مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام تطبيق الأمن السيبراني: بنك Danske الدنماركي أنموذجا

AI's contribution to detecting fraud in the banking sector using cybersecurity application- The case of "Danske" Danish Bank Experience

بن علي سمية*

جامعة باجي مختار–عنابة، الجزائر

benali.soumaya.dz@gmail.com

تاريخ الاستلام: 2023/08/20 تاريخ القبول: 2023/11/01 تاريخ النشر: 2023/12/31

ملخص:

تهدف هذه الدراسة الى إبراز مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام تطبيق الأمن السيبراني، على افتراض أن الأساليب المالية الرقمية كتطبيق الأمن السيبراني يساهم في توسيع نطاق الكشف عن الاحتيالات في المؤسسات المصرفية من خلال تحليل كميات هائلة من البيانات في الوقت المناسب، مما يمكّن المؤسسات المالية من تحديد الأنماط والاتجاهات التي سيكون من المستحيل اكتشافها يدويًا. ولتحقيق الهدف من الدراسة تم الاعتماد على المنهج الوصفي التحليلي وكذا دراسة حالة لتجربة بنك Danske الدنماركي.

توصلت الدراسة إلى أن تطبيق كشف الاحتيال والأمن السيبراني المعتمد على الذكاء الاصطناعي في بنك Danske، ساهم في الكشف عما نسبته 50 % من الاحتيال الفعلي واضعا بذلك حجر الأساس من أجل المساعدة على رفع درجة الأمان المالي الرقمي.

الكلمات المفتاحية: ذكاء اصطناعي، كشف الاحتيال، أمن سيبراني، بنك Danske.

تصنيف JEL : G21, G23 , G24

---

* **المؤلف المرسل**

Abstract:

This study aims to highlight the contribution of AI to the detection of fraud in the banking sector using the cybersecurity application, assuming that digital financial methods such as the cybersecurity application contribute to wider detection of fraud in banking institutions by analyzing vast amounts of data in due time. This enables financial institutions to identify patterns and trends that will be impossible to detect manually. To achieve the objective of the study, the analytical descriptive method as well as a case study of Danske's experience were relied upon.

The study found that Danske Bank's AI-based fraud detection and cybersecurity application contributed to detecting 50% of actual fraud, laying the foundation to help raise digital financial security.

Keywords: Artificial Intelligence, Fraud Detection, Cyber Security, Danske Bank.

JEL Classification Codes: G21, G23 , G24

مقدمة:

لقد جلبت الثورة الصناعية الرابعة تغيرات في القطاع المصرفي التقليدي المبني على الورق والتوزيع المادي للنقد، فأصبحت البنوك والمؤسسات المالية تعتمد على الطرق الرقمية، والتي كانت قيد الاستخدام لسنوات من خلال التطبيق المباشر للذكاء الاصطناعي، والذي يعتبر واحدا من تطبيقات التكنولوجيا المالية، كما يساعد على تحسين الوصول إلى الأشخاص الذين كانت تخدمهم المؤسسات المالية الرسمية السابقة. فقد تسارع استخدام الذكاء الاصطناعي في الصناعة المصرفية في السنوات الأخيرة، حيث تُسخر المؤسسات المالية قوة التحليلات المتقدمة وخوارزميات التعلم الآلي لتعزيز وتحسين تجارب العملاء وتخفيف المخاطر. ويشير الذكاء الاصطناعي إلى استخدام الآلات لأداء المهام التي تتطلب عادةً ذكاءً بشريًا، مثل التعلم وحل المشكلات .

كان أحد أهم تأثيرات تطبيقات الذكاء الاصطناعي في الصناعة المصرفية هو القدرة على تقديم تجارب أكثر تخصيصًا وملاءمة للعملاء من خلال روبوتات الدردشة الافتراضية التي تعمل بالذكاء الاصطناعي، والمساعدة في إيجاد حلول فعالة للكشف عن الاحتيال والأمن السيبراني في النظام المصرفي، من خلال تحليل كميات هائلة من البيانات في الوقت الفعلي، مما يمكّن المؤسسات المالية من تحديد الأنماط والاتجاهات التي سيكون من المستحيل اكتشافها يدويًا. كل هذا أدى إلى تحسين الكفاءة في الصناعة المصرفية بالإضافة إلى تحرير الموظفين من ساعات العمل الزائدة للتركيز على مهام أخرى أكثر تعقيدًا.

- **إشكالية الدراسة:** "كيف ساهمت تطبيقات الأمن السيبراني في الكشف عن الاحتيال في المؤسسات المصرفية على غرار تجربة بنك Danske الدنماركي ؟"

- **فرضية الدراسة:** ساهمت الأساليب المالية الرقمية كتطبيقات الأمن السيبراني في الكشف عن الاحتيالات في المؤسسات المصرفية من خلال تحليل كميات هائلة من البيانات في الوقت المناسب، مما يمكّن المؤسسات المصرفية من تحديد الأنماط والاتجاهات التي سيكون من المستحيل اكتشافها يدويًا.

- **أهداف الدراسة:** يمكن إيجاز أهداف الدراسة في العناصر الأساسية التالية:

– التعرف على ماهية الذكاء الاصطناعي من حيث المفهوم، والخصائص، والأنواع، وأهم تطبيقاته، والأهمية والمزايا التي يوفرها؛

– التقصي عن المساهمة التي قدمها الذكاء الاصطناعي باستخدام تطبيقات الأمن السيبراني في الكشف عن الاحتيال في القطاع المصرفي من خلال عرض وتحليل لتجربة بنك Danske الدنماركي؛

– الوصول إلى أهم العوامل التي ساهمت في نجاح الكشف عن الاحتيال والأمن السيبراني المعتمد على الذكاء الاصطناعي في بنك Danske الدنماركي.

- **منهجية الدراسة:** تماشيا مع طبيعة الدراسة وأهدافها تم الاعتماد على المنهج الوصفي التحليلي، وذلك لوصف المفاهيم المتعلقة بالذكاء الاصطناعي وتطبيقات الأمن السيبراني، في حين تم الاعتماد على منهج دراسة حالة للجانب التطبيقي، من أجل تحليل وتقييم أحد النماذج الدولية التي اعتمدت على تطبيقات الذكاء الاصطناعي للكشف عن الاحتيال في أكبر مؤسساتها المالية.

- **الدراسات السابقة:**

– The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion by David Mhlanga ,School of Accounting, University of Johannesburg, Johannesburg 2006, South AfricaInt. J. Financial Stud.

هدفت هذه الدراسة إلى التحقيق في تأثير تطبيقات الذكاء الاصطناعي بما فيها ربوتات الدردشة على الشمول المالي الرقمي. حيث استخدمت الدراسة التحليل المفاهيمي والوثائقي للمجلات والتقارير ...إلخ لتقييم تأثير تطبيقات الذكاء الاصطناعي على الشمول المالي الرقمي.

توصلت الدراسة إلى التأكيد على أن للذكاء الاصطناعي تأثيرا قويا على الشمول المالي الرقمي في المجالات المتعلقة باكتشاف المخاطر، معالجة مشكلة عدم تناسق المعلومات ومكتب المساعدة من خلال روبوتات المحادثة واكتشاف الاحتيال والأمن السيبراني؛ لذلك أوصت الدراسة بأن تقوم المؤسسات المالية والمؤسسات غير المالية والحكومات في جميع أنحاء العالم بتبني وتوسيع نطاق استخدام أدوات وتطبيقات الذكاء الاصطناعي لأنها تقدم فوائد في السعي لضمان أن الفئات الضعيفة من الأشخاص غير نشطين ماليًا، ودفعهم للمشاركة في السوق المالية الرسمية مع الحد الأدنى من التحديات.

- The role of artificial intelligence in financial in developing Kshetri Nir countries, journal of global information technology management 2021,

هدفت هذه الدراسة إلى معرفة مدى مساهمة تطبيقات الذكاء الاصطناعي بما فيها ربوتات الدردشة في تعزيز وتفعيل الشمول المالي الرقمي.

توصلت الدراسة الى إثبات قدرة الذكاء الاصطناعي في هذا المجال، من خلال القيام بأعمال وتحليلات لا يمكن للعنصر البشري القيام بها، وهذا الذي يؤدي إلى رفع كفاءة المؤسسات المالية وزيادة عدد الزبائن.

