Warith Scientific Journal

مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي بأستخدام الامن السيبراني: بنك Danske الدمناركي أنموذجا

Contribution of Artificial Intelligence to Detecting Fraud in the Banking Sector Using Cybersecurity: Danske Bank as a Model

م.م علي اياد علي الحمزة
Ali Ayad Ali AL Hamza
La5048628@gmail.com
كلية الإدارة والاقتصاد – جامعة وارث الانبياء
Faculty of Management and Economics - Warith Al-Anbiya University

المستخلص:
تهدف هذه الدراسة إلى تسليط الضوء على دور الذكاء الاصطناعي في تعزيز الكشف عن الاحتيال في القطاع المصرفي من خلال تطبيقات الأمن السيبراني. وتستند إلى فرضية أن الأدوات المالية الرقمية، مثل الأمن السيبراني، تسهم في توسيع قدرة المؤسسات المصرفية على رصد الاحتيالات من خلال تحليل كميات كبيرة من البيانات بشكل فعال وفي الوقت المناسب. يمكن هذا التحليل المؤسسات المالية من تحديد الأنماط والاتجاهات التي يصعب اكتشافها يدويًا. لتحقيق أهداف الدراسة، تم استخدام المنهج الوصفي التحليلي مع دراسة حالة لتجربة بنك Danske الدنماركي. أظهرت النتائج أن استخدام تقنيات الذكاء الاصطناعي للكشف عن الاحتيال في البنك ساعد في اكتشاف حوالي 50% من حالات الاحتيال الفعلي، مما يشكل أساسًا قويًا لرفع مستوى الأمان المالي الرقمي.
الكلمات المفتاحية: الذكاء الاصطناعي، كشف الاحتيال، الأمن السيبراني، بنك.Danske

Abstract:
This study aims to highlight the role of artificial intelligence in enhancing fraud detection in the banking sector through cybersecurity applications. It is based on the hypothesis that digital financial tools, such as cybersecurity, contribute to expanding the ability of banking institutions to detect fraud by analyzing large amounts of data effectively and in a timely manner. This analysis enables financial institutions to identify patterns and trends that are difficult to detect manually. To achieve the objectives of the study, the descriptive analytical approach was used with a case study of the Danish Danske Bank experience. The results showed that the use of artificial intelligence techniques to detect fraud in the bank helped detect about 50% of actual fraud cases, which constitutes a strong basis for raising the level of digital financial security.
Keywords: Artificial intelligence, fraud detection, cybersecurity, Danske Bank.

1. المقدمة :

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 تسخر 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 تخصيصا 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 يمكن 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 يمكن المؤسسات المصرفية من تحديد الأنماط والاتجاهات التي سيكون من المستحيل اكتشافها يدويا.

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

فيما يتعلق بالدراسات السابقة التي تناولتها الوثيقة، فقد تم ذكر العديد من الدراسات التي توضح مساهمة الذكاء الاصطناعي في مجالات مختلفة من الشمول المالي والكشف عن الاحتيال. وهنا ملخص لبعض الدراسات البارزة:

الدراسات السابقة:

1. The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion

- المؤلف: David Mhlanga

- الجامعة: 2006School of Accounting, University of Johannesburg,

هدفت هذه الدراسة إلى التحقيق في تأثير تطبيقات الذكاء الاصطناعي، بما في ذلك روبوتات الدردشة، على الشمول المالي الرقمي. اعتمدت الدراسة على التحليل المفاهيمي والوثائقي للمجلات والتقارير لتقييم تأثير هذه التطبيقات, وأكدت الدراسة أن للذكاء الاصطناعي تأثيرًا قويًا في الشمول المالي الرقمي، خاصة في مجالات اكتشاف المخاطر، معالجة عدم تناسق المعلومات، وتقديم المساعدة من خلال روبوتات الدردشة. كما يساهم في كشف الاحتيال وتعزيز الأمن السيبراني. أوصت الدراسة بتبني المؤسسات المالية والحكومات لتطبيقات الذكاء الاصطناعي بهدف إشراك الفئات المهمشة في السوق المالية الرسمية مع مواجهة تحديات محدودة.

2. The Role of Artificial Intelligence in Financial Inclusion in Developing Countries

- المؤلف: Kshetri Nir

- المجلة: 2021Journal of Global Information Technology Management,

هدفت الدراسة إلى معرفة مدى مساهمة تطبيقات الذكاء الاصطناعي، مثل روبوتات الدردشة، في تعزيز الشمول المالي الرقمي في البلدان النامية, وأثبتت الدراسة قدرة الذكاء الاصطناعي على تعزيز الشمول المالي من خلال تحليل ومعالجة البيانات بشكل يفوق قدرة العنصر البشري، مما يؤدي إلى تحسين كفاءة المؤسسات المالية وزيادة قاعدة العملاء.

3. Big Data and Artificial Intelligence for Financial Inclusion: Benefits and Issues

- السنة: 2021

ناقشت الدراسة فوائد وتحديات استخدام البيانات الضخمة والذكاء الاصطناعي لتحقيق الشمول المالي, وتوصلت الدراسة إلى أن هذه التقنيات تساهم في تحسين الكفاءة وإدارة المخاطر، وتقديم منتجات وخدمات مالية ذكية للبالغين المتعاملين مع البنوك. كما تساعد في تبسيط عملية فتح الحساب للبالغين الذين لا يتعاملون مع البنوك وتوفير درجات ائتمانية باستخدام معلومات بديلة. ومع ذلك، تناولت الدراسة أيضًا تحديات مثل نقص الكفاءات في مجال الذكاء الاصطناعي، زيادة البطالة، التحيز اللاواعي في تصميم الأنظمة، والقوانين الصارمة المتعلقة بخصوصية البيانات.

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 عام يشمل مجموعة متقدمة من التقنيات التي تطورت بشكل ملحوظ خلال العقود الأخيرة. نظرًا لتنوع استخداماته، لا يوجد تعريف موحد ينطبق على جميع السياقات. يُعتبر الذكاء الاصطناعي فرعًا من علوم الحاسب يركز على محاكاة السلوك الذكي في الآلات، مما يمكنها من تقليد تصرفات البشر. وفقًا لسعيدة صبري (2021)، يشير الذكاء الاصطناعي إلى قدرة الآلة على تنفيذ مهام تتطلب عادةً ذكاءً بشريًا، مما يعكس قدرة الآلات على التعلم والتكيف مع بيئات جديدة.

من جهة أخرى، يعرف Vijaykanade (2023) الذكاء الاصطناعي بأنه "ذكاء الآلات أو الكمبيوتر الذي يمكّنها من محاكاة القدرات البشرية". أما جون مكارثي، الذي يُعتبر أحد مؤسسي هذا المجال، فقد عرّف الذكاء الاصطناعي بأنه "علم وهندسة إنشاء آلات ذكية، وخاصة البرامج التي تُظهر سلوكًا ذكيًا". وفقًا له، يسعى الذكاء الاصطناعي إلى إدخال الذكاء في الآلات بحيث تستطيع العمل والتفاعل كما يفعل البشر، مما يُساعد في اتخاذ القرارات بناءً على سيناريوهات حقيقية, وتتضمن خصائص الذكاء الاصطناعي القدرة على التعلم من البيانات، والقدرة على التكيف مع التغيرات في البيئة، وفهم اللغة الطبيعية، وتحليل الصور، فضلاً عن القدرة على التفاعل مع البشر بطريقة طبيعية. يُظهر الذكاء الاصطناعي أيضًا القدرة على القيام بمهام معقدة، مثل قيادة السيارات، والمساعدة في التشخيص الطبي، وإدارة المخاطر المالية، مما يعكس تأثيره المتزايد في مختلف مجالات الحياة اليومية. (alshahry، 2023:. 79).

