دور الذكاء الاصطناعي في الكشف والحد من الاحتيال على البطاقات الائتمانية البنكية على المستوى الدولي

The role of artificial intelligence in detecting and reducing bank credit card fraud at the international level

بن خضرة حميدة*[1]، بضياف صالح[2]

[1]جامعة البليدة 2 (الجزائر)،مخبر البحث حول الابداع وتغيير المنظمات والمؤسسات،

h.benkhadra@univ-blida2.dz /benkhadrahamida83@gmail.com

[2]جامعة البليدة 2 (الجزائر)،مخبر التنمية الاقتصادية والبشرية في الجزائر،

s.beddiaf@univ-blida2.dz /profsalah2017@gmail.com

تاريخ الاستلام: 2024/04/27 تاريخ القبول: 2024/06/08 تاريخ النشر: 2024/07/01

ملخص:

تهدف هذه الدراسة الى معرفة طرقالاحتيال على البطاقات الائتمانية، باعتبارها وسيلة من وسائل الدفع الالكتروني الاساسية للبنوك، والتي يتعرض لها مصدري وحامليها لمخاطر عدة في العالم ، وللحد منها يتم استخدام تطبيقات الذكاء الاصطناعي والامن السيبيراني الى سنة 2023، وتم الاعتماد على منهجي الوصف والتحليل باستخدام أدوات في التحليل من بينها الاشكال والرسومات البيانية .

نتج عن الدراسة ان التطور التكنولوجي سلاح ذو حدين، اذ جعل وسائل الاحتيال في الذكاء الاصطناعي من اعلى درجات الخطر، وعرضة للهجمات السيبرانية، فلابد على البنوك التأقلم مع الوضع والبحث عن حلول بديلة.

الكلمات المفتاحية : الاحتيال؛ الغش؛ البطاقات الائتمانية؛ الذكاء الاصطناعي؛ الأمن السيبراني.

تصنيف JEL: **G210 ; G23 ; G24 ;G290 ;O330**.

Abstract:

This study aims to know the methods of credit card fraud, it's the basic means of electronic payment for banks, to which issuers and card holders are exposed to risks in the world. To reduce them, applications of artificial intelligence and cybersecurity are being used until the year 2023, has been placed on methodologies of description and analysis.

The study concluded that technological development is a double-edged sword, as it has made artificial intelligence fraud methods of the highest levels of danger and vulnerable to cyber attacks, so banks must adapt to the situation and search for alternative solutions.

Keywords: Fraud; cheat; credit cards; artificial intelligence; Cyber security.

Jel Classification Codes: G210 ; G23 ; G24 ;G290 ;O330.

*بن خضرة حميدة

I. مقدمة:

شهد العالم في الآونة الأخيرة عدة تطورات خاصة في مجال التكنولوجيا المعلومات والاتصال، فتعتبر اهم التطورات العالمية المعاصرة، والتي ساهمت بشكل كبير في تطور الخدمات المصرفية بصفة عامة ووسائل الدفع بصفة خاصة، فتعتبر بطاقات الائتمان من وسائل الدفع الالكتروني الأكثر انتشارا، نتيجة الاقبال الكبير الذي عرفته من طرف المتعاملين، فأصبحت تحتل حيزا كبيرا في التعاملات المالية مقارنة بوسائل الدفع الأخرى خاصة التقليدية منها.

كنتيجة الاقبال الكبير على استخدام الخدمات المالية الالكترونية بما فيها البطاقات الائتمانية، أدى الى ظهور أساليب احتيالية جديدة تعرض المتعامل المالي لعدة مخاطر، كالنصب، الاحتيال، انتحال الشخصية، التزوير والسرقة وعليه أصبحت تشكل أكبر التحديات التي تواجه المصارف، المؤسسات المالية، التجار، الافراد وبيئة الاعمال بصفة عامة، فهي تعيق الأداء وتهدر الأموال وتهدد النظم المالية العالمية، لذلك لابد من اتخاذ إجراءات ووسائل للحد من هذه الممارسات.

ومن هذا المنطلق لابد على جميع الأطراف المتعاملة بالبطاقات الائتمانية سواء كانت مصدرة او حاملة لها، اتخاذ تدابير وقائية للكشف والحد من الاحتيال، وتجدر الإشارة ان الذكاء الاصطناعي من اهم التطبيقات الحديثة التي قدمت خدمات متميزة في المجال المصرفي والمالي، حيث يقدم خدمات ذو كفاءة ودقة عالية، ومن اهم تطبيقاته التي تبنتها معظم المصارف الأمن السيبراني، فهو يحمل مسؤولية حماية أجهزة الكمبيوتر والبرامج والانظمة من مختلف الهجمات الإلكترونية.

استنادا الى ما سبق يمكن طرح إشكالية البحث من خلال التساؤل التالي:

كيف يساهم الذكاء الاصطناعي في الكشف والحد من الاحتيال على البطاقات الائتمانية؟

من أجل الإجابة على التساؤل الرئيسي يمكن طرح التساؤلات الفرعية التالية:

- ✓ ماهي اشكال الانتحال على البطاقات الائتمانية؟.
- ✓ فيما تتمثل اهم تطبيقات الذكاء الاصطناعي في المصارف؟.
- ✓ كيف تطبق المصارف الامن السيبراني لمنع عمليات الاحتيال على البطاقات الائتمانية؟.

الفرضيات: للإجابة على الإشكالية نقترح الفرضيات التالية:

- يتخذ الانتحال على البطاقات الائتمانية عدة اشكال.
- تتبنى المصارف عدة تطبيقات للذكاء الاصطناعي كالأمن السيبراني وروبوتات الدردشة.
- تطبق المصارف الامن السيبراني لمنع عمليات الاحتيال على البطاقات الائتمانية وفق بروتوكول محدد بدقة.

أهداف الدراسة: نحاول من خلال هذه الورقة البحثية تحقيق جملة من الأهداف وهي:

- تسليط الضوء على مختلف أنواع الاحتيال على البطاقات الائتمانية.
- التعرف على اهم الإجراءات الواجب اتخاذها لردع الاحتيال.
- معرفة كيفية تطبيق الذكاء الاصطناعي لكشف ومنع الاحتيال على البطاقات الائتمانية.

أهمية الدراسة: تكمن أهمية البحث لارتباطه بأهمية التطورات الحديثة في مجال الصناعة المالية وما نتج عنها من مخاطر، حيث يعتبر الاحتيال المالي من اهم تحديات المعاملات المالية، وفي نفس الصدد ابراز أهمية تبني تطبيقات الذكاء الاصطناعي من طرف البنوك والمؤسسات المالية للحد من هذه الجرائم المالية.

منهجية الدراسة: قصد الإجابة عن إشكالية الدراسة اعتمدنا على المنهج الوصفي والمنهج التحليلي في عرض مختلف المفاهيم المتعلقة بالاحتيال على البطاقات الائتمانية، من تعريف واشكال وإجراءات وقائية، وكذا تحليل نتائج التقارير المختلفة المتعلقة باستخدام الذكاء الاصطناعي والامن السيبراني.