- Big Data and Artificial Intelligence for Financial Inclusion: Benefits and Issues (January 14, 2021). Artificial Intelligence Fintech, and Financial Inclusion

هدفت هذه الدراسة إلى مناقشة مختلف الفوائد والقضايا المرتبطة بالبيانات الضخمة والذكاء الاصطناعي لتحقيق الشمول المالي.

توصلت الدراسة إلى أن هذه العوائد تتمثل فيما يلي: تحسين الكفاءة وإدارة المخاطر لمقدمي الخدمات المالية؛ توفير المنتجات والخدمات المالية الذكية للبالغين المتعاملين مع البنوك؛ تبسيط عملية فتح الحساب للبالغين الذين لا يتعاملون مع البنوك، وإنشاء درجات ائتمانية للبالغين الذين لا يتعاملون مع البنوك باستخدام معلومات بديلة. بالإضافة إلى معالجة نقائص العديد من القضايا المرتبطة بالذكاء الاصطناعي والبيانات الضخمة للشمول المالي، والتي تحتاج إلى معالجة: نقص العاملين المهرة في الذكاء الاصطناعي، وزيادة مستوى البطالة في النظام البيئي المالي، والتحيز اللاواعي في تصميم أنظمة الذكاء الاصطناعي، وغيرها. الحواجز التي تسببها قوانين خصوصية البيانات الصارمة.

ما يميز الدراسة الحالية عن الدراسات السابقة:

تناولت الدراسات السابقة مساهمة تطبيقات الذكاء الاصطناعي عموما في تعزيز وتفعيل الشمول المالي الرقمي على المستوى الكلي، لكن هذه الدراسة ستركز فقط على أحد تطبيقات الذكاء الاصطناعي، ويتعلق الأمر بتطبيقات الأمن السيبراني ومساهمته في الكشف عن الاحتيال على المستوى الجزئي، بتحليل وتقييم لأحد النماذج الرائدة في مجال الكشف عن الاحتيال بالاعتماد على تطبيقات الذكاء الاصطناعي.

- **تقسيم الدراسة:**

تم تقسيم الدراسة إلى ثلاثة أجزاء رئيسة، يتناول الجزء الأول ماهية المتغير الأول من متغيرات الدراسة، ويتعلق الأمر بالذكاء الاصطناعي، ليخصص الجزء الثاني في التعريف بالمتغير الثاني للدراسة، ويتعلق الأمر بتطبيقات الأمن السيبراني، وكذلك محاولة إبراز العلاقة بين متغيري الدراسة، أما الجزء الثالث فقد اشتمل على دراسة حالة لأحد النماذج الدولية الرائدة في اعتمادها لتطبيقات الأمن السيبراني على مستوى مؤسستها المصرفية للكشف عن الاحتيال.

أولا. الإطار العام للذكاء الاصطناعي

يعتبر الذكاء الاصطناعي نقطة تحول كبيرة في تاريخ البشرية، نظرا لما يقدمه من طرق جديدة وحديثة في عمليات التسيير والإدارة في مختلف الميادين والتخصصات، فلقد جاء هذا العلم نتيجة لخبرات وتجارب وأبحاث لكثير من المفكرين والباحثين، والتي تم ترجمتها إلى برامج وأجهزة توضع في خدمة الأفراد، مثل القيام بتجارب البحث العلمي أو خدمة المؤسسات للقيام بالمهام والأنشطة المختلفة. ونظرا للأهمية المتزايدة لهذا العلم سيتم من خلال هذا العنصر التعرف على مفهوم ونشأة مصطلح الذكاء الاصطناعي، المكونات الرئيسة للذكاء الاصطناعي وأنواعه، بالإضافة إلى أهداف وخصائص الذكاء الاصطناعي.

1. مفهوم الذكاء الاصطناعي:

الذكاء الاصطناعي هو مصطلح شامل لسلسلة متطورة من التقنيات التي شهدها العالم على مدى العقود القليلة الماضية، ولهذا السبب لا يوجد تعريف موحد له ليعمل في جميع السياقات ويخدم جميع المستخدمين "فهو فرع علم الحاسب الذي يتعامل مع محاكاة السلوك الذكي في أجهزة الكمبيوتر وقدرة الماكينة على تقليد السلوك البشري" (سعيدة صبري، 2021، صفحة 273)، كما يمكن تعريفه ببساطة على أنه "ذكاء الآلة أو الكمبيوتر الذي يمكنه من تقليد القدرات البشرية" (Vijaykanade، 2023)، يعرف جون مكارثي الذكاء الاصطناعي بأنه: "علم وهندسة صناعة الآلات الذكية، وخاصة برامج الكمبيوتر الذكية". ينقل الذكاء الاصطناعي الذكاء إلى الآلات حتى تتمكن الآلات الذكية من العمل والتشغيل والتفاعل تمامًا مثل البشر والمساعدة في اتخاذ القرار بناءً على سيناريوهات الوقت الفعلي (Top 10 Characteristics of Artificial Intelligence، 2023).

2. خصائص وأهداف الذكاء الاصطناعي

هناك العديد من الخصائص والأهداف المرتبطة بالذكاء الاصطناعي يمكن حصرها فيما يلي:

1.2. خصائص الذكاء الاصطناعي:

لقد تطور الذكاء الاصطناعي منذ نشأته حتى الآن، سنعرض فيما يلي بعض الخصائص التي يتميز بها الذكاء الاصطناعي: (Top 7 Artificial Intelligence Characteristics with Examples، 2023)

- التعلم العميق: هو أسلوب تعلم آلي يعلم أجهزة الكمبيوتر أن تفعل ما هو طبيعي للبشر. مثل المركبات ذاتية القيادة، وإنشاء النص التلقائي، وما شابه ذلك، خذ مثالاً على ميزة القيادة الذاتية في سيارات مثل Tesla أو الطيار الآلي، حيث يعد التعلم العميق تقنية أساسية وراء تمكينهم من التعرف على علامة التوقف أو تمييز المشاة عن عمود الإنارة.
- التعرف على الوجه: أتاح الذكاء الاصطناعي التعرف على الوجوه الفردية، وقد أدى ذلك إلى تطورات رائدة في تقنيات المراقبة. يقارن المعرفة بقاعدة بيانات الوجوه المعروفة للبحث عن تطابق. ومع ذلك، فقد واجه هذا أيضًا كثيرا من الانتقادات بسبب انتهاك الخصوصية.
- أتمتة المهام البسيطة والمتكررة: يتمتع الذكاء الاصطناعي بالقدرة على تنفيذ نفس النوع من العمل مرارًا وتكرارًا دون عناء. لنأخذ مثال Siri، المساعد الصوتي يمكنه التعامل مع العديد من الأوامر في يوم واحد من طلب تدوين الملاحظات لفترة وجيزة، إلى إعادة جدولة التقويم للاجتماع، إلى إرشادنا عبر الشوارع باستخدام التنقل، حيث قام المساعد الصوتي بتغطية كل شيء.
- استيعاب البيانات: تتزايد البيانات التي ننتجها بشكل كبير وهنا يتدخل الذكاء الاصطناعي، فاستيعاب البيانات هو نقل المعرفة من مصادر متنوعة إلى وسيط تخزين البيانات. فبدلاً من تغذية هذه البيانات يدويًا، يجمعها الذكاء الاصطناعي ثم يحللها بمساعدة تجاربه السابقة.
- روبوتات المحادثة: روبوتات المحادثة عبارة عن برنامج يوفر نافذة لحل مشكلات العملاء "من خلال الإدخال الصوتي أو النصي". هناك كثير من الشركات التي انتقلت من مديري العمليات الصوتية إلى روبوتات المحادثة لمساعدة العملاء على حل مشكلاتهم، وتقديم اقتراحات المنتجات للمستخدمين.