في السنوات الأخيرة، أصبحت تطبيقات الذكاء الاصطناعي جزءًا لا يتجزأ من الصناعات المختلفة، بما في ذلك الرعاية الصحية، والتجارة، والأمن السيبراني، مما يعزز من فعالية العمليات ويساهم في تحسين تجربة المستخدمين. ومع استمرار التقدم في هذا المجال، يُتوقع أن تلعب تقنيات الذكاء الاصطناعي دورًا محوريًا في تشكيل مستقبل العديد من الصناعات، مما يفتح آفاقًا جديدة للتطوير والابتكار.

2. خصائص وأهداف الذكاء الاصطناعي

1. خصائص الذكاء الاصطناعي

تطورت تقنيات الذكاء الاصطناعي بشكل ملحوظ منذ بدايتها، ولها عدة خصائص تميزها، ومنها: (artificial intelligence ، 2023:. 34).

1. التعلم العميق: يُعتبر التعلم العميق تقنية متقدمة في مجال التعلم الآلي، حيث يُمكّن الأجهزة من القيام بمهام تُعتبر طبيعية للبشر. على سبيل المثال، تُستخدم هذه التقنية في السيارات ذاتية القيادة مثل Tesla، حيث تساعدها على التعرف على إشارات المرور والتمييز بين المشاة والعوائق الأخرى.

2. التعرف على الوجه: يسهم الذكاء الاصطناعي في تقنيات التعرف على الوجوه، مما أدى إلى تطورات مهمة في مجالات المراقبة. تقوم هذه الأنظمة بمقارنة الوجوه مع قاعدة بيانات معروفة للبحث عن تطابق، لكن هذا الاستخدام واجه انتقادات تتعلق بخصوصية الأفراد.

3. أتمتة المهام: يُمكن الذكاء الاصطناعي من أتمتة المهام البسيطة والمتكررة بشكل فعال. مثلاً، يمكن للمساعد الصوتي مثل Siri تنفيذ مجموعة متنوعة من الأوامر اليومية، من تدوين الملاحظات إلى إدارة الجدول الزمني.

4. استيعاب البيانات: يساهم الذكاء الاصطناعي في معالجة كميات هائلة من البيانات بشكل سريع. بدلاً من إدخال البيانات يدويًا، يتمكن الذكاء الاصطناعي من جمع وتحليل المعلومات من مصادر متعددة باستخدام خبراته السابقة، مما يعزز من قدرته على اتخاذ قرارات مستندة إلى تحليل دقيق.

5. روبوتات المحادثة: تعمل روبوتات المحادثة كأداة لحل مشكلات العملاء، حيث تُقدم الدعم من خلال الإدخال الصوتي أو النصي. العديد من الشركات انتقلت من استخدام موظفين بشريين إلى هذه الأنظمة التلقائية لمساعدتهم في تقديم حلول فورية وتوصيات للمنتجات.

تظهر هذه الخصائص كيف يمكن للذكاء الاصطناعي تعزيز الكفاءة وتحسين تجربة المستخدمين في مختلف المجالات، مما يؤدي إلى إحداث تغييرات جذرية في طريقة تفاعل الأفراد مع التكنولوجيا.

2.2. أهداف الذكاء الاصطناعي

بشكل عام، يتمثل الهدف الرئيسي للذكاء الاصطناعي في تصميم خوارزميات تُنتج النتائج المرغوبة. ومن بين الأهداف الأخرى التي يسعى الذكاء الاصطناعي لتحقيقها: (sabry، 2021: 45).

1. حل المشكلات: يُساعد الذكاء الاصطناعي في تسهيل حياتنا من خلال تطوير خوارزميات فعالة لحل المشكلات، حيث يمكنها إجراء استنتاجات منطقية ومحاكاة التفكير البشري، كما في أنظمة التنبؤ بسوق الأوراق المالية.

2. تمثيل المعرفة: يتعلق هذا الجانب بتمثيل "المعلومات المعروفة" للآلات باستخدام مجموعة من المفاهيم والعلاقات. يُظهر هذا التمثيل معلومات من العالم الحقيقي التي يستفيد منها الكمبيوتر لحل مشكلات معقدة، مثل تشخيص الأمراض أو التفاعل مع البشر بلغة طبيعية.

3. التخطيط: يُمكن الذكاء الاصطناعي من إجراء تنبؤات حول المستقبل وتأكيد نتائج أفعالنا، ويتم استخدام التخطيط في مجالات مثل إدارة المخاطر والأمن السيبراني.
4. التعلم: يشمل التعلم الآلي دراسة خوارزميات الكمبيوتر التي تتحسن تلقائيًا من خلال التجربة. فنيًا، تعالج برامج الذكاء الاصطناعي مجموعة من المدخلات والمخرجات لوظيفة معينة، وتستخدم النتائج المتحصلة للتنبؤ بنتائج جديدة.
5. الذكاء الاجتماعي: يركز هذا الجانب على تطوير الأنظمة القادرة على تفسير ومعالجة ومحاكاة السلوك البشري، بما في ذلك قراءة تعابير الوجه ولغة الجسد ونغمات الصوت. تتيح هذه الأنظمة للذكاء الاصطناعي التفاعل والتواصل بشكل يشبه الإنسان.
6. الإبداع: يمكن للذكاء الاصطناعي معالجة كميات ضخمة من البيانات، والنظر في الخيارات المتاحة، وتطوير فرص إبداعية. على سبيل المثال، يمكن لنظام الذكاء الاصطناعي تقديم خيارات متعددة لتصميم داخلي لشقة ثلاثية الأبعاد.
7. الذكاء العام: يهدف الباحثون في مجال الذكاء الاصطناعي إلى تطوير آلات تتمتع بقدرات عامة تجمع بين جميع المهارات المعرفية للبشر، مما يمكنها من أداء المهام بكفاءة تفوق كفاءة البشر، مثل نزع فتيل القنابل، مما يحرر البشر من المهام الخطرة.
تساهم هذه الأهداف في تعزيز قدرة الذكاء الاصطناعي على تحسين حياتنا وتسهيل العديد من المهام المعقدة.

3. أهم تطبيقات الذكاء الاصطناعي في البنوك

أحدثت تطبيقات الذكاء الاصطناعي تحولًا جذريًا في القطاع المالي والمصرفي، حيث ساعدت على تحسين كفاءة وجودة الخدمات المالية التقليدية، مما أدى إلى جعلها أكثر ابتكارًا وفاعلية وتنوعًا. فيما يلي بعض التطبيقات الرئيسية للذكاء الاصطناعي في الصناعة المصرفية: (alshahry، 2023: 22).