هيكل الدراسة: تم تقسيم الدراسة الى قسمين رئيسيين، القسم الأول خصص للإطار العام للاحتيال على البطاقات الائتمانية، بينما خصص القسم الثاني للأساليب الحديثة للكشف والوقاية من الاحتيال على البطاقات الائتمانية.

II. الإطار العام للاحتيال على البطاقات الائتمانية:

ارتئينا قبل التطرق الى تعريف الاحتيال وشرح مختلف اشكاله، لابد من التطرق لتعريف البطاقات الائتمانية.

II – 1 تعريف بطاقة الائتمان:

تعرف بطاقات الائتمان بعدة مصطلحات منها: بطاقات الدفع الالكتروني، النقود الائتمانية، النقود البلاستيكية، بطاقات الائتمان الممغنطة، النقود الالكترونية (عماروش، 2017، صفحة 61).

عرف مجمع الفقه الإسلامي الدولي بطاقات الائتمان أنها " مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناء على عقد بينها يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن حالا لتضمنه التزام المصدر بالدفع، ومنها ما يمكن من سحب النقود من المصارف"(برابح، مزايا ومخاطر استخدام العامل لبطاقة الائتمان البنكية، 2021، صفحة 246).

تعتبر بطاقات الائتمان أحد أهم أنواع البطاقات المالية، تعطي القدرة لصاحبها على اقتراض الأموال من أجل دفع ثمن المشتريات من السلع والخدمات مع التجار الذين يقبلون بطاقات الدفع، حيث تقوم الجهة المصدرة للبطاقة بضمان معاملات العميل والدفع بدلا عنه، دون أن يكون لديه مبلغ مالي في رصيده يغطي تلك المعاملة، على أن يتم تحصيل مبلغها لاحقا، ولا يتم اصدار هذه البطاقات الا بعد دراسة جيدة للعملاء لتجنب البنك المصدر لمخاطر عدم السداد (عبدالكافي و بورابة، 2022، صفحة 413).

من خلال التعارف السابقة يمكن تعريف بطاقات الائتمان على انها أداة سداد ووفاء بالدين تصدرها جهات معينة في حدود مبالغ معينة.

II – 2تعريف الاحتيال: تعتبر عمليات الاحتيال والنصب متواجدة منذ زمن بعيد، لكن في وقتنا الحالي زادت عدد عمليات الاحتيال ومخاطرها مع زيادة التقدم التكنولوجي، فقد تطورت أساليب الاحتيال وانتشرت بشكل كبير وازداد حجم الخسائر الناجمة عنها.

وعرف المشرع الجزائري جريمة الاحتيال في المادة 372 من قانون العقوبات "كل من توصل الى استلام او تلقي أموال أو منقولات أو مسندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو ابراء من التزامات استعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي".

كما ان الاحتيال يعبر بالاستيلاء على مال مملوك للغير بخادعه وحمله على تسليم ذلك المال (عزوز و بن عبد العزيز، 2022، صفحة 1366).

ومنه نستنتج أن الاحتيال هو كل فعل متعمد سواء كان سرقة او تغيير بيانات او انتحال شخصية قصد الاستيلاء على أموال الغير بغير حق.

II – 3الاحتيال المعلوماتي: الاحتيال المعلوماتي هو التلاعب العمدي بمعلومات وبيانات حول قيمة مادية يختزنها نظام الحاسب الآلي، أو الادخال غير مصرح به على معلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تسير عملية البرمجة، أو أي طريقة تعمل على التأثير على الحاسب الآلي ليقوم بإنجاز العمليات بناء على هذه المعلومات من أجل الحصول على ربح غير مشروع وإلحاق الضرر بالغير(عبدالكافي و بورابة، 2022، صفحة 414).

II – 4أشكال الاحتيال على البطاقات الائتمانية: انتشرت بطاقات الدفع الالكتروني في كافة انحاء العالم، واجتاحت كل الأنظمة الفنية، نظرا لتسهيلات التي تمنحها لحاملها، الا أن مخاطرها تنوعت حيث ساعدت بيئة تكنولوجيا المعلومات والاتصال على ابتكار وسائل احتيال وخداع جديدة من الصعب الكشف عنها، سواء كانت من مالك البطاقة او من طرف الغير، فيمكن تمييز نوعين من الاحتيال باستخدام البطاقة إما بالاستعمال المادي للبطاقة البنكية، أو الاحتيال بدون وجود البطاقة أي الاحتيال عن بعد.

تعددت أشكال الاحتيال على البطاقات الائتمانية نذكر أشهرها:

4. 1–الاحتيال من طرف صاحب البطاقة نفسه:

قد تكون لصاحب البطاقة نية سيئة فيقوم باستخدام البطاقة بطريقة غير مشروعة في احدى الصور التالية:

- ✓ استعمال البطاقة بعد انتهاء مدة صلاحيتها: ينص العقد المبرم بين العميل والبنك على أن يسلم العميل البطاقة للبنك بعد انتهاء مدة صلاحيتها، الا انه في بعض الحالات يقوم العميل باستخدام البطاقة المنتهية الصلاحية قصد التحايل والسرقة.
- ✓ استعمال البطاقة بعد إلغائها: يحق للبنك في أي وقت إلغاء البطاقة لعدة أسباب منها: تخلف الحساب أو تغيير نظام التعامل، تغيير نوعية الخدمة التي تؤديها البطاقة، في حالة استعمال العميل البطاقة بعد اطلاعه على هذه الإجراءات يعد تزوير بسبب استعمالها بصفة غير صحيحة(حسن، 2011، الصفحات 62-63).
- ✓ تجاوز حد السحب: لكل بطاقة بنكية سقف معين يتحدد عند اصدار البطاقة ويلتزم العميل بهذا السقف، ولا يجوز استخدام البطاقة الا في حدود الرصيد المسموح، الا أنه أحيانا يمارس صاحب البطاقة طرق احتيالية فيقوم بتجاوز الحد واجراء معاملات مالية بطريقة غير مشروعة.

4. 2–الاحتيال من طرف البنك مصدر البطاقة: في أغلب الأحيان يكون الاحتيال في هذه الحالة من طرف موظفي البنك وحدهم او بالتواطؤ مع الغير ويأخذ أحد الاشكال التالية:

- تواطؤ موظف البنك مع حامل البطاقة في (برابح، مزايا ومخاطر استخدام العامل لبطاقة الائتمان البنكية، 2021، صفحة 254):
- استخراج بطاقة سليمة ببيانات مزورة.
- السماح لحامل البطاقة بتجاوز سقف البطاقة في عمليات السحب.
- السماح لحامل البطاقة باستخدام بطاقة منتهية الصلاحية.
- تواطؤ موظف البنك مع أفراد العصابات الاجرامية بتزويدهم ببيانات بطاقات الائتمان الصحيحة لعملائهم، لاستخدامها في نسخ وتقليد هذه البطاقات، ويتم التركيز على البطاقات ذات السقف المرتفع .