2.2. أهداف الذكاء الاصطناعي

إجمالاً، الهدف العام للذكاء الاصطناعي هو إدخال خوارزمية وإنشاء المخرجات المرغوبة، وفيما يلي بعض الأهداف الأخرى: (Goals of Artificial Intelligence، 2023)

- حل المشكلات: إن قدرة الذكاء الاصطناعي على حل المشكلات تساهم في جعل حياتنا أسهل، وذلك بتطوير خوارزميات فعالة لحل المشكلات يمكنها إجراء استنتاجات منطقية ومحاكاة التفكير البشري، مثل نظام التنبؤ بسوق الأوراق المالية.
- تمثيل المعرفة: يتعلق الأمر بتمثيل "ما هو معروف" للآلات باستخدام مجموعة من العلاقات والمفاهيم. يكشف التمثيل عن معلومات من العالم الحقيقي والتي يستخدمها الكمبيوتر لحل مشاكل الحياة الواقعية المعقدة، مثل تشخيص مرض طبي أو التفاعل مع البشر بلغة طبيعية.
- التخطيط: يمكننا إجراء تنبؤات مستقبلية والتأكد من نتائج أفعالنا. حيث نستعمل التخطيط عبر الروبوتات في إدارة المخاطر والأمن السيبراني...الخ.
- التعلم: التعلم الآلي، هو دراسة خوارزميات الكمبيوتر التي تتحسن تلقائيًا من خلال التجربة. من الناحية الفنية، تعالج برامج الذكاء الاصطناعي مجموعة من أزواج المدخلات والمخرجات لوظيفة محددة وتستخدم النتائج للتنبؤ بنتائج المدخلات الجديدة.
- الذكاء الاجتماعي: هي دراسة وتطوير الأنظمة التي يمكنها تفسير ومعالجة ومحاكاة الإنسان. وتسمى أيضًا "العاطفة "باستخدامه، يمكن لأجهزة الكمبيوتر قراءة تعابير الوجه ولغة الجسد ونغمات الصوت للسماح لأنظمة الذكاء الاصطناعي بالتفاعل والتواصل الاجتماعي على المستوى البشري.
- الإبداع: يمكن للذكاء الاصطناعي نقل كميات هائلة من البيانات والنظر في الخيارات والبدائل وتطوير مسارات أو فرص إبداعية لنا للتقدم. على سبيل المثال، يمكن أن يوفر نظام AI خيارات متعددة للتصميم الداخلي لتخطيط شقة ثلاثي الأبعاد.
- الذكاء العام: يهدف باحثو الذكاء الاصطناعي إلى تطوير آلات ذات قدرات عامة للذكاء الاصطناعي تجمع بين جميع المهارات المعرفية للبشر وتؤدي المهام بكفاءة أفضل منا. كما سيساعد على تحرير البشر من أداء المهام الخطرة مثل نزع فتيل القنابل.

3. أهم تطبيقات الذكاء الاصطناعي في البنوك:

قدمت تطبيقات الذكاء الاصطناعي خدمات متميزة في المجال المالي والمصرفي نتيجة تمتعه بكفاءة عالية على تغيير طبيعة الخدمات المالية التقليدية وتطويرها، فأصبحت أكثر ابتكاراً وكفاءة وتنوعاً، من شأنها تحسين وتسهيل تجربة العملاء. فيما يلي بعض تطبيقات الذكاء الاصطناعي الرئيسية في الصناعة المصرفية.

1.3. تطبيق روبوت الدردشة –Chatbot–

منذ أن بدأ الوباء شهدت الصناعة المالية أشخاصًا على استعداد للتحرك نحو المعاملات الرقمية عبر المؤسسات المالية، واضطرت البنوك إلى تقليل اعتمادها على البشر عندما يكون ذلك ممكنًا واللجوء إلى روبوت الدردشة، سواء أكان الأمر يتعلق بمعالجة المعاملات والاستشارات أم الوصول إلى خدمة العملاء (Helena Franco، 2023).

تتكوّن كلمة Chatbot من كلمتين، وهما شات Chat، مثل الدردشة على الإنترنت، وبوت botمثل الروبوت؛ فالشات بوت هو برمجية مصمّمة لمحاكاة محادثة باللغة الطبيعية.

أما بالنسبة لروبوتات الدردشة الخاصة بالخدمات المصرفية فهي في الأساس روبوتات محادثة للمحادثة، يتم نشرها من قبل البنوك لتعزيز تجربة العملاء على جميع منصات الخدمات المصرفية الرقمية. تساعد روبوتات الدردشة المصرفية على تحسين مشاركة العملاء وتسهيل العمليات القديمة، مما يجعل الوصول المصرفي أكثر سهولة في هذا العصر (Ananya Azad، 2023).

حيث المهام التي كان يتم إكمالها من خلال التحدث إلى إنسان في فرع أو على الهاتف تتم الآن في واجهة محادثة مع مساعدين افتراضيين للدعم الآلي، كما توفر روبوتات المحادثة المصرفية للمؤسسات المالية القدرة على التحدث إلى ملايين العملاء في وقت واحد وتنبيه العملاء بشكل استباقي إلى المشكلات المحتملة أو المدفوعات القادمة. (Emily Cummins، 2023)

بالنسبة لحالات استخدام روبوت الدردشة في البنوك تتمثل فيما يلي: (Shambhavi Sin، 2023)

- تحويل الأموال: يمكن للمستخدمين استخدام روبوتات الدردشة لدفع الفواتير وتعيين المدفوعات أو إلغائها وتتبع المعاملات المالية وسداد فواتير بطاقات الائتمان.

- الإجابة عن الأسئلة الأساسية: على سبيل المثال يمكن لبرامج الدردشة الآلية الإجابة عن أسئلة مثل "كيف يمكنني التقدم بطلب للحصول على بطاقة ائتمان".
- يوفر الإخطارات والتذكيرات في الوقت المحدد: تستخدم معظم البنوك روبوتات المحادثة لتقدم لعملائها تذكيرات في الوقت المناسب وإشعارات منتظمة بشأن حساباتهم المصرفية. غالبًا تتعلق بالمواعيد النهائية لدفع فواتيرهم، وعرض قروض اليوم الأخير، وغير ذلك.
- التحقق من رصيد الحساب: يمكن للمستخدمين أن يطلبوا من روبوتات الدردشة تزويدهم بتفاصيل رصيد الحساب بأسمائهم. كما يمكنهم أيضًا تنبيه العملاء إذا كان رصيد حساباتهم معرضًا لخطر الانخفاض إلى أقل من متوسط الرصيد.
- يقدم تفاصيل الحساب كاملة: يمكن للمستخدمين أيضًا السؤال عن تفاصيل أخرى للحسابات، مثل المدفوعات والنفقات المتكررة وحدود تحويل الأموال. يمكن للمرء أيضًا استرداد تفاصيل حسابه وإجراء تغييرات مثل تحديث العنوان الحالي أو رقم الهاتف.
- تتبع الموقع في الوقت الحقيقي: يمكن لـ Chatbot تتبع الموقع من خلال GPS المحمول، ومن ثم توفير الإجابات الصحيحة في كل مرة.
- حل القضايا العاجلة ذات الأولوية: تتضمن هذه القضايا فتح البطاقات أو إقفالها وإعادة الضبط والتحقق من كشوف الحسابات المصرفية واستكمال عمليات تحويل الأموال.

في هذا المجال يعد Erica أحد أفضل الأمثلة على روبوتات الدردشة بالذكاء الاصطناعي في التطبيقات المصرفية، وهو مساعد افتراضي من بنك أمريكا. قامت Erica بإدارة أكثر من 50 مليون طلب عملاء في عام 2019(Saurabh Singh, 2023) .

2.3. تطبيق الأمن السيبراني وكشف الاحتيال

كل يوم يتم إجراء عدد كبير من المعاملات الرقمية، حيث يقوم المستخدمون بدفع الفواتير وسحب الأموال وإيداع الشيكات والقيام بالكثير من خلال التطبيقات أو الحسابات عبر الإنترنت. وبذلك هناك حاجة متزايدة للقطاع المصرفي لتكثيف جهود الأمن السيبراني واكتشاف الاحتيال (Massimiliano Aschi, Susanna Bonura, Nicola Masi, 2023). سيتم التعرض لهذا التطبيق بالتفصيل في العنصر الآتي من هذه الدراسة.

3.3. تطبيق الإقراض

يُعد الإقراض الأكثر شمولاً بواسطة الذكاء الاصطناعي بمثابة ربح لجميع الأطراف المعنية. بالنسبة للمقرضين، فهو يجمع بين كونه أداة تسويق رائعة ووسيلة لتحقيق المنافسة مع البنوك بأقل التكاليف. ومن جهة أخرى يحصل المقترضون، خاصة أولئك الذين لديهم ملفات رفيعة وبدون تواريخ ائتمان، على فرصة أفضل للحصول على تمويل بسعر معقول وفي وقت قليل. ومع ذلك يركز منتقدو الذكاء الاصطناعي على جودة البيانات المستخدمة، قائلين إن هناك احتمالًا لأن تصبح التكنولوجيا متحيزة عندما تستخدم الخوارزميات بيانات خاطئة للوصول إلى استنتاجات، أو تعمل في مناطق لا تتوفر فيها بيانات كافية (مثل البيئات الأقل تنافسية أو سلوك التسوق المنخفض). ويمكن أن يحدث هذا في المجتمعات التي تعاني من نقص البنوك(Dmitry Dolgorukov, 2023) .

