Computer Vision and Deep Learning Transforming Image Recognition and Beyond. *International Journal of Computer Science and Information Technology*, 2 (1), 2024.

• مواقع الانترنت:

1. *bottomline*. (2026). Retrieved 03 18, 2026, from *bottomline*: <https://www.bottomline.com/resources/new-fraud-battlefield>
2. *computerweekly*. (2025). Retrieved 03 22, 2026, from *computerweekly*: https://www.computerweekly.com/news/366634531/Microsoft-unveils-AI-agents-to-automate-security-operations?utm_source=whattheai.beehiiv.com&utm_medium=referral&utm_campaign=gemini-3-is-here
3. *deepstrike*. (2025). *deepstrike*. Retrieved 01 03, 2025, from <https://deepstrike.io/blog/vulnerability-statistics-2025>
4. *ibm* (2025). Retrieved 03 18, 2026, from *ibm*: <https://www.ibm.com/reports/data-breach>
5. *isc2*. (2025). Retrieved 03 21, 2026, from *isc2*: <https://www.isc2.org/insights/2025/07/isc2-research-cybersecurity-teams-cautious-on-ai-adoption?queryID=5766ca7db6d4b9b9f7732373d922dde4>

6. *kaspersky*. (2024). Retrieved 02 08, 2025, from kaspersky: <https://me.kaspersky.com/resource-center/threats/top-7-cyberthreats>
7. *kaspersky*. (2025). Retrieved 03 18, 2026, from kaspersky: <https://me.kaspersky.com/about/press-releases/kaspersky-shares-top-trends-in-the-financial-sector>
8. *kaspersky*. (2026). Récupéré sur kaspersky: <https://me.kaspersky.com/about/press-releases/kaspersky-885-of-phishing-attacks-focus-on-stealing-account-credentials>
9. *kaspersky*. (2026). Retrieved 03 18, 2026, from kaspersky: <https://me.kaspersky.com/about/press-releases/kaspersky-885-of-phishing-attacks-focus-on-stealing-account-credentials>
10. *kaspersky*. <https://me.kaspersky.com/resource-center/definitions/sql-injection> .
11. *kaspersky*. (2024). <https://me.kaspersky.com/resource-center/definitions/sql-injection>.
12. *marketresearch*. (2025). Retrieved 03 21, 2026, from marketresearch: <https://www.marketresearch.com/Statistics-Market-Research-Consulting-v4058/AI-Powered-Cybersecurity-Forecasts-Global-43010462/>
13. *neuraking*. (2025). Retrieved 03 22, 2026, from neuraking: <https://neuraking.com/ar/36973/limpact-des-agents-ia-autonomes-dans-la-cybersecurite-en-2025/>
14. *newagebd*. (2025). Retrieved 03 18, 2026, from newagebd: <https://www.newagebd.net/print/post/282437>
15. *stack.watch*. (2025, 03 24). Retrieved 03 18, 2026, from stack.watch: <https://stack.watch/product/anujkumar/bank-locker-management-system>
16. *TechMagic*. (2025). Retrieved 02 07, 2025, from cybersecurity-in-banking: <https://www.techmagic.co/blog/cybersecurity-in-banking>
17. *uktechnews*. (2026). Retrieved 03 18, 2026, from uktechnews: <https://uktechnews.co.uk/2026/01/29/ddos-attacks-surge-82-worldwide-as-hackers-shift-toward-financial-motives-from-hacktivism/>