4. 3–الاحتيال عن طريق سرقة او فقدان البطاقة: يتحصل المحتالون في هذه الحالة على بطاقات الائتمان عن طريق السرقة أو الحصول على بطاقة ضائعة و مفقودة، فيقومون باستخدام معلومات هذه البطاقة و القيام بعمليات الشراء، أو إجراء معاملات عبر شبكة المعلومات العالمية، وفي هذه الحالة تتم سرقة صاحب البطاقة مباشرة، أو عن طريق سرقة بطاقة الائتمان المرسلة الى

أصحابها عبر البريد، أو من خلال السطو على المنازل أو سرقة المحافظ وغيرها من الوسائل غير المشروعة ، او استخدام بطاقة فقدها شخص ما أو نساها في جهاز الصراف الالي خاصة اذا وجد معها الرقم السري فيسهل سحب ما فيها من رصيد(الحميدي، 2023، صفحة 12).

4. 4–التزوير:يقصد بتزوير البطاقات البنكية التغيير في بياناتها كالأرقام الموجودة عليها، أو الامضاءات، أو اسم حاملها، أو المعطيات الالكترونية، الا ان هذا التزوير يأخذ شكل مادي وشكل معنوي، حيث تتعدد صور التزوير وذلك حسب الوسائل التكنولوجيا المتاحة والمستعملة، كتغيير بيانات البطاقة البنكية ففي هذه الحالة يتم تغيير بيانات حامل البطاقة عن طريق حذف معلومة من بيانات ووضع معلومات اخرى، أو عن طريق إضافة أو محو كلمة أو حرف أو رقم في البطاقة المزورة (عمراني، 2017، صفحة 313).

4. 5–التصيد:هو عبارة عن مكالمات هاتفية يتم استعمالها من طرف المحتالين لخداع الأشخاص والاستيلاء على معلوماتهم الشخصية والمالية، وذلك عن طريق اجراء اتصالات كمكالمات الفوز بجائزة أو مكالمات التحقق من الحسابات البنكية، أو طلب مساعدة في استبيان، أو عن طريق إرسال رسائل عبر البريد الالكتروني أو الهاتف تطلب منهم تقديم معلومات شخصية، فيتم تسجيل هاته المعلومات ويتم استعمالها في التلاعب بالحسابات(الاردني، 2023، صفحة 6).

وبالتالي التصيد هو الحصول على معلومات حساسة ومهمة عن العميل عن طريق اتصال هاتفي أو رسائل نصية كالإيميلات وغيرها، هدفها إغراء وتضليل العميل كالفوز بجوائز مالية يطلب منه رقم حسابه أو رقمه السري أو التسجيل في قرعة كلها من شأنها الإيقاع به وسرقته.

II – 5تطور حجم عمليات الاحتيال على البطاقات الائتمانية على المستوى العالمي:

عرف الاحتيال على البطاقات الائتمانية انتشارا كبيرا في جميع انحاء العالم خاصة في الآونة الأخيرة نتيجة لعدة عوامل يرجع بعضها لهفوات غير عمدية ويرجع البعض الاخر لأفعال مقصودة لهز الثقة المصرفية ونشر الهلع في نفوس المتعاملين والاستيلاء أكثر على ممتلكات الغير بغير حق من طرف صغار المحتالين وكبار العصابات.

شكل 01: الاحتيال على البطاقات الائتمانية في جميع انحاء العالم لسنة 2020

المصدر: من اعداد الباحثين بالاعتماد على: تقرير نيلسون ديسمبر 2021

سجلت خسائر المستثمرون والتجار و مستخدمو المعاملات التجارية و أجهزة الصرف الآلي بشكل جماعي 28,58 مليار دولار بسبب الاحتيال سنة 2020، أي ما يعادل 6,84 سنت لكل 100 دولار من حجم الشراء (robertson, 2021, p.

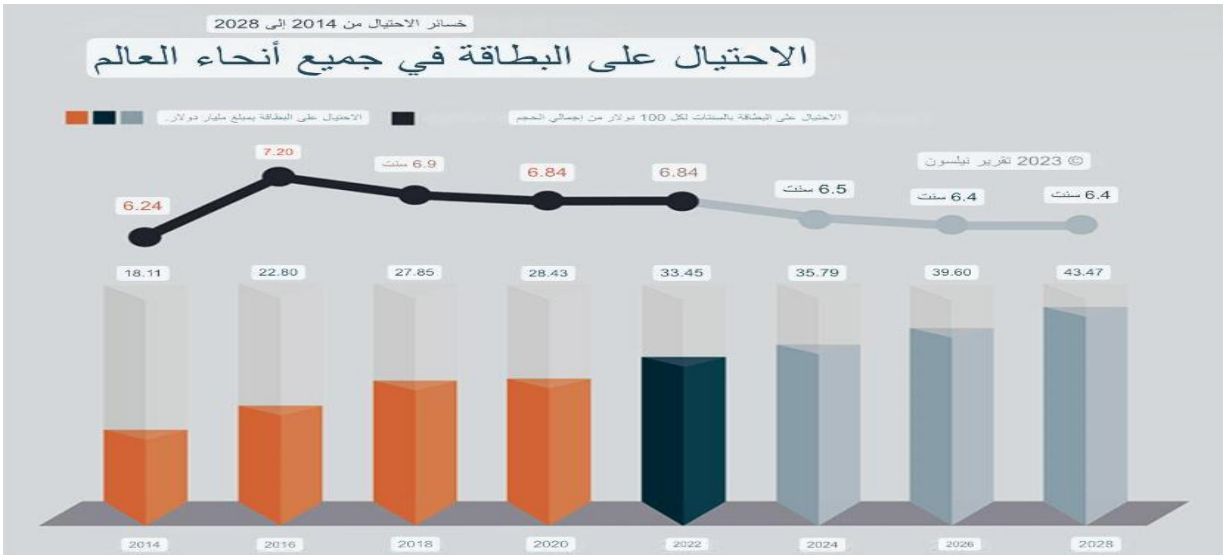
(5، كما نلاحظ من الشكل السابق ان حجم الخسائر بسبب الاحتيال قدر بـ 4,5 سنت لكل 100 دولار من حجم التجارة سنة 2010 ، وارتفعت النسبة الى 5,5 في سنة 2013 ، ثم ارتفعت الى 7,24 سنة 2016 ، بعدها انخفضت الى 6,90 سنة 2018 ثم انخفضت الى 6,84 سنة 2019 لتستقر عند نفس النسبة سنة 2020 ، نلاحظ ان هذه النسب في الاحتيال كانت في ارتفاع مستمر من سنة 2010 الى غاية سنة 2017 ، حيث اصبح التلاعب بالحسابات يشكل خطرا على وسائل الدفع الحديثة، ويرجع هذا لصعوبة الكشف عن الاحتيال خاصة في ظل التطور التقني الكبير.