1. تطبيق روبوت الدردشة - Chatbot -

مع بداية جائحة كورونا، شهدت الصناعة المالية زيادة ملحوظة في التوجه نحو المعاملات الرقمية، مما دفع البنوك إلى تقليل الاعتماد على الموظفين واستخدام روبوتات الدردشة. تتكون كلمة "Chatbot" من كلمتين: "شات" (الدردشة) و"بوت" (روبوت)، وهي برامج مصممة لمحاكاة المحادثات باستخدام اللغة الطبيعية. (artificial intelligence ، 2023. 55).
روبوتات الدردشة الخاصة بالخدمات المصرفية هي عبارة عن أدوات تفاعلية تستخدمها البنوك لتحسين تجربة العملاء عبر مختلف منصات الخدمات المصرفية الرقمية. تُسهم هذه الروبوتات في تعزيز تفاعل العملاء وتسهيل العمليات، مما يجعل الوصول إلى الخدمات المصرفية أكثر سهولة في الوقت الراهن. حيث يمكن لهذه الروبوتات القيام بمهام كانت تتطلب التفاعل مع موظفين بشريين في الفروع أو عبر الهاتف، مثل توفير الدعم للعميل من خلال واجهة محادثة مع مساعدين افتراضيين.
استخدامات روبوتات الدردشة في البنوك تتضمن ما يلي: (Amazon Web Services، 2023: 11).
- **تحويل الأموال:** يمكن للمستخدمين استخدام روبوتات الدردشة لإجراء المدفوعات، وتعيين المدفوعات أو إلغائها، وتتبع المعاملات المالية، ودفع فواتير بطاقات الائتمان.
- **الإجابة عن الأسئلة الأساسية:** تستطيع الروبوتات الرد على استفسارات مثل "كيف يمكنني التقدم بطلب للحصول على بطاقة ائتمان؟".
- **توفير الإخطارات والتذكيرات في الوقت المناسب:** تعتمد معظم البنوك على روبوتات الدردشة لإرسال تذكيرات وإشعارات منتظمة للعملاء حول حساباتهم المصرفية، مثل مواعيد دفع الفواتير أو عرض القروض.
- **التحقق من رصيد الحساب:** يمكن للمستخدمين الاستفسار عن رصيد حساباتهم، بالإضافة إلى تلقي تنبيهات إذا كان الرصيد منخفضًا.
- **تقديم تفاصيل الحساب كاملة:** بإمكان المستخدمين سؤال الروبوتات عن معلومات إضافية تتعلق بحساباتهم، مثل المدفوعات والنفقات المتكررة وحدود التحويلات، وكذلك إجراء تغييرات مثل تحديث البيانات الشخصية.
- **تتبع الموقع في الوقت الحقيقي:** يمكن لروبوتات الدردشة استخدام GPS لتوفير إجابات دقيقة بناءً على الموقع.
- **حل القضايا العاجلة:** تشمل هذه القضايا مثل فتح أو إغلاق البطاقات، إعادة تعيين كلمات المرور، والتحقق من كشوف الحسابات.
من أبرز الأمثلة على روبوتات الدردشة في المجال المصرفي هو "Erica"، المساعد الافتراضي من بنك أمريكا، الذي أدار أكثر من 50 مليون طلب من العملاء خلال عام 2019.
تُعد هذه التطبيقات جزءًا من اتجاه أوسع نحو تحسين الخدمات المصرفية وتقديم تجارب أفضل للعملاء باستخدام تقنيات الذكاء الاصطناعي.

2.3. تطبيق الأمن السيبراني وكشف الاحتيال

مع تزايد عدد المعاملات الرقمية يوميًا، مثل دفع الفواتير وسحب الأموال وإيداع الشيكات عبر التطبيقات أو الحسابات عبر الإنترنت، تبرز الحاجة المتزايدة في القطاع المصرفي لتعزيز جهود الأمن السيبراني وكشف الاحتيال. سيتناول هذا العنصر من الدراسة تفاصيل هذا التطبيق وأهميته في حماية البيانات والمعاملات المالية.

3.3. تطبيق الإقراض

يعتبر الإقراض المدعوم بتقنيات الذكاء الاصطناعي من الفوائد الكبيرة لجميع الأطراف المعنية. بالنسبة للمقرضين، يُعتبر هذا النظام أداة تسويقية فعالة ويساعدهم في التنافس مع البنوك بتكاليف منخفضة. ومن جهة أخرى، يُمكن المقترضين، خصوصًا أولئك الذين لديهم سجلات ائتمانية ضعيفة أو لا يمتلكون تاريخًا ائتمانيًا، من الحصول على فرص تمويل ملائمة وبأسعار مناسبة في فترة زمنية قصيرة,

ولكن يُشير بعض منتقدي استخدام الذكاء الاصطناعي إلى أهمية جودة البيانات المستخدمة في هذه الأنظمة، محذرين من إمكانية التحيز إذا اعتمدت الخوارزميات على بيانات غير دقيقة أو عملت في بيئات تفتقر إلى المعلومات اللازمة، مثل المناطق ذات التنافس المنخفض أو سلوك التسوق الضعيف. وقد يحدث هذا التحدي في المجتمعات التي تعاني من نقص في الخدمات المصرفية. (ibraheem، 2023. 85).

اتجاهات اعتماد الذكاء الاصطناعي في الإقراض تشمل:.(Williamson2023 ،48.)

- **تقليل وقت دورة الإقراض:** باستخدام تقنيات الذكاء الاصطناعي، يمكن للمقرضين تقليل الوقت اللازم لمعالجة طلبات القروض من أسابيع إلى ساعات. حيث تتطلب المراحل الأولية معالجة الوثائق، وهو ما يستغرق وقتًا طويلاً.
- **توافر البيانات لتحسين اتخاذ القرارات الائتمانية:** أصبحت أنظمة اتخاذ القرارات الائتمانية المؤتمتة ممكنة بفضل حلول الذكاء الاصطناعي، مما يقلل من الوقت اللازم لتقييم الوضع المالي للمتقدمين.
- **التعامل مع حجم كبير من طلبات القروض:** تُساعد نماذج الذكاء الاصطناعي البنوك ومؤسسات الإقراض في تحسين الدقة، خاصة عند معالجة طلبات القروض بكميات كبيرة.
- **استخدام البيانات الرقمية في معالجة القروض:** يحل الإقراض الآلي والعمليات المدعومة بالذكاء الاصطناعي محل العمليات اليدوية، مما يضمن إجراءات سلسة في الموافقة على القروض وصرفها.

تُظهر هذه التطبيقات كيف يُمكن للذكاء الاصطناعي أن يُحدث فرقًا جوهريًا في تحسين عمليات الإقراض وتسهيل الوصول إلى التمويل.

4. فوائد وتحديات الذكاء الاصطناعي في الصناعة المصرفية

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

4. 1. فوائد الذكاء الاصطناعي في القطاع المصرفي

تتضمن فوائد الذكاء الاصطناعي في الصناعة المالية والمصرفية ما يلي: (Azad، 2023 .:15).