أما بالنسبة لاتجاهات اعتماد الذكاء الاصطناعي في الإقراض نذكر فيما يلي: (أوستاب زابولوتني، 2023)

- تقليل وقت دورة الإقراض: من خلال تقنية الذكاء الاصطناعي الذكية، يمكن للمقرضين تقصير الوقت الذي تستغرقه معالجة القرض من أسابيع إلى ساعات. تتطلب المراحل الأولية من معالجة القرض أعمال توثيق كبيرة، والتي تستغرق كثيرا من الوقت.
- توافر البيانات لاتخاذ قرارات ائتمانية أفضل: يتم تقليل الوقت المستغرق لتقييم الوضع المالي للشركة من خلال أنظمة اتخاذ القرار الائتماني المؤتمتة التي أصبحت ممكنة بفضل حلول الذكاء الاصطناعي القائمة على البيانات.
- عدم القدرة على التعامل مع الحجم الكبير لطلبات القرض: يمكن أن تساعد نماذج الذكاء الاصطناعي البنوك ومؤسسات الإقراض على تعزيز الدقة، لاسيما عند معالجة طلبات القروض بكميات كبيرة .
- معالجة القروض باستخدام البيانات الرقمية: يحل الإقراض الآلي ومعالجة القروض بالذكاء الاصطناعي محل العمليات اليدوية في الرابطة الرقمية عالية الاتصال؛ مما يضمن الموافقة على القروض وصرفها بشكل سلس.

4. فوائد وتحديات الذكاء الاصطناعي في الصناعة المصرفية

نستعرض في هذا العنصر فوائد الذكاء الاصطناعي في القطاع المصرفي بشكل خاص مع التطرق أيضًا إلى بعض المخاطر والتحديات التي تواجه صناعة الخدمات المالية عند استخدام الذكاء الاصطناعي.

1.4. فوائد الذكاء الاصطناعي في القطاع المصرفي

فيما يلي قائمة بأهم خمس فوائد للذكاء الاصطناعي في الصناعة المالية والمصرفية كالآتي: (Top 5 Benefits of Artificial Intelligence in Banking and Finance, 2023)

- الامتثال التنظيمي وكشف الاحتيال: مع زيادة يقظة المؤسسات المالية يغير المحتالون سلوكهم. ولكن مع وجود نظام للكشف عن الاحتيال بالذكاء الاصطناعي، يمكن أن يتم اكتشاف النشاط الإجرامي على الفور، لأن الذكاء الاصطناعي يستطيع تحليل كميات كبيرة من البيانات من أجل انتقاء المعاملات المشبوهة.
- تجربة أفضل للعملاء: يبحث العملاء باستمرار عن الراحة. فعلى سبيل المثال كانت أجهزة الصراف الآلي ناجحة لأن العملاء يمكنهم الوصول إلى خدمة حيوية حتى عندما كانت البنوك مغلقة، هذا المستوى من الراحة ألهم المزيد من الابتكار، فالآن يمكن للعملاء فتح حسابات مصرفية والتحقق من أنفسهم باستخدام هواتفهم الذكية من الأريكة في المنزل.
- تخفيض تكاليف التشغيل والمخاطر: بقدر ما نستمتع بالتفاعل البشري، فإن له عيبًا واحدًا مهمًا وهو الأخطاء الشائعة، ويمكن أن يكون لها تداعيات خطيرة، فحتى عندما يتولى الموظفون المتمرسون القيادة، فإن الضغط الخاطئ على المفتاح قد يعرض المؤسسة للمسؤولية، ويسبب ضررًا لا يمكن إصلاحه لسمعتها. تقلل أنظمة الذكاء الاصطناعي من هذه المخاطر عن طريق الجمع بين التقنيات التنبؤية والتعليمية لحل مشاكل الأعمال.
- تحسين تقييم القروض والتسهيلات: يمكن للنظام القائم على الذكاء الاصطناعي أن يعطي توصيات بالموافقة أو الرفض من خلال النظر في المزيد من المتغيرات حتى عندما يكون لدى الطرف القليل من الوثائق.

2.4. التحديات الرئيسية للذكاء الاصطناعي

يُعد الذكاء الاصطناعي تقنية ناشئة، خاصة في البنوك، لذلك قد يمثل خطرًا تجاريًا، ونتيجة لذلك يجب على المؤسسات المالية أن توازن ما بين فوائد الذكاء الاصطناعي من جهة، وبين المخاطر والتحديات التالية من جهة أخرى: (فايز الشهري، 2023)

- تحديات قانونية محفوفة بالخطر: إحدى الحالات التي نوقشت على نطاق واسع هي كيفية تحديد المسؤوليات القانونية الناتجة عن خطأ قرارات الذكاء الاصطناعي في العلاج والأجهزة والمركبات ذاتية القيادة. على سبيل المثال كيف يمكن مواجهة شراهة منتجات الذكاء الاصطناعي

للمعلومات وإشكالات انتهاكات الخصوصية والتحيز واتخاذ القرارات التي لا يمكن الرجوع عنها أو الطعن فيها.

- الخوف من تنامي تأثير تطبيقات الذكاء الاصطناعي على الوظائف (العمل): مما سيزيد من معدلات فقدان الوظائف. على سبيل المثال الروبوت (أحد تطبيقات الذكاء الاصطناعي) الذي بدأ استخدامه بشكل واضح في المصانع ونقاط التوزيع والتسليم وأثره على معدلات البطالة في هذه المهن. ووفقًا لدراسة أجراها معهد ماكينزي العالمي، يمكن للروبوتات والوكلاء الأذكياء أن يحلوا محل ما يقرب من 30 ٪ من العمالة البشرية الحالية في العالم بحلول عام 2030.
- خروج الذكاء الاصطناعي عن السيطرة البشرية: يقول الفيزيائي الراحل ستيفن هوكينغ: "إنه إذا بدأ الذكاء الاصطناعي نفسه في تصميم ذكاء اصطناعي أفضل من المبرمجين البشر، فقد تكون النتيجة آلات تتجاوز ذكاء الإنسان الذي صممها". ويحذر إيلون ماسك من أن الذكاء الاصطناعي "هو أكبر تهديد وجودي للبشرية". وقد ظهرت دراسات عما يسمى تفرد الذكاء الاصطناعي حين ينمو الذكاء الاصطناعي في المستقبل بشكل لا يمكن السيطرة عليه.
- التكلفة العالية لبناء منظومات الذكاء الاصطناعي: ناهيك عن تكلفة التطوير والصيانة، إن إنشاء آلة يمكنها محاكاة البشر يستهلك كثيرا من الموارد والوقت، ما يجعلها مكلفة جداً لغير القادرين، وبهذا يزيد الذكاء الاصطناعي من الفجوة بين الدول الغنية والفقيرة.
- تحدي إدمان استخدامات الذكاء الاصطناعي: إن إدمان استخدام الذكاء الاصطناعي له عواقب بعيدة المدى على الأجيال المقبلة واحتمالية جعله الناس أقل ذكاءً. إذ مع تزايد استخدام الآلات في الأعمال الروتينية سيصبح الناس أقل نشاطًا بدنياً ما يعني معدلات أعلى من الأمراض على رأسها السمنة والسكري الثانوي وأمراض القلب.

ثانيا. ماهية تطبيق الأمن السيبراني وكشف الاحتيال

كل يوم يتم إجراء عدد كبير من المعاملات الرقمية، حيث يقوم المستخدمون بدفع الفواتير وسحب الأموال وإيداع الشيكات والقيام بالكثير من خلال التطبيقات أو الحسابات عبر الإنترنت. ومن ثم هناك حاجة متزايدة للقطاع المصرفي لتكثيف جهود الأمن السيبراني واكتشاف الاحتيال (Massimiliano Aschi, Susanna Bonura, Nicola Masi, Domenico Messina, Davide Profeta, 2023).