شكل 02: تطور تكلفة الاحتيال على البطاقات الائتمانية على المستوى العالمي داخل وخارج الولايات المتحدة الامريكية (2014–2021).

المصدر:من اعداد الباحثين بالاعتماد على تقرير نيلسون ديسمبر 2022

لازال العالم يشهد نموا متزايدا في عمليات الاحتيال على البطاقات الائتمانية، حيث تحمل كل من مصدرو البطاقات والتجار ومتلقو المدفوعات وكذا المعاملات عن طريق أجهزة الصراف الآلي خسائر احتيال كبيرة قدرت اجماليا 32.34 مليار دولار أمريكي سنة 2021، وبارتفاع قدره 13.8 % مقارنة بسنة 2020 ,rebertson, card fraud worldwide) (2022, p. 5 ، نلاحظ من خلال المنحنى ان نسبة خسائر الاحتيال على البطاقات الائتمانية داخل وخارج الولايات المتحدة الامريكية في تزايد مستمر، حيث بلغت نسبة الخسائر داخل الولايات المتحدة الأمريكية 10,09 مليار دولار امريكي في حين بلغت 18,34مليار دولار امريكي خارج الولايات المتحدة الامريكية، بينما سجلت نسبة خسائر الاحتيال داخل الولايات الأمريكية سنة 2021 قيمة 11,91 مليار دولار امريكي في مقابل نسبة 20,43 مليار دولار امريكي خارج الولايات المتحدة الأمريكية، ويرجع ارتفاع هذه نسبة الخسائر بالولايات المتحدة الأمريكية كونها دولة متقدمة تعتمد على التجارة الإلكترونية، وعلى وسائل الدفع الالكتروني بما فيها البطاقات الائتمانية بشكل كبير، مما أدى لارتفاع نسبة الاحتيال وكذلك ارتفاع تكلفة الخسائر.

شكل 03: حجم الاحتيال على البطاقات في جميع انحاء العالم المتوقع الى غاية2028



المصدر:من اعداد الباحثين بالاعتماد علىتقرير نيلسون ديسمبر 2023

حقق الاحتيال في جميع انحاء العالم على العلامات التجارية وبطاقات الصراف الالي 33,45 مليار دولار في سنة 2022 ، بحجم إجمالي قدر 49,149 مليار دولار(rebertson, card fraud worldwide, 2023, p. 6)، كما يتوقع ان يسجل حجم الاحتيال حوالي 35،79 مليار دولار في سنة 2024 ، و حوالي 39،60 مليار دولار في سنة 2026 ، ويتوقع في سنة 2028 حوالي 43،47 مليار دولار من اجمالي المعاملات ، نلاحظ أن حجم الاحتيال المتوقع في تزايد مستمر وهذا اعتمادا على المعطيات والاحصائيات للسنوات السابقة و بناءا على تصور توسع حجم المعاملات باستخدام البطاقات وهذا راجع لرواج وانتشار استعمال الوسائل الحديثة للدفع لما تقدمه من مزايا للمتعاملين بها، ومن زاوية أخرى زادت أساليب واشكال الاحتيال على البطاقات بفعل هذا التقدم التكنولوجي.

III. الأساليب الحديثة للكشف والوقاية من الاحتيال على البطاقات الائتمانية:

أدى تطور التكنولوجيا المالية على مستوى العالمي الى اشتداد المنافسة، وابتكار تطبيقات عديدة وسعت من خدمات ونطاق عمل الجهاز المصرفي، الا ان هذا التطور صاحبه العديد من المخاطر التقنية والفنية، وكذا مخاطر الاحتيال والتزوير والسرقة، الا ان تطبيق الذكاء الاصطناعي اعطى قفزة نوعية في هذا المجال، حيث أصبحت معظم البنوك تتبنى هذه التقنية نظرا لمزايا التي تحققها من دقة وسرعة الأداء، خفض التكاليف وتقليل المخاطر.

III – 1تعريف الذكاء الاصطناعي: يعدالذكاء الاصطناعي قفزة نوعية في عالم البرمجيات وتكنولوجيا المعلومات اجتاح جميع مجالات الحياة، ولا يفوتنا ان ننوه أنه مصطلح قديم النشأة ظهر في سنوات الخمسينات، استعمل هذا المصطلح كأول مرة في مؤتمر جامعة دارت مورث عام 1956(بوبحة، 2022، صفحة 91)، بعدها تعددت التعاريف حول الذكاء الاصطناعي نذكر منها:

الذكاء الاصطناعي يعتبر فرع من فروع العلوم، يهتم بالآلات التي تستطيع حل المسائل التي يعتمد الانسان عند حلها على ذكائه (الفرا، 2012، صفحة 3).

الذكاء الاصطناعي فرع من الاعلام الآلي يهدف الى اعداد برامج تنسخ سلوكيات إنسانية سميت بالذكية، كتحليل المحيط، حل المشكلات واتخاذ القرارات (عزوز و.، 2022، صفحة 60)، ومن هنا انطلق مفهوم الذكاء الاصطناعي من مبدأ محاكاة الانسان في طريقة تفكيره ومنطقه، حيث انتقل من فكرة الآلة الذكية الى حيز تطبيق برامج أولى قادرة على التعلم والتطور بالتعامل مع العنصر البشري .

ومما سبق يمكن تعريف الذكاء الاصطناعي على أنه فرع من فروع الاعلام الآلي يختص ببرمجة وتزويد الألة ببعض خصائص الإنسان كالتحليل والربط من أجل جعل تعلم وابداع الكمبيوتر أكثر ذكاء لتكميل وتسهيل العمل الإنساني.

III – 2أهداف الذكاء الاصطناعي: الهدف الأساسي من الذكاء الاصطناعي هو إدخال خوارزميات على الآلات لإنشاء المخرجات المرغوبة، و فيا يلي بعض الأهداف الأخرى (بن علي، 2023، صفحة 46):

- ✓ حل المشكلات من أجل جعل الحياة أسهل وأبسط واجراء استنتاجات منطقية تحاكي التفكير البشري.
  تمثيل المعرفة عن طريق استخدام الآلات لمجموعة من العلاقات من العالم الحقيقي من أجل حل مشاكل الحياة الواقعية المعقدة.
- ✓ التخطيط ووضع توقعات مستقبلية عن طريق روبوتات من أجل إدارة المخاطر.
- ✓ الذكاء الاجتماعي من خلال تطوير الأنظمة لتمكينها من تفسير ومعالجة ومحاكاة العقل البشري، كقراءة تعابير الوجه، لغة الجسد، تغيرات الصوت والتفاعل مع البشر.
- ✓ الابداع من خلال نقل كميات هائلة من المعلومات وتقديم خيارات وبدائل وفرص إبداعية يمكن من خلالها اختيار الحلول المناسبة للمشاكل.
- ✓ الذكاء العام حيث أصبحت الآلة تجمع بين المهارات المعرفية البشرية وتؤدي معظم المهام بكفاءة أفضل من الانسان مما يساعد على تحرير الانسان من أداء المهام الخطرة.
- ✓ فهم الذكاء الإنساني عن طريق تصميم لحاسب آلي قادر على محاكاة السلوك الإنساني في المتسم بالذكاء (شيلي، 2023، صفحة 86).
- ✓ توليد وتطوير معارف، خبرات جديدة، تفعيل المعرفة واستخدامها في اتخاذ القرارات.