- **الامتثال التنظيمي وكشف الاحتيال:** مع زيادة يقظة المؤسسات المالية، تتكيف أساليب المحتالين، ولكن أنظمة كشف الاحتيال المعتمدة على الذكاء الاصطناعي يمكنها الكشف عن النشاط الإجرامي بشكل فوري. حيث تتيح هذه الأنظمة تحليل كميات هائلة من البيانات لاكتشاف المعاملات المشبوهة بسرعة وفعالية.
- **تجربة أفضل للعملاء:** يسعى العملاء دائمًا لتحقيق أقصى درجات الراحة. وقد أدت الابتكارات مثل أجهزة الصراف الآلي إلى إمكانية الوصول إلى الخدمات المصرفية خارج ساعات العمل التقليدية. الآن، يمكن للعملاء فتح حسابات والتحقق من هويتهم عبر هواتفهم الذكية، مما يعزز من تجربة العميل ويزيد من الرضا.
- **تخفيض تكاليف التشغيل والمخاطر:** رغم أن التفاعل البشري له مزاياه، إلا أنه يحمل عيوبًا، مثل الأخطاء البشرية التي يمكن أن تضر بالسمعة وتعرض المؤسسة للمسؤولية. أنظمة الذكاء الاصطناعي تقلل من هذه المخاطر من خلال استخدام تقنيات تنبؤية وتعليمية تعمل على تحسين العمليات التجارية وتخفيف الأخطاء.
- **تحسين تقييم القروض والتسهيلات:** يمكن للأنظمة المعتمدة على الذكاء الاصطناعي تقديم توصيات دقيقة بشأن الموافقة أو الرفض للقروض من خلال تحليل عدد أكبر من المتغيرات، حتى في حالة عدم وجود الكثير من الوثائق لدى المتقدمين.

تُظهر هذه الفوائد كيف يُمكن للذكاء الاصطناعي أن يُساهم في تحسين كفاءة الخدمات المصرفية وتعزيز التجربة العامة للعملاء، بينما يسعى المصرفيون إلى تحقيق التوازن بين الابتكار واحتياجات الأمان.

2.4. التحديات الرئيسية للذكاء الاصطناعي

يمثل الذكاء الاصطناعي تقنية ناشئة، خصوصًا في القطاع المصرفي، حيث يتعين على المؤسسات المالية التوازن بين فوائد هذه التقنية ومخاطرها والتحديات المرتبطة بها. (Azad، 2023 .74).

1. التحديات القانونية المحفوفة بالخطر

تعتبر مسؤوليات الذكاء الاصطناعي في اتخاذ القرارات محورًا للنقاش. يتعين تحديد من يتحمل المسؤولية القانونية عند حدوث أخطاء ناتجة عن قرارات الذكاء الاصطناعي، سواء في مجالات الرعاية الصحية أو الأجهزة أو المركبات ذاتية القيادة. من بين القضايا المطروحة: كيف يمكن التصدي لمشاكل انتهاك الخصوصية والتحيز، إضافة إلى اتخاذ قرارات قد لا يمكن الطعن فيها.

2. الخوف من تأثير الذكاء الاصطناعي على الوظائف

هناك مخاوف من أن يؤدي انتشار تطبيقات الذكاء الاصطناعي إلى زيادة معدلات فقدان الوظائف. على سبيل المثال، الروبوتات، التي تمثل إحدى تطبيقات الذكاء الاصطناعي، بدأت تُستخدم بشكل متزايد في المصانع ونقاط التوزيع، مما قد يؤثر سلبًا على معدلات البطالة في هذه القطاعات. تشير دراسات معهد ماكينزي إلى أن الروبوتات قد تحل محل حوالي 30% من العمالة البشرية بحلول عام 2030.

3. خروج الذكاء الاصطناعي عن السيطرة البشرية

يُحذر بعض العلماء مثل ستيفن هوكينغ من إمكانية أن يصبح الذكاء الاصطناعي قادرًا على تصميم ذكاء اصطناعي متفوق على قدرة المبرمجين البشر. كما أشار إيلون ماسك إلى أن الذكاء الاصطناعي قد يشكل أكبر تهديد وجودي للبشرية، حيث تتزايد المخاوف من تفرد الذكاء الاصطناعي وقدرته على النمو بشكل غير قابل للتحكم.

4. التكلفة العالية لبناء منظومات الذكاء الاصطناعي

يتطلب إنشاء أنظمة الذكاء الاصطناعي موارد كبيرة من الوقت والمال، مما يجعلها مكلفة للدول غير القادرة على تحمل هذه التكاليف. هذه الفجوة في التكلفة قد تعمق الفجوة بين الدول الغنية والفقيرة، حيث ستكون الدول الغنية أكثر قدرة على تطوير واستخدام هذه التقنية.

5. إدمان استخدامات الذكاء الاصطناعي

يمكن أن يؤدي الإدمان على استخدام الذكاء الاصطناعي إلى آثار سلبية على الأجيال القادمة. مع زيادة الاعتماد على الآلات في الأعمال الروتينية، قد يصبح الأفراد أقل نشاطًا جسديًا، مما يزيد من مخاطر الأمراض مثل السمنة والسكري وأمراض القلب.

تُظهر هذه التحديات أهمية التفكير النقدي في استخدام الذكاء الاصطناعي، والتأكد من أن تطوير هذه التكنولوجيا يتم بشكل مسؤول يتماشى مع القيم الأخلاقية والاجتماعية.

ثانياً. ماهية تطبيق الأمن السيبراني وكشف الاحتيال

يتم إجراء عدد كبير من المعاملات الرقمية يوميًا، حيث يقوم المستخدمون بدفع الفواتير وسحب الأموال وإيداع الشيكات من خلال التطبيقات أو الحسابات عبر الإنترنت. لذلك، هناك حاجة متزايدة للقطاع المصرفي لتعزيز جهود الأمن السيبراني واكتشاف الاحتيال.

1. تعريف تطبيق الأمن السيبراني

تطبيق الأمن السيبراني هو إحدى تطبيقات الذكاء الاصطناعي، ويعرف بأنه مجموعة من الممارسات التي تهدف إلى حماية أجهزة الكمبيوتر والشبكات وبرامج التطبيقات والأنظمة المهمة والبيانات من التهديدات الرقمية المحتملة. يتحمل المؤسسات مسؤولية تأمين البيانات لضمان ثقة العملاء والامتثال للمتطلبات التنظيمية. تعتمد هذه المؤسسات تدابير وأدوات الأمن السيبراني لحماية البيانات الحساسة من الوصول غير المصرح به، ولمنع أي انقطاع في العمليات التجارية بسبب النشاطات غير المرغوب فيها على الشبكة. (sabry، 2021: 15).

تطبق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي عبر الأفراد والعمليات والتقنيات المختلفة. يُعرف الهجوم السيبراني بأنه الاستغلال غير المشروع لأنظمة الحاسوب والشبكات في المنظمات التي تعتمد على تقنية المعلومات والاتصالات الرقمية بهدف إحداث الأضرار. تشمل هذه الهجمات أي نوع من الأنشطة الخبيثة التي تسعى للوصول بطريقة غير مشروعة، أو تعطيل، أو منع، أو تدمير موارد النظم المعلوماتية أو المعلومات ذاتها.