1. تعريف تطبيق الأمن السيبراني

تطبيق الأمن السيبراني هو أحد تطبيقات الذكاء الاصطناعي، ويعرف على أنه ممارسة الحماية لأجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية. فهي تعتمد تدابير وأدوات الأمن السيبراني من أجل حماية البيانات الحساسة من الوصول غير المصرح به، وكذلك منع أي انقطاع للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه. تطبق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأفراد والعمليات والتقنيات.

الهجوم السيبراني، ويقصد به الاستغلال غير المشروع لأنظمة الحاسب، الشبكات والمنظمات التي يعتمد عملها على تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار به. وتشمل أي نوع من الأنشطة الخبيثة التي تحاول الوصول بطريقة غير المشروعة، أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية أو المعلومات نفسها. (البنك المركزي السعودي، 2023)

2. كيفية عمل تطبيق الأمن السيبراني

تنفذ المؤسسات استراتيجيات الأمن السيبراني من خلال العمل مع متخصصين في الأمن السيبراني. يقيّم هؤلاء المتخصصون المخاطر الأمنية لأنظمة الحوسبة الحالية، والشبكات، ومخازن البيانات، والتطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك ينشئ متخصصو الأمن السيبراني إطار عمل شامل له وينفذون تدابير وقائية في المؤسسة. تعمل هذه العناصر معًا لإنشاء طبقات متعددة من الحماية ضد التهديدات المحتملة على جميع نقاط الوصول إلى البيانات. فهي تحدد المخاطر، وتحمي الهويات والبنية الأساسية والبيانات، وترصد أوجه الخلل والأحداث، وتستجيب وتحلل السبب الجذري، وتتعافى بعد وقوع الحدث (Amazon Web Services، 2023).

يمكن للذكاء الاصطناعي معالجة العديد من القيود، ويساعد على تحديد المعاملات الخطرة بشكل أكثر فعالية من الإنسان، مما يعني أنه كلما تم تدريب الآلة على المزيد من عينات العمليات الاحتيالية، زاد ذلك من إمكانية تعرف الآلة على الاحتيال.

إن وجود نظام أكثر كفاءة للكشف عن الاحتيال، ويعتمد على التعلم الآلي، من شأنه أن يقلل التكاليف من خلال الكفاءات الناتجة عن التشغيل الآلي العالي، ومعدلات الخطأ المنخفضة، واستخدام الموارد بشكل أفضل. بالإضافة إلى ذلك يمكن لأصحاب المصلحة المالية أو التأمين معالجة أنواع جديدة من عمليات الاحتيال، وتقليل الاضطرابات للعملاء الشرعيين، ومن ثم زيادة ثقة

العميل وأمنه (Massimiliano Aschi, Susanna Bonura, Nicola Masi, Domenico Messina, Davide Profeta، 2022).

3. تقنية عمل تطبيق الأمن السيبراني الحديثة وتحدياته

فيما يلي سيتم التطرق إلى كل من تقنية عمل تطبيق الأمن السيبراني والتحديات التي تواجهه:

1.3. تقنية عمل تطبيق الأمن السيبراني

فيما يلي تقنيات الأمن السيبراني الحديثة التي تساعد المؤسسات على تأمين بياناتها: (Amazon Web Services، 2023)

- انعدام الثقة: انعدام الثقة هو أحد مبادئ الأمن السيبراني الذي يَفترض عدم الوثوق بأي تطبيقات أو مستخدمين تلقائيًا، حتى في حالة استضافتهم داخل المؤسسة، ما يتطلب مصادقة صارمة من السلطات المعنية ومراقبة مستمرة للتطبيقات.
- تحليلات السلوك: تراقب تحليلات السلوك عملية نقل البيانات من الأجهزة والشبكات لاكتشاف الأنشطة المشبوهة والأنماط غير المعتادة. على سبيل المثال يتم تنبيه فريق أمن تكنولوجيا المعلومات بحدوث ارتفاع مفاجئ في نقل البيانات أو بتنزيل ملفات مشبوهة إلى أجهزة معينة.
- نظام كشف التسلل: تستخدم المؤسسات أنظمة كشف التسلل لتحديد الهجوم السيبراني والاستجابة له بسرعة. تحدّد آلية الدفاع ضد التسلل مسارًا للبيانات في حالة وقوع حادث، ما يساعد فريق الأمن على اكتشاف مصدر الحادث.
- التشفير السحابي: يعمل التشفير السحابي على تشفير البيانات قبل تخزينها في قواعد البيانات السحابية، وهذا يمنع الأطراف غير المصرح لها من إساءة استخدام البيانات في انتهاكات محتملة.

2.3. تحديات تطبيق الأمن السيبراني:

يُعد الذكاء الاصطناعي مناسبًا بشكل مثالي لحل بعض أصعب مشكلاتنا، ومن المؤكد أن الأمن السيبراني يقع ضمن هذه الفئة. مع تطور الهجمات الإلكترونية اليوم وانتشار الأجهزة، يمكن استخدام التعلم الآلي والذكاء الاصطناعي "لمواكبة المحتالين"، وأتمتة اكتشاف التهديدات والاستجابة بشكل أكثر كفاءة من الأساليب التقليدية التي تعتمد على البرامج. في الوقت نفسه، يواجه الأمن

السيبراني بعض التحديات نذكرها في الآتي: (Using Artificial Intelligence in Cybersecurity، 2023)

- مساحة هجوم واسعة، حيث يوجد من عشرة إلى آلاف الأجهزة المعرضة للهجوم في كل مؤسسة؛
- نقص كبير في عدد المهنيين الأمنيين المهرة؛
- كتل البيانات التي تجاوزت مشكلة النطاق البشري، والتي يجب حمايتها.

يجب أن يكون نظام إدارة الأمن السيبراني القائم على التعلم الذاتي وعلى الذكاء الاصطناعي قادرًا على حل العديد من هذه التحديات. ويشمل ذلك كل ما يلي: (Using Artificial Intelligence in Cybersecurity، 2023)

- جرد أصول تكنولوجيا المعلومات: الحصول على جرد كامل ودقيق لجميع الأجهزة والمستخدمين والتطبيقات مع أي وصول إلى أنظمة المعلومات.
- التعرض للتهديدات: يمكن أن توفر أنظمة الأمن السيبراني المستندة إلى الذكاء الاصطناعي معرفة محدثة بالتهديدات العالمية والصناعية، ومنه اكتساب خبرة عن التهديدات المحتملة للمساعدة في اتخاذ القرارات الحاسمة لمنع الاحتيال.
- فعالية الضوابط: من المهم فهم تأثير أدوات الأمان المختلفة وعمليات الأمان التي استخدمتها للحفاظ على وضع أمني قوي. يمكن أن يساعد الذكاء الاصطناعي في فهم مواطن القوة في البرنامج وأين توجد الثغرات به.
- توقع مخاطر الاختراق: يمكن للأنظمة المستندة إلى الذكاء الاصطناعي أن تتنبأ بكيفية وأين من المرجح أن يتم خرقك، بحيث يمكنك التخطيط لتخصيص الموارد والأدوات نحو مناطق الضعف. يمكن أن تساعدك الرؤى الوصفية المستمدة من تحليل الذكاء الاصطناعي في تكوين وتعزيز الضوابط والعمليات لتحسين المرونة الإلكترونية لمؤسستك بشكل أكثر فاعلية.
- الاستجابة للحوادث: يمكن للأنظمة التي تعمل بالذكاء الاصطناعي أن توفر سياقًا محسنًا لتحديد الأولويات وللتنبيهات الأمنية للاستجابة السريعة للحوادث، ولإظهار الأسباب الجذرية من أجل التخفيف من نقاط الضعف وتجنب المشكلات المستقبلية.