III – 3خصائص الذكاء الاصطناعي: يتميز الذكاء الاصطناعي بمجموعة من الخصائص جعلت منه استثمارا ذو فعالية عالية في كثير من المجالات، من بين هذه الخصائص نذكر ما يلي:

- ✓ تطبيق الذكاء الاصطناعي على الأجهزة والآلات، حيث يمكنها من التخطيط وتحليل المشكلات باستخدام المنطق.
- ✓ يتعرف على الأصوات، الكلام واللغات.
- ✓ تستطيع الأجهزة المبرمجة بالذكاء الاصطناعي من فهم المدخلات وتحليلها جيدا، وبعدها تقديم مخرجات تلبي حاجات المستخدم بكفاءة عالية.
- ✓ يمكن من التعلم المتواصلبحيث تكون عملية التعلم آلية وذاتية دون خضوعه لمراقبة والاشراف؛
- ✓ يستطيع معالجة الكم الهائل من المعلومات المعروضة عليه في وقت وجيز؛
- ✓ يستطيع تحديد الأنماط المتماثلة في البيانات وتحليلها بفعالية تفوق الادمغة البشرية؛
- ✓ يستطيع إيجاد حلول للمشاكل غير مألوفة باستخدام قدراته المعرفية(صيمود و دهماني ، 2022، صفحة 91)؛
- ✓ التعرف على الوجه فله القدرة على معرفة الوجوه الفردية حيث أحدث تطورات في تقنيات المراقبة؛
- ✓ يوفر نافذة المحادثة عن طريق روبوتات المحادثة لحل مشكلات العملاء(بن علي، 2023، صفحة 45).

III – 4استخدام الذكاء الاصطناعي في البنوك والمؤسسات المالية: تعددت تطبيقات الذكاء الاصطناعي وتختلف باختلاف المجال المطبقة فيه، وكذلك حسب الأهداف المرجوة منه، فيما يلي سنعرض أهم تطبيقات الذكاء الاصطناعي المطبقة في البنوك والمؤسسات المالية بغض النظر عن الامن السيبراني الذي سنتطرق اليه لاحقا:

-التصنيف الائتماني: تعتمد البنوك عند قياس الجدارة الائتمانية لعملائها على العديد من النماذج الإحصائية، التحليل الاحصائي و شجرة القرار لتقدير مخاطر الائتمان للمقترض وتحديد درجة ملائته، الا ان استخدام تقنيات الذكاء الاصطناعي قدمت دقة اكبر في دراسة الائتمان وقللت المخاطر الناجمة عنه، من خلال تبني نموذج أفضل للتقييم الائتماني يساعد البنوك على تنمية الاعمال الائتمانية (بوحنك، 2024، صفحة 174).

-روبوتات المحادثة (الشات بوت): و هي أكثر التطبيقات شيوعا لأنها تسمح بالتواصل الدائم مع الزبائن لتلبية طلباتهم في كل وقت و في أي مكان، فالشات بوت هو برنامج لمحاكاة المحادثة البشرية مما يجعل الزبائن يتفاعلون معه بنفس الطريقة التي يتفاعلون بها مع البشر، فزاد توجه المؤسسات الأئمة في معالجة الاستفسارات المتكررة الواردة، مما يخفف عبئي العمل على موظفي الخطوط الأمامية في البنوك (حريري و ديدوش، 2022، صفحة 313).

-مكافحة غسيل الأموال: تتوجه معظم البنوك الكبرى في جميع انحاء العالم لتبني أنظمة وبرامج قائمة على الذكاء الاصطناعي لأنها اكثر قوة وذكاء في مكافحة غسيل الأموال، وتقدم نتائج سريعة ودقيقة (حريري و ديدوش، 2022، صفحة 312).

III -5تطبيق الامن السيبراني لكشف الاحتيال على البطاقات الائتمانية:

يعتبر الأمن السيبراني من أهم تطبيقات الذكاء الاصطناعي، حيث يمثل الحل الامثل لصد الهجمات الالكترونية وضمان السلامة الرقمية للبنوك والمؤسسات المالية:

الأمن السيبراني هو عبارة قوانين، أدوات، نصوص، آليات الأمن، أساليب إدارة لمخاطر والممارسات الفنية المتعلقة بتكنولوجيا المعلومات والاتصالات المستعملة لحماية مصالح الدول والأشخاص، بهدف الدفاع ضد التهديدات والتهجمات المتعمدة كقرصنة المعلومات والبيانات(قطاف و بوقرين، 2022، صفحة 42).

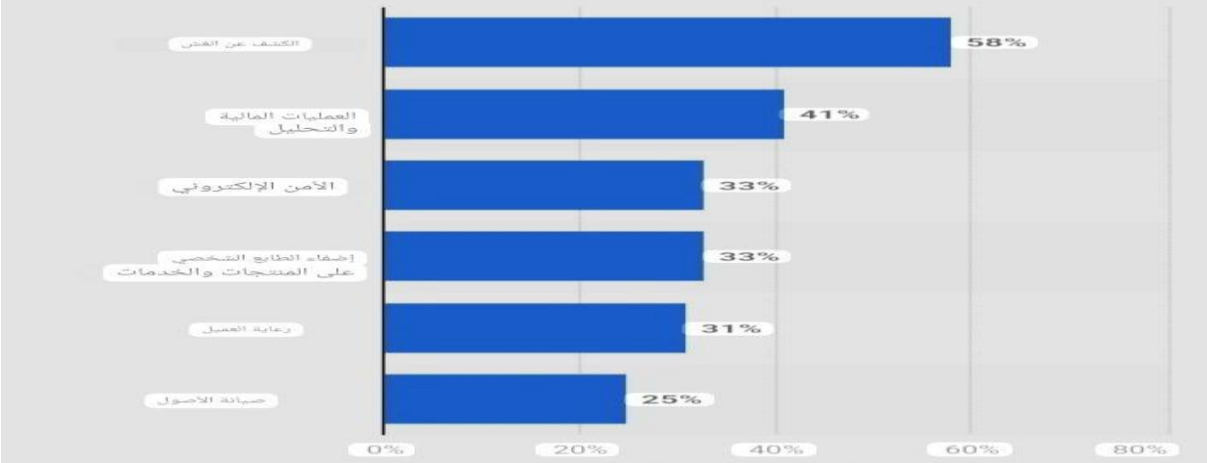
كما يعرف الامن السيبراني على انه ممارسة حماية أجهزة الكمبيوتر، الشبكات، التطبيقات، البرامج والأنظمة من التهديدات الرقمية المحتملة (جغل و زقرير عادل، 2023، صفحة 308).