2. كيفية عمل تطبيق الأمن السيبراني

تقوم المؤسسات بتنفيذ استراتيجيات الأمن السيبراني بالتعاون مع متخصصين في هذا المجال. يقوم هؤلاء المتخصصون بتقييم المخاطر الأمنية التي تواجه أنظمة الحوسبة الحالية، بما في ذلك الشبكات، مخازن البيانات، التطبيقات، والأجهزة المتصلة الأخرى. بعد ذلك، يقومون بإنشاء إطار عمل شامل لتنفيذ تدابير وقائية داخل المؤسسة.

تعمل هذه العناصر معًا لإنشاء طبقات متعددة من الحماية ضد التهديدات المحتملة التي قد تواجه جميع نقاط الوصول إلى البيانات. تشمل هذه العمليات تحديد المخاطر، حماية الهويات والبنية الأساسية والبيانات، رصد أوجه الخلل والأحداث، استجابة وتحليل السبب الجذري، والتعافي بعد وقوع الحدث. (artificial intelligence ، 2023. 44).

يساعد الذكاء الاصطناعي على معالجة العديد من القيود، مما يمكنه من تحديد المعاملات الخطرة بشكل أكثر فعالية من البشر. فكلما تم تدريب الآلة على المزيد من عينات العمليات الاحتيالية، زادت قدرتها على التعرف على الأنماط الاحتيالية.

يساهم وجود نظام فعال للكشف عن الاحتيال، يعتمد على التعلم الآلي، في تقليل التكاليف بفضل الكفاءات الناتجة عن التشغيل الآلي العالي ومعدلات الخطأ المنخفضة. بالإضافة إلى ذلك، يمكن لأصحاب المصلحة في القطاعين المالي والتأميني معالجة أنواع جديدة من عمليات الاحتيال، مما يقلل من الاضطرابات التي قد يتعرض لها العملاء الشرعيون ويزيد من ثقة العملاء وأمانهم.

3. تقنية عمل تطبيق الأمن السيبراني الحديثة وتحدياته

1.3. تقنية عمل تطبيق الأمن السيبراني

تتضمن تقنيات الأمن السيبراني الحديثة التي تساعد المؤسسات على تأمين بياناتها ما يلي: (Zabolotny ، 2023 57).

1. انعدام الثقة: يُعتبر مبدأ انعدام الثقة أحد المبادئ الأساسية في الأمن السيبراني، حيث يفترض عدم الوثوق بأي تطبيقات أو مستخدمين تلقائيًا، حتى إذا كانوا داخل المؤسسة. يتطلب هذا المبدأ مصادقة صارمة من السلطات المعنية ومراقبة مستمرة للتطبيقات.

2. تحليلات السلوك: تُستخدم تحليلات السلوك لمراقبة عملية نقل البيانات من الأجهزة والشبكات لاكتشاف الأنشطة المشبوهة والأنماط غير المعتادة. على سبيل المثال، يتم تنبيه فريق أمن تكنولوجيا المعلومات في حال حدوث ارتفاع مفاجئ في نقل البيانات أو تنزيل ملفات مشبوهة إلى أجهزة معينة.

3. نظام كشف التسلل: تعتمد المؤسسات على أنظمة كشف التسلل لتحديد الهجمات السيبرانية والاستجابة لها بسرعة. تحدد آلية الدفاع ضد التسلل مسار البيانات في حالة وقوع حادث، مما يساعد فريق الأمن على اكتشاف مصدر الحادث.

4. التشفير السحابي: يعمل التشفير السحابي على تشفير البيانات قبل تخزينها في قواعد البيانات السحابية، مما يمنع الأطراف غير المصرح لها من إساءة استخدام البيانات في حال حدوث انتهاكات محتملة.

2.3. تحديات تطبيق الأمن السيبراني

في ضوء تطور الهجمات الإلكترونية وانتشار الأجهزة، يُعتبر الذكاء الاصطناعي مناسبًا لحل بعض من أصعب مشكلات الأمن السيبراني. إلا أن هذا المجال يواجه العديد من التحديات، منها: (ibraheem، 2023: 98).

1. المساحة الواسعة للهجوم: يوجد من عشرة إلى آلاف الأجهزة المعرضة للهجوم في كل مؤسسة، مما يزيد من تعقيد إدارة الأمن السيبراني.

2. نقص المهنيين الأمنيين المهرة: يُعاني القطاع من نقص كبير في عدد المتخصصين المدربين في مجال الأمن السيبراني.

3. كتل البيانات الضخمة: تواجه المؤسسات تحديات تتعلق بكتل البيانات التي تتجاوز نطاق المعالجة البشرية، مما يتطلب حلولًا متطورة.

يجب أن يكون نظام إدارة الأمن السيبراني القائم على التعلم الذاتي والذكاء الاصطناعي قادرًا على مواجهة هذه التحديات، ويشمل ذلك ما يلي:

- **جرد أصول تكنولوجيا المعلومات:** الحصول على جرد كامل ودقيق لجميع الأجهزة والمستخدمين والتطبيقات التي تمتلك أي وصول إلى أنظمة المعلومات.

- **التعرض للتهديدات:** يمكن أن تقدم أنظمة الأمن السيبراني المستندة إلى الذكاء الاصطناعي معرفة محدثة بالتهديدات العالمية والصناعية، مما يساعد في اتخاذ قرارات حاسمة لمنع الاحتيال.

- **فعالية الضوابط:** من المهم فهم تأثير أدوات الأمان المختلفة وعمليات الأمان المستخدمة للحفاظ على وضع أمني قوي. يمكن أن يساعد الذكاء الاصطناعي في تحديد مواطن القوة والضعف في البرنامج.

- **توقع مخاطر الاختراق:** يمكن للأنظمة المستندة إلى الذكاء الاصطناعي أن تتنبأ بكيفية وأين من المرجح أن يحدث الاختراق، مما يساعد في تخطيط تخصيص الموارد والأدوات نحو مناطق الضعف.

- **الاستجابة للحوادث:** توفر الأنظمة المدعومة بالذكاء الاصطناعي سياقًا محسنًا لتحديد الأولويات والتنبيهات الأمنية، مما يسمح بالاستجابة السريعة للحوادث وتحديد الأسباب الجذرية لتخفيف نقاط الضعف وتجنب المشكلات المستقبلية.

4. تطبيق الأمن السيبراني والسلامة الرقمية

يتميز تطبيق الذكاء الاصطناعي في الأمن السيبراني للسلامة الرقمية بالعديد من الفوائد والاستخدامات التي تعزز من حماية البيانات وتساهم في تحسين الأمان المؤسسي، وفيما يلي بعض هذه الفوائد: (alshahry، 2023: 72).

1. الكشف عن الأنماط الشاذة ونقاط الضعف:

- تُعد قدرة الذكاء الاصطناعي على اكتشاف وتحديد الأنماط الشاذة داخل الشبكات الواسعة أمرًا بالغ الأهمية. تستغرق عملية مراقبة وتحليل هذه الشبكات وقتًا طويلاً ومعقدًا عند الاعتماد على البشر. مع استخدام الذكاء الاصطناعي، يصبح تحليل البيانات أكثر كفاءة وأسرع، مما يساهم في الكشف السريع عن نقاط الضعف والتهديدات قبل تنفيذ أي هجوم.