4. تطبيق الأمن السيبراني والسلامة الرقمية

يتمتع تطبيق الذكاء الاصطناعي في الأمن السيبراني للسلامة الرقمية بالعديد من الفوائد والاستخدامات تتمثل فيما يلي: (الذكاء الاصطناعي، 2023)

- القدرة على اكتشاف وتحديد الأنماط الشاذة ونقاط الضعف داخل الشبكات الواسعة: يستغرق البشر وقتًا طويلاً أو بالأحرى معقدًا في مراقبة وتحليل الشبكات واسعة النطاق. باستخدام الذكاء الاصطناعي يصبح تحليل البيانات أكثر كفاءة وأسرع، مما يؤدي إلى الكشف السريع عن نقاط الضعف والتهديدات قبل تنفيذ أي هجوم.
- تقييمات دقيقة للمخاطر وتحسين استخبارات التهديدات: يمكن إجراء تحديد دقيق وتحليل وتقييم للمخاطر، وتقديم توصيات بشأن ضوابط أمنية قوية للمخاطر المكتشفة من خلال المعلومات الاستخباراتية المجمعة للذكاء الاصطناعي. يؤدي هذا أيضًا إلى تطوير نماذج الأمان المؤتمتة، ومن ثم بناء موقف أمان تنظيمي قوي.
- القدرة على أتمتة المهام: يمكن أتمتة العمليات التي تستغرق وقتًا طويلاً دون أي فترات زمنية، مما سيزيد من أوقات الاستجابة، ويقلل من ضغط التعامل مع المهام الأمنية المعقدة للمحللين البشريين.

ثالثا: عرض تجربة بنك Danske الدنماركي في الحد من الاحتيال بتطبيق الذكاء الاصطناعي

يُعد الحد من الاحتيال أولوية قصوى للبنوك، فوفقًا لجمعية مدققي الاحتيال المعتمدين تخسر الشركات أكثر من 3.5 تريليون دولار سنويًا بسبب الاحتيال. هذه المشكلة منتشرة في جميع أنحاء الصناعة المالية، وتصبح أكثر انتشارًا وتعقيدًا كل شهر. نظرًا لأن العملاء يُجرون المزيد من الخدمات المصرفية عبر الإنترنت عبر مجموعة أكبر من القنوات والأجهزة، فهناك المزيد من فرص حدوث الاحتيال. إضافة إلى ذلك أصبح المحتالون أكثر إبداعًا وذكاءً من الناحية التكنولوجية، فهم يستخدمون أيضًا تقنيات متقدمة مثل التعلم الآلي والتطور بسرعة لإيجاد مخططات جديدة للاحتيال على البنوك. ومع زيادة استخدام الرقمنة واستخدام التكنولوجيا، فإنها تزيد أيضًا من طرق ووسائل المحتالين للاستفادة من نفس التكنولوجيا لارتكاب الاحتيال.

ولهذا تحتاج البنوك والمؤسسات المالية وأي مؤسسة أخرى تتعامل مع الأموال أو التمويل أو أي أداة مالية أخرى إلى تنفيذ تدابير وأنظمة وعمليات صارمة للكشف عن الاحتيال في مرحلة مبكرة أو قبل حدوثه إن أمكن. في هذا المجال يساعد الذكاء الاصطناعي والتعلم الآلي في إيجاد حلول فعالة

للكشف عن الاحتيال في النظام المصرفي، ومنعها في الوقت الفعلي، وتعد برامج منع الاحتيال المصرفي جزءًا أساسيًا من الدروع التي تستخدمها البنوك. وفي هذا العنصر سيتم عرض تجربة بنك Danske الدنماركي في الكشف عن الاحتيال بالاستعانة بكل من: شركة Teradata، شركة Featurespace الذين استعملوا الذكاء الاصطناعي في محاربة الاحتيال في المعاملات المالية على مستوى البنك (Ryan Williamson، 2023).

1. التعريف ببنك Danske

هو بنك عالمي من بلدان الشمال الأوروبي، ذو جذور محلية قوية وجسور مع بقية العالم. تأسس بنك Danske في أكتوبر 1871، وساعد الأشخاص والشركات في بلدان الشمال الأوروبي على تحقيق طموحاتهم لأكثر من 145 عامًا. مقره الرئيسي في الدنمارك وأسواقه الأساسية هي الدنمارك، وفنلندا، والنرويج، والسويد. له أكثر من 5 ملايين عميل تجزئة. يعمل هذا البنك في 16 دولة، ويخدم أكثر من 1800 شركة ومؤسسة و236000 شركة صغيرة ومتوسطة الحجم و2.7 مليون عميل شخصي (Danske Bank Fights Fraud with Deep Learning and AI, 2023).

يحتفظ بنك Danske بما يقرب من 50 ٪ من السوق المصرفية الدنماركية. وتشمل الشركات الأخرى التابعة له بنك شمال إيرلندا والبنك الإيرلندي الوطني، وكذلك داخل شركات العقارات ورؤوس الأموال والتأجير في الدنمارك (تغريد ابراهيم، 2023).

2. الكشف عن الاحتيال بواسطة شركة Teradata

أعلنت شركة Teradata المدرجة في بورصة نيويورك أن Danske Bank، رائد الخدمات المالية في دول الشمال، قد عمل مع Think Big Analytics، وهي شركة Teradata، لإنشاء وإطلاق نظام أساسي للكشف عن الاحتيال يعتمد على الذكاء الاصطناعي.

Teradata عبارة عن منصة بيانات متصلة متعددة السحابة لشركة تحليلات المؤسسة. تحل تحليلات المؤسسة الخاصة بها تحديات الأعمال من البداية إلى النهاية، يمنحك Teradata فقط المرونة للتعامل مع أعباء عمل البيانات الضخمة والمختلطة (Doug Henschen، 2023).

كان نظام الكشف عن الاحتيال الأصلي لبنك Danske يعتمد إلى حد كبير على قواعد مصنوعة يدويًا تم تطبيقها بشكل استباقي من قبل الشركة، بمرور الوقت، ومع وجود أرقام قياسية

للإيجابيات الكاذبة، وصلت في بعض الأحيان إلى 99.5 % من جميع المعاملات، ومع ارتفاع التكاليف والوقت المرتبطين بالتحقيق، بالإضافة الى افتقارها للخبرة في إدخال تقنياته في الإنتاج، لجأ البنك إلى Think Big Analytics، وهي وحدة إستراتيجية للبيانات الضخمة والاستشارات والتنفيذ في Teradata، والتي قدمت الخبرة والتجربة لعمليات مماثلة وعالية المستوى في كبرى شركات الخدمات المالية وغيرها من المؤسسات. من خلال العمل مع مستشاري Think Big Analytics في عمليات التطوير لمدة 12 أسبوعًا، طور فريق Danske Bank ونشر نماذج مجموعات تعلم الآلة التي قللت الإيجابيات الكاذبة بنسبة 20 إلى 30 %. ومن المتوقع بالفعل أن تحقق عائد استثمار بنسبة 100 % في عامها الأول من الإنتاج (Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real, 2023).

تمكن الفريق من أخذ الإيجابيات الزائفة من النماذج وتقليلها بنسبة 50 %، في الوقت نفسه يمكنهم اكتشاف المزيد من الاحتيال، في الواقع يزيدون معدل الكشف بحوالي 60 %. يعد برنامج مكافحة الاحتيال في بنك Danske هو أول برنامج يضع تقنيات التعلم الآلي في الإنتاج مع تطوير نماذج التعلم العميق في نفس الوقت لاختبار التقنيات. حيث قال Mads Andjoiar، مدير خدمات العملاء فيThink Big Analytics : "بالنسبة للمعاملات عبر الإنترنت وبطاقات الائتمان والمدفوعات عبر الهاتف المحمول، تحتاج البنوك إلى حل في الوقت الفعلي حيث إن منصة الاحتيال المدعومة بالذكاء الاصطناعي التي طورناها بالتعاون مع بنك Danske تسجل المعاملات الواردة في أقل من 300 ملي ثانية" (Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real, 2023).

كما قدم Nadim Golzer، رئيس التحليلات المتقدمة في بنك Danske، تصريحا مفاده: "إن المحتالين جيدون باستخدام تقنيات التعلم الآلي المتطورة للهجوم، لذلك من المهم استخدام تقنيات متقدمة، مثل التعلم الآلي للقبض عليهم. وباستخدام الذكاء الاصطناعي، قمنا بالفعل بتخفيض النتائج الإيجابية الزائفة بنسبة 50 % وبالتالي تمكنا من إعادة تخصيص نصف وحدة الكشف عن الاحتيال إلى مسؤوليات ذات قيمة أعلى" (Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real, 2023).