اذن الأمن السيبراني هو آلية حديثة متطورة تحاكي العقل البشري تعمل على حماية البيانات والمعلومات السرية من مختلف الهجمات الالكترونية.

ويمكن تلخيص تقنيات الأمن السيبراني الحديثة في النقاط التالية(بن علي، 2023، صفحة 53):

- مبدأ انعدام الثقة: هو مبادئ الأمن السيبراني الذي يقوم على عدم الوثوق بأي تطبيقات أو مستخدمين تلقائيا، فهو يعتمد على رقابة صارمة في جميع تعاملاته.
- تحليلات السلوك: عن طريق مراقبة عملية نقل البيانات من الأجهزة والشبكات لاكتشاف العمليات المشبوهة والانحرافات المسجلة.
- نظام كشف التسلل: هو نظام تحديد الهجوم السيبراني والاستجابة له بسرعة، وكذلك تحديد آلية الدفاع ضد التسلل في حالة وقوعه ومساعدة فريق الأمن على اكتشاف مصدره.
- التشفير السحابي: يعمل على تشفير البيانات قبل تخزينها في قواعد البيانات السحابية مما يمنع الأطراف الدخيلة من سرقة واستعمال هذه البيانات.

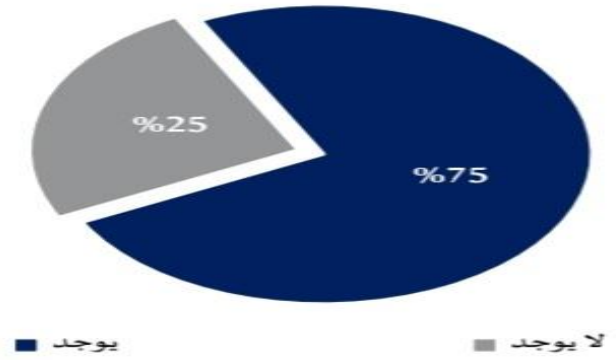
شكل 04: حالات استخدام الذكاء الاصطناعي في صناعة الخدمات المالية في العالم سنة2020



المصدر:من اعداد الباحثين بالاعتماد على:Statista 2020(بن الضب، 2023، صفحة 21)

من خلال الشكل نلاحظ ان اعلى نسبة استخدام للذكاء الاصطناعي في سنة 2020 كانت للكشف عن الغش والاحتيال، حيث بلغت 58% ويرجع هذا لفعالية التطبيق في كشف عن الاحتيال في المعاملات المالية ومنحه الثقة والأمان للبنوك والمتعاملين، كما سجل استعمال الذكاء الاصطناعي بنسبة 41% في إدارة العمليات المالية عن طريق تسيير المحافظ المالية والاستثمارات المالية، وبنسبة 33% استخدم لأغراض الحماية والامن الالكتروني كالأمن السيبراني، وبنسبة 33% لإضفاء الطابع الشخصي على المنتجات والخدمات ، وبنسب أقل فيما يخص رعاية العميل وصيانة الأصول.

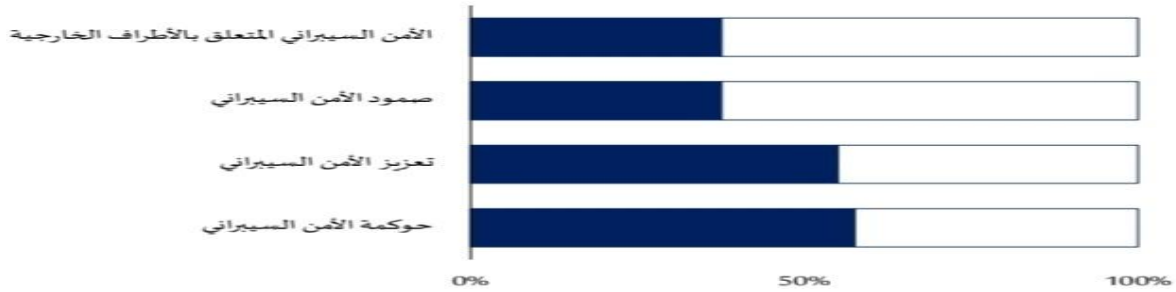
شكل 05: نسبة التشريعات المتعلقة بالأمن السيبراني المتخذة من طرف البنك المركزي في البلدان العربية.



المصدر:من اعداد الباحثين بالاعتماد على تقرير صندوق النقد العربي2023(الحميدي، 2023، صفحة 214)

من خلال الشكل نلاحظ ان البنوك المركزية في الدول العربية تقوم باجتهادات جبارة، حيث تخصص نسبة 75% من التشريعات تتعلق بالأمن السيبراني، الا انه لا يقف الامر على اصدار التشريعات والتعليمات فقط، وانما يتطلب وضع آليات خاصة بالمتابعة والتنفيذ، وتفعيل عملية الرقابة، من اجل تحقيق نتائج أفضل.

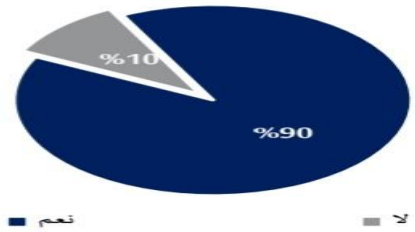
شكل 06: الضوابط السيبرانية حسب الأولوية من وجهة نظر البنوك المركزية للدول العربية



المصدر:من اعداد الباحثين بالاعتماد على تقرير صندوق النقد العربي 2023(الحميدي، 2023، صفحة 214)

ترى البنوك المركزية في الدول العربية ان إعطاء الأولوية في وضع الضوابط السيبرانية لحكومة الأمن السيبراني بنسب تفوق 50%، من اجل خلق بيئة عمل تتسم بالشفافية والمصداقية، ثم تعزيز الأمن السيبراني بنفس الدرجة 50% من اجل التصدي للهجمات السيبرانية ومنع الاختلاسات لحماية أصحاب المصالح، وبعدها الأمن السيبراني المتعلق بالأطراف الخارجية وصمود الامن السيبراني بنسب تقارب 40%.

شكل 07: تقديم برامج تدريبية خاصة بالأمن السيبراني من طرف البنوك المركزية في الدول العربية



المصدر: من اعداد الباحثين بالاعتماد على تقرير صندوق النقد العربي2023(الحميدي، 2023، صفحة 217)

تقوم البنوك المركزية في الدول العربية بعمليات تدريب لموظفيها في مجال الامن السيبراني بنسبة 90%، بالإضافة الى تقديم برامج تعليمية لإدارة المخاطر السيبرانية، وعرض الإجراءات الأمنية للتحكم في هذه المخاطر، واحتواء هذه الانحرافات في الوقت المناسب لتقليل من حدة الخسائر.