2. تقييمات دقيقة للمخاطر وتحسين استخبارات التهديدات:

- يسمح الذكاء الاصطناعي بإجراء تحديد دقيق وتحليل وتقييم للمخاطر، مما يساعد في تقديم توصيات بشأن ضوابط أمنية قوية. من خلال المعلومات الاستخباراتية المجمعة، يتم تطوير نماذج أمان مؤتمنة، مما يعزز من موقف الأمان التنظيمي.

3. أتمتة المهام:

- يمكن للذكاء الاصطناعي أتمتة العمليات التي تستغرق وقتًا طويلاً، مما يزيد من أوقات الاستجابة ويقلل الضغط على المحللين البشريين، مما يتيح لهم التركيز على المهام الأمنية المعقدة.

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

يُعد الحد من الاحتيال أولوية قصوى للبنوك، حيث تخسر الشركات أكثر من 3.5 تريليون دولار سنويًا بسبب الاحتيال، وفقًا لجمعية مدققي الاحتيال المعتمدين. تعتبر هذه المشكلة منتشرة في الصناعة المالية، وتتزايد تعقيدًا مع مرور الوقت، حيث يُجري العملاء المزيد من الخدمات المصرفية عبر الإنترنت باستخدام مجموعة أكبر من القنوات والأجهزة، مما يزيد من فرص الاحتيال.

تستخدم البنوك تقنيات متقدمة مثل التعلم الآلي لمواجهة هذه التحديات، حيث أصبح المحتالون أكثر إبداعًا وتطورًا في استخدام التكنولوجيا. نتيجة لذلك، تحتاج المؤسسات المالية إلى تنفيذ تدابير صارمة للكشف عن الاحتيال في مراحل مبكرة.

دور الذكاء الاصطناعي:

يساعد الذكاء الاصطناعي والتعلم الآلي في تطوير حلول فعالة للكشف عن الاحتيال ومنعه في النظام المصرفي، حيث تُعتبر برامج منع الاحتيال جزءًا أساسيًا من الدروع التي تستخدمها البنوك.

نموذج العمل في بنك Danske

استعان بنك Danske بشركتي Teradata وFeaturespace لتطبيق الذكاء الاصطناعي في محاربة الاحتيال في المعاملات المالية. من خلال هذه الشراكة، تمكن البنك من تحسين أنظمة كشف الاحتيال، مما ساهم في تقليل الخسائر وتعزيز ثقة العملاء في خدماته المصرفية.

هذا النموذج يُظهر كيف يمكن لتطبيقات الذكاء الاصطناعي أن تُحدث فرقًا كبيرًا في سلامة العمليات المالية، مما يعكس أهمية استثمار المؤسسات في التكنولوجيا الحديثة لتعزيز الأمن السيبراني والسلامة الرقمية.

1. التعريف ببنك Danske

بنك Danske هو مؤسسة مالية عالمية تنتمي إلى بلدان الشمال الأوروبي، حيث يحتفظ بجذور محلية قوية ويقوم بتعزيز الروابط مع بقية العالم. تأسس البنك في أكتوبر 1871، ومنذ ذلك الحين ساهم في تحقيق طموحات الأفراد والشركات في هذه المنطقة لأكثر من 145 عامًا. يتمركز البنك في الدنمارك، وتركز أسواقه الرئيسية على الدنمارك وفنلندا والنرويج والسويد، حيث يخدم أكثر من 5 ملايين عميل في مجال التجزئة. يمتد نشاطه إلى 16 دولة، ويقدم خدماته لأكثر من 1800 شركة ومؤسسة، بالإضافة إلى 236000 شركة صغيرة ومتوسطة و2.7 مليون عميل شخصي (Danske Bank Fights Fraud with Deep Learning and AI, 2023).

يمتلك بنك Danske حوالي 50% من السوق المصرفية في الدنمارك، وتضم مجموعته شركات فرعية مثل بنك شمال إيرلندا والبنك الوطني الإيرلندي، فضلاً عن انخراطه في مجالات العقارات ورؤوس الأموال والتأجير في الدنمارك (tagreed ibraheem، 2023).

2. الكشف عن الاحتيال بواسطة شركة Teradata

أعلنت شركة Teradata، المدرجة في بورصة نيويورك، أن بنك Danske، الذي يعد رائدًا في تقديم الخدمات المالية في الدول الاسكندنافية، تعاون مع Think Big Analytics، وهي وحدة تابعة لشركة Teradata، لتطوير نظام للكشف عن الاحتيال يعتمد على الذكاء الاصطناعي. Teradata هي منصة بيانات متعددة السحابة تقدم حلولًا تحليلية متقدمة لمواجهة التحديات التجارية من الألف إلى الياء، مما يمنح الشركات القدرة على التعامل مع أحمال البيانات الكبيرة والمتنوعة (Doug Henschen، 2023).

كان النظام الأصلي للكشف عن الاحتيال في بنك Danske يعتمد بشكل كبير على قواعد تم إنشاؤها يدويًا، وقد تم تطبيقها بشكل استباقي مع مرور الوقت. ومع ذلك، كانت نسبة الإيجابيات الكاذبة مرتفعة، حيث وصلت إلى 99.5% من جميع المعاملات. بالإضافة إلى ذلك، كان هناك تحديات تتعلق بتكاليف التحقيقات والافتقار إلى الخبرة في إدخال التقنيات الحديثة في العمليات. لذلك، لجأ البنك إلى Think Big Analytics، التي قدمت الخبرة اللازمة لعمليات مشابهة في الشركات الكبرى. بعد العمل مع مستشاري Think Big Analytics لمدة 12 أسبوعًا، طور فريق بنك Danske نماذج تعلم آلة ساهمت في تقليل نسبة الإيجابيات الكاذبة بنسبة 20 إلى 30%. ومن المتوقع أن تحقق هذه المنصة عائد استثمار بنسبة 100% في عامها الأول من التشغيل (Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real, 2023).

تمكن الفريق من تقليل الإيجابيات الزائفة بنسبة 50%، بينما زاد معدل اكتشاف الاحتيال بنسبة 60%. يُعتبر برنامج مكافحة الاحتيال في بنك Danske الأول من نوعه الذي يدمج تقنيات التعلم الآلي في العمليات، بالإضافة إلى تطوير نماذج التعلم العميق لاختبار هذه التقنيات. كما أشار Mads Andjoiar، مدير خدمات العملاء في Think Big Analytics، إلى أن البنوك تحتاج إلى حلول فورية للمعاملات عبر الإنترنت وبطاقات الائتمان والمدفوعات عبر الهاتف المحمول. وبفضل النظام المدعوم بالذكاء الاصطناعي الذي تم تطويره مع بنك Danske، يمكن معالجة المعاملات في أقل من 300 مللي ثانية (Danske Bank and Teradata Implement Artificial Intelligence (AI) Engine that Monitors Fraud in Real, 2023).