3. الكشف عن الاحتيال بواسطة شركة Featurespace

تشتهر Featurespace بأنها قامت ببناء أول محرك تحليلات سلوكية في العالم –منصة ARIC–لحل هذا التحدي المتمثل في إنشاء تقنية قوية بما يكفي لاكتشاف الاحتيال، لقد اختار Danske Bank، أكبر بنك في الدنمارك والرائد في الأسواق المالية في شمال أوروبا، شركة Featurespace، الشركة الرائدة في مجال التعلم الآلي لمنع الاحتيال، كمزود استراتيجي له لتعزيز قدراته في الحد من الاحتيال. Featurespace هي الشركة الرائدة عالميًا في مجال منع الجرائم المالية للشركات فيما يتعلق بالاحتيال ومكافحة غسيل الأموال. ابتكرت شركة Featurespace التحليلات السلوكية التكيفية وأنشأت منصة ARIC، وهي منصة برمجية للتعلم الآلي في الوقت الفعلي تخاطر بتسجيل الأحداث في أكثر من 180 دولة لمنع الاحتيال والجرائم المالية (Michael Touchton, 2023).

تم اختيار ARIC من Featurespace من قبل البنك للتخفيف من الاحتيال على البطاقة على مستوى العميل في الوقت الفعلي وعبر جميع القنوات، حيث اعتبر البنك أنه قادر على منح العملاء أفضل تجربة من خلال تقليل عدد الإيجابيات الزائفة. يأتي هذا الخبر بعد الإعلان عن أن Danske كانت تبحث عن شركات تكنولوجيا مالية للدخول في شراكة معها. تقول مارتينا كينج، الرئيس التنفيذي لشركة Featurespace: "إن التخفيف من الاحتيال يمثل تحديًا كبيرًا لأن التهديد يستمر في التطور. يسلط النظام التكيفي في الوقت الفعلي الضوء على الهجمات الجديدة في وقت حدوثها، مما يحمي البنك وعملاءه، يشرفنا أن يتم اختيارنا من قبل Danske Bank كشريك له لمكافحة البطاقات المزيفة والاحتيال الرقمي".

تستخدم Featurespace التعلم الآلي، فيما تسميه التحليلات السلوكية، لاكتشاف المعاملات الاحتيالية، ولمراقبة ملفات تعريف السلوك الفردية في الوقت الفعلي لاكتشاف الحالات الشاذة ومنع الاحتيال عبر جميع طرق الدفع والقنوات(Henry Vilar, 2023) .

ويتم ذلك عن طريق القيام بتحليلات سلوكية في الوقت الفعلي معدة للتخفيف من تعرض البنك للاحتيال على البطاقة وحماية القنوات عبر الإنترنت، بالإضافة الى أنه يستخدم كشفًا متقدمًا وقابلا لتفسير الاحتيال، لتمكين المؤسسات المالية من تحديد المخاطر تلقائيًا واكتشاف هجمات الاحتيال الجديدة، وتحديد الأنشطة المشبوهة في الوقت الفعلي. تستخدم أكثر من 30 مؤسسة مالية عالمية كبرى شركة ARIC لحماية أعمالها وعملائها(Michael Touchton, 2023) .

4. تقييم تجربة بنك Danske في محاربة الاحتيال بواسطة الذكاء الاصطناعي

أدت صناعة الخدمات المصرفية والدفع المتطورة إلى تسريع الحركة المصرفية، مما مكن المزيد من المستخدمين من الوصول إلى الخدمات المالية. الآن، التوجه سيكون نحو "موجة جديدة من الشمول المالي الرقمي" حيث يبدأ فيها المستخدمون في الاستفادة بشكل كامل من الخدمات المصرفية الرقمية. وفي هذا السيناريو الجديد، يؤدي الارتفاع المفاجئ في عمليات الاحتيال إلى عكس الجهود الأخيرة في جلب الفئات المستبعدة سابقًا إلى الاقتصاد الرقمي، وفي دراسة لبنك Danske الذي شمل أكثر من خمسة ملايين عميل حول محاولته في القضاء على الاحتيال فقام بأداء دور رئيسي في زيادة هذا الشمول باستخدام البرامج الإلكترونية المعتمدة على تطبيقات الذكاء الاصطناعي (Arvid O.I. Hoffmann, Cornelia Birnbrich, 2012, P 5).

كان بنك Danske الدنماركي يلتقط 1200 نتيجة إيجابية كاذبة يوميًا (بمعنى يوجد حالات احتيال) ولكن 99.5٪ منها كانت إيجابية كاذبة، وفي تصريح آخر Nadim Golzer رئيس التحليلات العالمية في البنك: "غالبًا ما يمكن حل المشكلة في بضع دقائق بواسطة محقق، ولكن حتى دقيقة أو دقيقتين على 1200 معاملة يعد كثيرا من الوقت الضائع. وفي بعض الأحيان يمكن للمحقق فقط إلقاء نظرة على البيانات ومسحها، بينما يمكن الموافقة على المدفوعات الأخرى عن طريق التحقق من التفاصيل مثل التاجر أو مبلغ الدفع" (Doug Henschen، 2023).

وبعد أن قرر البنك العمل مع Think Big Analytics، من شركة Teradata قام بإنشاء برامج لمكافحة الاحتيال، وباستخدام التعلم الآلي تمكنوا من تقليل الإيجابيات الزائفة بنسبة 35%، وتحسين اكتشاف الإيجابيات الحقيقية، أي الاحتيال الفعلي بنفس النسبة تقريبًا. وعندما أضافوا التعلم العميق، تضاعفت الأرقام تقريبًا لتصل إلى نسبة 60 % من الإيجابيات الكاذبة وتحسن بنسبة 50% في الكشف عن الاحتيال الفعلي. ومع تقليل الإيجابيات الكاذبة، يمكن للمحققين التركيز على القضايا الأخرى الأكثر أهمية، أي توفير الوقت والجهد والأمان لكل الأطراف (Doug Henschen، 2023).

قد يكون لدى العملاء انطباع بأن "البنك ليس مكانًا آمنًا وغير قادر على حماية أصول عملائه". فيفقدون الثقة ويصبحون غير راضين، وقد يتحولون إلى مزود خدمات مالية مختلف. ويمكن أن يكون لحوادث الاحتيال المتراكمة تأثير سلبي عميق على سمعة البنك بعدة طرق، تعد الإدارة الاستباقية للاحتيال فرصة للبنوك (لإعادة) تأكيد ثقة العملاء، وقد تكون وسيلة للاحتفاظ بالعملاء

الحاليين وجذب عملاء جدد (Arvid O.I. Hoffmann, Cornelia Birnbrich, 2012).

فمثلا وصلت درجة الشمول المالي الرقمي في بنك Danske حتى إلى الأطفال الذين تتراوح أعمارهم بين 8 و14 عامًا، وذلك بفضل التطبيق الرقمي Pocket Money والذي يُعد حلا رقميا لمساعدة الآباء والأطفال على تتبع الأموال. وهي تتألف من تطبيق في الهاتف المحمول للآباء وبطاقة مصروف جيب للأطفال، ويمكن للأطفال معرفة متى يتم دفع مصروفهم إلى حسابهم وكيف تتطور مدخراتهم. (Danske Bank Fights Fraud with Deep Learning and AI, 2023)

من جهة أخرى، إن الأشخاص والنساء من ذوي الدخل المنخفض، ولاسيما الذين ليست لديهم خبرة في التعاملات الرقمية هم الأكثر عرضة للاحتيال، حيث تمكن المحتالون من الاستفادة من هذه المجموعات إلى حد كبير بسبب انخفاض مستويات تعليمهم المالي. وفي هذا السياق شدد المتحدثون على الحاجة إلى تحسين التعليم لمواكبة الثورة الرقمية، في النهاية إذا لم نخفف من مخاطر الاحتيال، فإننا نجازف بإبطاء عجلة الشمول المالي الرقمي (Shabtai Gold، 2023).