رغم الجهود المبذولة من طرف الدول، البنوك، المؤسسات المالية، التجار والافراد، حرصا على كبح عمليات الاحتيال على البطاقات الائتمانية، إضافة الى التطبيقات الحديثة الا انه لا يمكن ردع هذه الاختلاسات بصفة قطعية، ولاكن يجب تظافر جهود جميع البنوك المركزية والبنوك والمؤسسات المالية والحكومات على منع هذه الاختلاسات وتوفير حماية لعملائهم، فيما يلي سنعرض اهم الهجمات السيبرانية التي تواجه المؤسسات المالية في الدول العربية.

شكل رقم08: اهم الهجمات السيبرانية التي تواجه المؤسسات المالية في الدول العربية

المصدر: من اعداد الباحثين بالاعتماد علىتقرير صندوق النقد العربي 2023 (الحميدي، 2023، صفحة 212)

ان تبني القطاع المالي والمصرفي لتقنيات مالية متطورة كالأمن السيبراني ينتج عنه العديد من المخاطر ابرزها الهجمات السيبرانية المختلفة، من خلال الشكل السابق نلاحظ ان أكثر الهجمات السيبرانية التي تواجه المؤسسات المالية في الدول العربية هي هجمات التصيد والهندسة الاجتماعية بنسبة تفوق 50% من اجمالي الهجمات وتكون عن طريق رسائل الكترونية نصية او عبر البريد الالكتروني، اما البرمجيات الخبيثة هي سرقة بيانات دخول المستخدمين الى المنصات المختلفة كالدفع الالكتروني او أنظمة الخدمات المصرفية عبر الأنترنت او ارقام حسابات او بطاقات مصرفية، وتمثل نسبة قريب من 50% من الهجمات، اما هجوم حجب الخدمة يقصد به ارسال ملايين من الطلبات الالكترونية غير الشرعية الى المواقع المصرفية بحيث تمنع المستخدمين الشرعيين من الدخول الى الأنظمة لفترة من الزمن، بسبب انشغال هذه الأنظمة بهذه الطلبات غير الشرعية مما يؤدي الى خسائر مالية كبيرة، وتمثل حوالي 40 %، كما تمثل هجمات الاحتيال وسرقة الهوية حوالي 35%، وتمثل خدمات الجهات الخارجية غير الامنة حوالي 20%من الهجمات، لذلك لابد من السلطات تكثيف الجهود الرقابية لمواجهة هذه المخاطر السيبرانية الناتجة عن التشابك في الفضاء السيبراني، فعليها تحقيق المرونة والمتانة السيبرانية في الجهاز المصرفي.

III –6الاجراءات الوقائية لمنع الاحتيال على البطاقات الائتمانية:

تعتبر عملية مكافحة الاحتيال مسؤولية مشتركة بين عدة أطراف أهمها البنك وعملائه، حيث يلعب العميل دور كبير في كشف ومنع الاحتيال وحماية نفسه من خلال الالتزام بإجراءات النصح والارشاد المقدمة سواء من طرف الجهة المصدرة للبطاقات او من طرف الحكومة، فيما يلي نذكر أهم هذه الإجراءات:

6. 1–إجراءات من طرف الجهات الحكومية والتنظيمية:

على الحكومات وضع العديد من التشريعات و اللوائح للحد من الاحتيال على بطاقات الائتمان ، بإلزام الشركات للامتثال للتدابير الامنية المحددة، كأن تطلب من الشركات استخدام تقنية الشريحة و الرقم السري لمعاملات بطاقات الائتمان و الخصم، والتي توفر طبقة إضافية من الأمان مقارنة بالبطاقات التقليدية ذات الشريط الممغنط، كما قد تطلب الحكومات من الشركات بالتقيد بمعايير خاصة لأمن البيانات لمنع اختراق المعلومات لمنع العمليات الاحتيالية والوقاية منها، والحث على استخدام أدوات الخوارزميات وتعلم الآلة لتحليل المعاملات وكشف الانحرافات والمعاملات المشبوهة، ويمكن تلخيص أهم الأنشطة الاحترازية المقترحة فيما يلي (بن الضب، 2023، صفحة 14):

–وضع قوانين لحماية المتعاملين من الاحتيال على البطاقات الائتمانية وفرض عقوبات صارمة على المحتالين.

–القيام برقابة منتظمة وتقييمات للمخاطر لمصدري بطاقات الائتمان.

–وضع معايير ومبادئ ارشادية وتوجيهات لحماية بيانات حامل البطاقة.

–إعداد اللوائح التنظيمية وتحيينها بصفة مستمرة.

–الاستفادة من مزايا التقنيات الحديثة كالذكاء الاصطناعي لبناء أنظمة إنذار حديثة.

–إنشاء نظام مركزي للإبلاغ عن حالات الاحتيال والتحقيق فيها.

–اتباع بروتوكولات فعالة للتحقق من الهوية للمعاملات عبر شبكة المعلومات العالمية للتقليل من مخاطر انتحال الهوية.

–إعداد معايير أمن عالمية تكون منسجمة ومتوافقة مع التطبيق الجغرافي المتسع والممتد على أوسع نطاق في العالم، خاصة تطوير وتجديد معايير الامن بالتعاون بين الحكومات والمنظمات والمنتجين والموردين والمستخدمين لنظم المعلومات (بولحية و سويح ، 2019، صفحة 44).

6. 2–إجراءات من طرف البنوك والمؤسسات المالية:

تعتبر البنوك والمؤسسات المالية المسؤولة عن معالجة المعاملات والموافقة عليها، فلا بد عليها من حماية عملائها باتخاذ تدابير احترازية للحد من مخاطر الاحتيال والتزوير على بطاقات الائتمان، ومنع الوصول غير المصرح به الى المعلومات الحساسة وضمان الأمان والسرية.

تقوم البنوك و المؤسسات المالية باتخاذ تدابير وقائية قبلية لحماية المعلومات الشخصية و المالية للعملاء نذكر منها (بن الضب، 2023، صفحة 15):

-تنفيذ إجراءات متطورة لأمن البيانات مثل التشفير والتخزين الآمن لحماية المعلومات والبيانات الحساسة.

-استخدام أدوات الكشف عن الاحتيال والوقاية منه مثل تعلم الآلة والذكاء الاصطناعي لمراقبة المعاملات في الوقت المناسب وكشف المعاملات المشبوهة.

-توعية العملاء بتقديم نصائح وارشادات لحماية أنفسهم من الاحتيال.

-تقديم توجيهات بشأن انشاء كلمات المرور، والتحلي باليقظة تجاه الرسائل البريد الالكتروني والمكالمات الهاتفية المشبوهة.