وصرح Nadim Golzer، رئيس التحليلات المتقدمة في بنك Danske، بأن المحتالين يتقنون استخدام تقنيات التعلم الآلي المتطورة. لذا من الضروري استخدام تقنيات مماثلة للكشف عنهم. من خلال الذكاء الاصطناعي، تمكّن البنك من تقليل النتائج الإيجابية الزائفة بنسبة 50%، مما سمح بإعادة تخصيص نصف وحدة الكشف عن الاحتيال إلى مهام 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

تُعرف شركة Featurespace بأنها قامت بتطوير أول محرك لتحليلات السلوك على مستوى العالم، وهو منصة ARIC، والتي تهدف إلى معالجة التحديات المرتبطة بكشف الاحتيال. اختار بنك Danske، وهو أكبر بنك في الدنمارك والرائد في أسواق الشمال الأوروبي، Featurespace كمزود استراتيجي لتعزيز إمكانياته في مواجهة الاحتيال. تُعتبر Featurespace رائدة عالمياً في مجال مكافحة الجرائم المالية، بما في ذلك الاحتيال وغسيل الأموال، حيث قامت بابتكار التحليلات السلوكية التكيفية وأطلقت منصة ARIC، وهي منصة برمجية تستخدم تقنيات التعلم الآلي في الوقت الفعلي لرصد الأحداث في أكثر من 180 دولة لمنع الاحتيال والجرائم المالية (Michael Touchton, 2023).

تم اختيار منصة ARIC من قبل البنك للحد من الاحتيال المرتبط بالبطاقات على مستوى العملاء، مع التركيز على تقديم أفضل تجربة ممكنة من خلال تقليل الإيجابيات الزائفة. جاء هذا الإعلان بعد أن قام Danske بالبحث عن شركات التكنولوجيا المالية لإقامة شراكات معها. وأوضحت مارتينا كينج، الرئيس التنفيذي لشركة Featurespace، أن مواجهة الاحتيال تمثل تحديًا كبيرًا نظرًا لتطور التهديدات المستمرة. وأضافت أن النظام التكيفي في الوقت الحقيقي يمكنه تسليط الضوء على الهجمات الجديدة حال حدوثها، مما يساهم في حماية البنك وعملائه، معبرة عن فخر الشركة بكونها شريكًا لبنك Danske في مكافحة الاحتيال الرقمي.

تستعمل Featurespace تقنيات التعلم الآلي، التي تُعرف بالتحليلات السلوكية، لاكتشاف المعاملات الاحتيالية من خلال مراقبة ملفات تعريف السلوك الفردية في الوقت الفعلي، مما يساعد في تحديد الحالات الشاذة ومنع الاحتيال عبر جميع وسائل الدفع. يتم ذلك من خلال إجراء تحليلات سلوكية معدة خصيصًا للتقليل من تعرض البنك للاحتيال على البطاقات وحماية القنوات الإلكترونية. كما تقدم تقنيات كشف متقدمة وقابلة للتفسير، مما يمكّن المؤسسات المالية من تقييم المخاطر تلقائيًا والتعرف على هجمات الاحتيال الجديدة وتحديد الأنشطة

المشبوهة في الوقت الفعلي. تعتمد أكثر من 30 مؤسسة مالية على منصة ARIC لحماية أعمالها وعملائها (Michael Touchton, 2023).

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

أدت التطورات في صناعة الخدمات المصرفية والدفع إلى تسريع العمليات المصرفية، مما سمح لمزيد من المستخدمين بالوصول إلى الخدمات المالية. هذا التوجه يعكس "موجة جديدة من الشمول المالي الرقمي"، حيث بدأ المستخدمون في الاستفادة الكاملة من الخدمات المصرفية الرقمية. ومع ذلك، شهدت هذه المرحلة ارتفاعًا ملحوظًا في حالات الاحتيال، مما يهدد الجهود الرامية لإدماج الفئات التي كانت مستبعدة سابقًا في الاقتصاد الرقمي. في دراسة شملت أكثر من خمسة ملايين عميل، قام بنك Danske بتقييم جهوده لمكافحة الاحتيال، حيث كان له دور رئيسي في تعزيز الشمول المالي باستخدام برامج تعتمد على تطبيقات الذكاء الاصطناعي (Arvid O.I Hoffmann, Cornelia Birnbrich, 2012, 5).

كان البنك يعاني من حوالي 1200 نتيجة إيجابية كاذبة يوميًا، حيث كانت 99.5% من هذه الحالات غير صحيحة. كما أشار ناديم غولزر، رئيس التحليلات العالمية في البنك، إلى أن المشكلة يمكن حلها في غضون دقائق، ولكن كل دقيقة أو دقيقتين على 1200 معاملة تعتبر وقتًا ضائعًا. أضافت Teradata من شركة Think Big Analytics أن البنك قرر العمل على تطوير برامج لمكافحة الاحتيال باستخدام التعلم الآلي، مما ساهم في تقليل الإيجابيات الزائفة بنسبة 35%، وتحسين الكشف عن الاحتيال الفعلي بنفس النسبة تقريبًا. ومع إضافة التعلم العميق، حقق البنك انخفاضًا في الإيجابيات الكاذبة بنسبة 60% وزيادة في كشف الاحتيال الفعلي بنسبة 50%. وبهذا، أصبح بإمكان المحققين توجيه جهودهم نحو القضايا الأكثر أهمية، مما يوفر الوقت والجهد ويعزز الأمان لكل الأطراف (Doug Henschen, 2023).

يمكن أن يشعر العملاء بأن "البنك ليس مكانًا آمنًا وغير قادر على حماية أصولهم"، مما يؤدي إلى فقدان الثقة والتحول إلى مزودين آخرين. إن الحوادث المتكررة للاحتيال قد تؤثر بشكل سلبي على سمعة البنك بطرق متعددة. من هنا، تعتبر الإدارة الاستباقية للاحتيال فرصة للبنوك لإعادة بناء ثقة العملاء والحفاظ عليهم. مثلاً، قدم بنك Danske تطبيقًا رقميًا يُدعى Pocket Money، يتيح للأطفال بين 8 و14 عامًا تتبع أموالهم، مما يعزز الشمول المالي الرقمي.

يُظهر البحث أن الأفراد، وخاصة النساء ذوات الدخل المنخفض، هم الأكثر عرضة للاحتياج بسبب انخفاض مستويات تعليمهم المالي، مما يسهل على المحتالين استغلالهم. لذا، يُشدد على أهمية تعزيز التعليم المالي بالتوازي مع الثورة الرقمية. إذا لم يتم الحد من مخاطر الاحتيال، فإن ذلك قد يؤدي إلى إبطاء تقدم الشمول المالي الرقمي (Shabtai Gold, 2023).

يؤمن بنك Danske بأن على البنك حماية عملائه من الإهمال أو الجهل. يعتقد البنك أن العملاء، رغم استخدامهم للتكنولوجيا، قد لا يدركون كيفية حماية أنفسهم. لذا يقدم البنك استشارات ونصائح لزيادة وعي المستخدمين حول سبل تقليل فرص الاحتيال. على سبيل المثال، إذا كانت السرعة المعتادة لتعبئة نموذج ما أسرع بأربع مرات من المعدل الطبيعي، فإن ذلك قد يشير إلى احتمال عدم كون العميل هو نفسه. كما تسعى Danske لقياس سرعات حركة الماوس، مما سيمكنها قريبًا من التعرف على الأنماط الكتابية، وبالتالي التفريق بين العملاء الحقيقيين والمحتالين. من المتوقع أن تحقق منصة الكشف عن الاحتيال في البنك عائد استثمار بنسبة 100% في عامها الأول من التشغيل (Doug Henschen, 2023).