يعتقد Danske أن البنك يجب أن يحمي العميل أحيانًا ضد الإهمال أو الجهل. ربما يستخدمون جهاز هاتف أو كمبيوتر شخصي، لكنهم لا يفهمون كيفية حماية أنفسهم، ففي بعض الأحيان يكون سلوك المستخدم بمثابة هدية للمحتال، ولهذا يقوم بتقديم استشارات ونصائح لإرشاد المستخدمين على الطرق الصحيحة لتقليل فرص الاحتيال عليهم. على سبيل المثال لدى البنك بيانات توضح مدى سرعة قيام العميل بتعبئة النموذج، وإذا كانت السرعة المعتادة أسرع بأربع مرات، فمن المحتمل ألا يكون العميل". ومنه تبحث Danske في قياس سرعات حركة الماوس، وستتمكن قريبًا من تحديد الأشخاص والمصادقة عليهم من خلال أنماط الكتابة الخاصة بهم، وبهذا تفرق بين العميل الحقيقي والمحتال. من المتوقع أن تحقق منصة الكشف عن الاحتيال في البنك عائد استثمار بنسبة 100 % في عامها الأول من الإنتاج (Doug Henschen، 2023)

الخاتمة:

إن مكافحة الاحتيال بشكل صحيح هو حجر الزاوية في المساعدة على رفع درجة الوصول المالي، حيث إن سمات الخدمة، مثل منع الاحتيال، يمكن أن تؤثر بشكل إيجابي على استمرار العلاقة والمعاملات المتبادلة. فمن خلال إظهار معرفتها ودرايتها بمنع الاحتيال، يمكن للبنوك أن تخلق شعورًا بالأمان، ومن ثم تحسين جودة هذه العلاقة، مما قد يؤدي في النهاية إلى تحسين ولاء العملاء. فالنظرة الإيجابية لعميل واحد، يمكن أن تقدمنا خطوة أخرى نحو هدف تحقيق شمول مالي يتبعه شمول مالي رقمي أوسع.

ومن خلال عرض تجربة بنك Danske في محاربة الاحتيال بواسطة تطبيق الذكاء الاصطناعي يمكن أن نصل إلى أن تطبيق كشف الاحتيال والأمن السيبراني المعتمد على الذكاء الاصطناعي في بنك Danske، يساهم في الكشف عن نسبة 50 % من الاحتيال الفعلي واضعا به حجر الأساس من أجل المساعدة على رفع درجة الوصول المالي الرقمي، من خلال خلق شعور بالأمان عن طريق حمايته لأموال الفئات عديمة الخبرة مع التكنولوجيا، والتي كانت سابقا هدفا للمحتالين. ومن جهة أخرى اكتسب شهرة وسمعة فريدة وواسعة تدفع المتخوفين من الاحتيال الرقمي في البنوك إلى الإقبال عليه، ومن ثم تحسين العلاقة بين العميل وبنكه، **وهو ما يؤكد صحة الفرضية المطروحة.**

اقتراحات الدراسة:

بناءً على نتائج الدراسة يمكن أن نقترح توصيات، والتي توجه بالدرجة الأولى إلى القائمين على تطوير الخدمات المصرفية في الجزائر:

- توفير البنية التحتية، كوضع إطار تشريعي للخدمات المالية الرقمية، بما يوضح جميع الالتزامات الواجب احترامها من البنوك الجزائرية وعملائها.
- تدريب موظفي البنوك ونشر ثقافة الخدمات المصرفية الرقمية المعتمدة على تطبيقات الذكاء الاصطناعي لدى العملاء.
- توعية البنوك والمؤسسات المالية الجزائرية على ضرورة استخدام تطبيقات الذكاء الاصطناعي في خدماتها المالية، فحتى مع وجود بعض القنوات الإلكترونية كالصرافات الآلية، إلا أننا لا نزال متأخرين جدا بالمقارنة مع الدول الرائدة في هذا المجال.
- تخصيص غطاء مالي يسمح بشراء هذه التطبيقات لاستخدامها من قبل المؤسسات، لما سيكون لها من عائد إيجابي على هذه المؤسسات.

- الاهتمام بعملية التدريب للموظفين على استخدام هذه التطبيقات بهدف التخلي عن القدرات الذهنية الأجنبية.
- تشجيع البحث العلمي في هذا المجال، وإقامة مراكز أبحاث مهيأة بغرض تنمية الكفاءات المحلية والاستفادة منها قدر الإمكان.

قائمة المراجع

1. البنك المركزي السعودي. (15 04, 2023). *المخاطر السيبرانية*. تم الاسترداد من https://www.sama.gov.sa
2. الذكاء الاصطناعي. (15 04, 2023). *فصل جديد للأمن السيبراني*. تم الاسترداد من https://www.tripwire.com
3. أوستاب زابولوتني. (15 04, 2023). *الذكاء الاصطناعي في الإقراض*. تم الاسترداد من https://firstbridge.io
4. تغريد ابراهيم. (10 04, 2023). *Danske Bank A/S*. تم الاسترداد من https://www.marefa.org
5. سعيدة صبري" .(2021) .تبني الذكاء الاصطناعي في شركات التأمين كآلية لتعزيز الشمول المالي –دراسة حالة شركة أكسا ."–المجلة الجزائرية لاقتصاد الإدارة، المجلد 15، العدد 01.
6. فايز الشهري. (14 04, 2023). تحديات الذكاء الاصطناعي الخمسة، الرياض، السعودية. تم الاسترداد من https://elaph.com/Web
7. Amazon Web Services من الاسترداد تم .*السيبراني بالأمن المقصود ما*. (14 04, 2023) https://aws.amazon.com/
8. Ananya Azad. (2023, 03 05). *8 ways chatbots in banking can improve customer engagement*. Récupéré sur https://www.engati.com/
9. Arvid O.I. Hoffmann, Cornelia Birnbrich. (2012, 04 19). "The impact of fraud prevention on bank-customer relationships",. *International Journal of Bank, Vol 30 No 5*.
10. Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real. (2023, 04 11). Récupéré sur https://www.teradata.com/
11. Danske Bank Fights Fraud with Deep Learning and AI,. (2023, 04 09). *ARTIFICIAL INTELLIGENCE / CASE STUDY*. Récupéré sur https://assets.teradata.com/
12. Dmitry Dolgorukov. (2023, 04 15). *How AI can support inclusive lending*. Récupéré sur https://www.bai.org

13. Doug Henschen. (2023, 04 09). *CASE STUDY: TERADATA THINK BIG ANALYTICS AND DANSKE BANK, Danske Bank Fights Fraud with Machine Learning and AI*. Récupéré sur https://www.constellationr.com/
14. Doug Henschen, CASE STUDY. (s.d.). *TERADATA THINK BIG ANALYTICS AND DANSKE BANK, Danske Bank Fights Fraud with Machine Learning and AI*. Récupéré sur https://www.constellationr.com/
15. Emily Cummins. (2023, 03 05). *The 10 Best Banking Chatbots (And How Your Financial Institution Can Use Them, Too)*. Récupéré sur https://www.netomi.com/banking-chatbots
16. Goals of Artificial Intelligence. (2023, 04 13). Récupéré sur https://www.javatpoint.com
17. Helena Franco. (2023, 03 05). *"Chatbots in Banking: The New Must-Have in Customer Care"*. Récupéré sur https://www.inbenta.com/
18. Henry Vilar. (2023, 04 09). *Featurespace foils fraud for Danske Bank*. Récupéré sur https://www.fintechfutures.com/
19. Massimiliano Aschi, Susanna Bonura, Nicola Masi, Domenico Messina, Davide Profeta. (2023, 03 04). *Big Data and Artificial Intelligence in Digital*. Récupéré sur https://link.springer.com
20. Michael Touchton. (2023, 04 09). *Danske Bank boosts fraud prevention with Featurespace ARIC "Risk Hub News"*. Récupéré sur https://www.featurespace.com
21. Ryan Williamson. (2023, 04 10). *Benefits of AI to Fight Fraud in the Banking System*. Récupéré sur https://www.datasciencecentral.com
22. Saurabh Singh. (2023, 03 04). *AI in Banking – article How Artificial Intelligence is Used in Banks*. Récupéré sur https://appinventiv.com/blog/
23. Shambhavi Sin. (2023, 03 05). *Chatbot for Banking: Everything you Need to Know*. Récupéré sur https://www.ameyo.com/,
24. Top 10 Characteristics of Artificial Intelligence. (2023, 02 26). Récupéré sur https://www.interviewbit.com
25. *Top 5 Benefits of Artificial Intelligence in Banking and Finance*. (2023, 02 10). Récupéré sur actico.com/blog-en/
26. Top 7 Artificial Intelligence Characteristics with Examples. (2023, 04 13). Récupéré sur https://techvidvan.com
27. Using Artificial Intelligence in Cybersecurity. (2023, 04 15). Récupéré sur https://www.balbix.com/
28. Vijaykanade. (2023, 02 10). *"What Is Artificial Intelligence (AI) Definition, Types, Goals, Challenges, and Trends in 2022"*. Récupéré sur spiceworks: https://www.spiceworks.com/