الخاتمة:

تعتبر مكافحة الاحتيال بشكل فعّال عنصرًا أساسيًا في تعزيز الوصول المالي، حيث إن سمات الخدمة مثل منع الاحتيال تلعب دورًا إيجابيًا في استدامة العلاقة والمعاملات بين البنوك والعملاء. من خلال إثبات خبرتها في مجال منع الاحتيال، يمكن للبنوك تعزيز شعور الأمان لدى عملائها، مما يؤدي بدوره إلى تحسين جودة هذه العلاقة وزيادة ولاء العملاء. فالتجربة الإيجابية لعميل واحد يمكن أن تمثل خطوة نحو تحقيق شمول مالي أوسع، يتبعه شمول مالي رقمي.

وفي سياق تجربة بنك Danske في مواجهة الاحتيال باستخدام تقنيات الذكاء الاصطناعي، يتبين أن تطبيقات كشف الاحتيال والأمن السيبراني المعتمدة على الذكاء الاصطناعي قد أسهمت في اكتشاف 50% من حالات الاحتيال الفعلية. وهذا يشكل أساسًا لتعزيز الوصول المالي الرقمي من خلال تعزيز الشعور بالأمان لدى الفئات الأقل خبرة في التكنولوجيا، التي كانت تُعتبر أهدافًا سهلة للمحتالين. كما ساهمت هذه الإجراءات في تحسين سمعة البنك وجعله خيارًا مفضلًا لدى العملاء المتخوفين من الاحتيال الرقمي، مما يعزز العلاقة بينهم وبين بنكهم، وهو ما يدعم صحة الفرضية المطروحة.

اقتراحات الدراسة:

استنادًا إلى نتائج الدراسة، يمكن تقديم التوصيات التالية لمطوري الخدمات المصرفية في الجزائر:

1. توفير البنية التحتية: من الضروري وضع إطار تشريعي واضح ينظم الخدمات المالية الرقمية، مع تحديد الالتزامات المطلوبة من البنوك الجزائرية وعملائها.

2. تدريب الموظفين: يتعين تدريب موظفي البنوك وتعزيز ثقافة الخدمات المصرفية الرقمية المستندة إلى تطبيقات الذكاء الاصطناعي بين العملاء.

3. التوعية بأهمية الذكاء الاصطناعي: يجب أن تدرك البنوك والمؤسسات المالية الجزائرية أهمية استخدام تطبيقات الذكاء الاصطناعي في خدماتها المالية، إذ لا يزال هناك تأخر كبير مقارنة بالدول المتقدمة في هذا المجال، رغم توفر بعض القنوات الإلكترونية مثل الصرافات الآلية.

4. تخصيص ميزانية للتكنولوجيا: يجب تخصيص ميزانية لشراء تطبيقات الذكاء الاصطناعي لاستخدامها من قبل المؤسسات، نظرًا للعوائد الإيجابية المحتملة على أدائها.

5. التدريب المستمر: ينبغي الاهتمام بتدريب الموظفين على استخدام هذه التطبيقات بهدف تقليل الاعتماد على القدرات الأجنبية.

6. تشجيع البحث العلمي: يتطلب الأمر تعزيز البحث العلمي في هذا المجال من خلال إنشاء مراكز أبحاث مخصصة لتنمية الكفاءات المحلية والاستفادة منها بشكل فعال.

المصادر والمراجع

1.Saudi Central Bank. 2023. "Cyber Risks". Retrieved from https://www.sama.gov.sa

2.Artificial Intelligence. 2023. "A New Chapter for Cybersecurity". Retrieved from https://www.tripwire.com

3.Zabolotny, Ostap. 2023. "Artificial Intelligence in Lending". Retrieved from https://firstbridge.io

4.Ibrahee.tagreed https://www.marefa.org. 2023 "Case Study of Danske Bank A/S". Retrieved from

5.Sabri, Saida. 2021. "A Study on Artificial Intelligence in AXA Companies". *Algerian Journal of Management Economics*, Vol. 52, No. 20.

6.Al-Shehri, Fayez. 2023. "Challenges of Artificial Intelligence". Retrieved from: https://elaph.com/Web

7.Amazon Web Services. 2023. "What is Cybersecurity?" Retrieved from: https://aws.amazon.com

8.Azad, Ananya. 2023. "8 Ways to Improve Customer Interaction in Banks Using Smart Chat." Retrieved from: https://www.engati.com

9.Hoffmann, Arvid O.I., and Cornelia Birnbrich. 2012. "The Impact of Fraud Prevention on Bank-Customer Relationships." *International Journal of Bank*, Vol. 30, No. 5.

10.Danske Bank and Teradata. 2023. "Artificial Intelligence (AI) Engine that Monitors Fraud in Real." Retrieved from: https://www.teradata.com

11.Dolgorukov, Dmitry. 2023. "How AI Can Support Inclusive Lending." Retrieved from: https://www.bai.org

12.Henschen, Doug. 2023. "Teradata Think Big Analytics and Danske Bank Case Study". Retrieved from: https://www.constellationr.com

13.Cummins, Emily. 2023. "The 10 Best Banking Chatbots". Retrieved from: https://www.netomi.com

14.Franco, Helena. 2023. "Chatbots in Banking: The New Must-Have in Customer Care". Retrieved from: https://www.inbenta.com

15.Vilar, Henry. 2023. "Featurespace Foils Fraud for Danske Bank". Retrieved from: https://www.fintechfutures.com

16.Aschi, Massimiliano, Susanna Bonura, Nicola Masi, Domenico Messina, and Davide Profeta. 2023. "Big Data and Artificial Intelligence in Digital Finance". Retrieved from: https://link.springer.com

17.Williamson, Ryan. 2023. "Benefits of AI to Fight Fraud in the Banking System". Retrieved from: https://www.datasciencecentral.com

18.Saudi Central Bank. 2023. "Cyber Risks". Retrieved from: https://www.sama.gov.sa

19. Artificial Intelligence. 2023. "A New Chapter for Cybersecurity". Retrieved from: https://www.tripwire.com

20.Zabolotny, Ostap. 2023. "Artificial Intelligence in Lending". Retrieved from: https://firstbridge.io

21.Ibrahim, Taghreed. 2023. "Danske Bank A/S Case Study". Retrieved from: https://www.marefa.org

22.Sabry, Saida. 2021. "A Study on Artificial Intelligence in AXA Companies". *Algerian Journal of Management Economics*, Volume 52, Issue 20.

23.Al-Shahri, Fayez. 2023. "Challenges of Artificial Intelligence". Retrieved from: https://elaph.com/Web

24.Amazon Web Services. 2023. "What is Cybersecurity?" Retrieved from: https://aws.amazon.com

25.Azad, Ananya. 2023. "8 Ways to Improve Customer Engagement in Banks Using Smart Chat." Retrieved from: https://www.engati.com