-تجميد البطاقة هو اجراء تقوم البنوك والمؤسسات المالية على العديد من البطاقات الائتمانية كإجراء احترازي بسبب شكها في وجود عمليات مشبوهة للوقاية من عمليات الاحتيال.

-تغيير الرقم السري هو اجراء نظامي تحث عليه البنوك والمؤسسات المالية لضمان أمان حسابات عملائها.

-يجب ان يعتمد البنك على إجراءات للتأكد من صحة وسلامة العمليات المصرفية الالكترونية، واتخاذ وسائل كفيلة بحماية أنظمة الدفع الالكتروني(صواق، بوداود ، و حيمودة، 2023، صفحة 359).

-تقديم إرشادات وتعليمات للعملاء حول عملية السحب من الموزعات الالية (شايب و بارك، 2011، صفحة 80).

-التنبيه بالتأكد من عدم وجود أي شخص يراقب العميل اثناء ادخال الرمز السري.

-النصح بكتابة الرقم السري بسرعة مستخدما اليدين في نفس الوقت لتضليل المترصدين.

-الارشاد بعد استخدام البطاقة من التأكد من وضعها على الفور في مكان آمن.

-التحذير إذا لوحظ انه تم العبث بجهاز الموزع او الشباك الآلي يجب ابلاغ السلطات المعنية.

-إذا علقت البطاقة في الجهاز يجب ابلاغ على الفور البنك لكي يقوم بتجميدها.

-اجتناب استخدام أجهزة الموزعات الآلية للأوراق النقدية في الليل.

6. 3-إجراءات من طرف التجار:

على التجار القيام بالعديد من الإجراءات الاحترازية لمنع عمليات الاحتيال نذكر منها(بن الضب، 2023، صفحة 16):

-استخدام نظام دفع آمن مصمم للحماية من الاحتيال كالتشفير لمنع الاطلاع على المعلومات المهمة.

-التحقق من هوية حامل البطاقة كطلب معلومات إضافية مثل رقم التعريف الشخصي أو الرمز البريدي أو رمز الأمان.

-استخدام أدوات الكشف عن الاحتيال كوضع علامة على المعاملات المشبوهة.

-مراقبة المعاملات بانتظام للكشف على أي نشاط مشبوه.

-تدريب الموظفين عن كشف الاحتيال لتحقق من هوية حامل البطاقة، كيفية استخدام أدوات الكشف، الإبلاغ عن أي نشاط مشبوه.

-يجب على التجار الاحتفاظ بسجلات جميع المعاملات.

-تأمين المعدات الخاصة بهم مثل قارئات البطاقات وأجهزة الكمبيوتر وبرامج الحماية من الفيروسات.

6. 4-إجراءات من طرف حاملي البطاقات:

يعتبر حاملو بطاقات الائتمان الفئة المستهدفة من عملية الاحتيال، بحيث يقوم المحتالين باستخدام البيانات الشخصية والمالية الخاصة بالغير للقيام بعمليات السرقة، فيتعين على حامل البطاقة القيام بمجموعة من الإجراءات والتدابير الوقائية لحماية بطاقته وحسابه من أي نوع من أنواع الاحتيال، ويمكن تلخيص أهم هذه الإجراءات في:

-الحرص على عدم إهمال البطاقة ووضعها في مكان يصعب سرقتها أو تضييعها.

-عدم إعطاء البطاقة أو الرمز السري لأي كان وعدم كتابة الرمز على البطاقة.

-يجب إخفاء الوصل الذي يحمل الرقم السري للبطاقة أو اتلافه لمنع الاطلاع عليه.

-حرص صاحب البطاقة على ان لا يكون محاطا بغرباء اثناء ادخال الرقم السري في أجهزة الصراف الآلي.

-مطالبة حامل البطاقة من الجهة المصدرة لعدم قبول وتأكيد عملياته التجارية التي تتعدى السقف المسموح به.

-الابلاغ على الفور الجهة المصدرة للبطاقة والجهات الأمنية في حالة السرقة أو ضياع البطاقة.

-اختيار المحلات التجارية والأماكن الآمنة المعروفة بالثقة وتفادي المحلات المشكوك فيها (برابح، بطاقة الائتمان البنكية والجرائم المتعلقة بها (اطروحة دكتوراه)، 2022، الصفحات 205-206).

-تجنب التعامل مع المواقع غير الآمنة والتحقق من هوية التاجر والمطالبة بالضمانات ان لزم الأمر.

-التحقق والتدقيق في فواتير البيع المقدمة من طرف التاجر قبل التوقيع عليها والاحتفاظ بنسخة منها كدليل.

-إبلاغ الجهة المصدرة في حالة الشك في أي معاملة.

-تجنب الرد على الرسائل قبل التحقق من مصدرها.

-تجنب إرسال البيانات الشخصية المتعلقة بالبطاقة الا إذا كان الارسال مشفر.

IV. النتائج ومناقشتها:

تم التوصل من خلال دراستنا لهذا الموضوع لجملة من النتائج، وتتمثل في النقاط التالية:

-عمليات الاحتيال المالي ظهرت منذ القدم، ولابد من الإشارة ان الاحتيال على البطاقات الائتمانية ظهر مع ظهور هذه الأخيرة، وعرف انتشارا كبيرا، ويرجع هذا لعدة أسباب، فهناك أسباب ترجع للهيئات المصدرة لهذه البطاقات كضعف الأجهزة الأمنية المستعملة، وأخرى ترجع لكل من التجار مستعملي الات الدفع كغياب عنصر الرقابة، دون ان ننسى حاملي البطاقات من أخطاء مرتكبة بسبب نقص الوعي.

-قدم التطور التكنولوجي فوائد عديدة لحياة البشرية ككل، فضلا عن ذلك صاحبه ظهور مخاطر جديدة فلكل اختراع ثغرات يستفيد منها المحتالين، فيستغلون هذا التطور في ممارسات غير مشروعة، من بينها الاحتيال على البطاقات الائتمانية.

-عرف الاحتيال على البطاقات الائتمانية اشكال عديدة وجديدة لم تعرف من قبل، واحدثها يعتمد على وسائل تكنولوجية متطورة.

-الذكاء الاصطناعي سلاح ذو حدين، من جهة يقدم خدمات جبارة بكفاءة وسرعة فائقة تحاكي العقل البشري، ومن جهة أخرى يخلق مخاطر حديثة يصعب التصدي لها.

-ضعف البنية التحتية الرقمية للقطاع المالي، ضعف عمليات الرقابة والتفتيش بالإضافة نقص التشريعات التي تنظم العمليات الرقمية.

-عدم وعي الافراد واهمالهم لإجراءات الحيطة والحذر، عند تعاملهم بوسائل الدفع الالكتروني، ساهم بشكل كبير انتشار عمليات الاحتيال.

V. الخلاصة:

نظرا لتسارع التقدم التكنولوجي وتوجه اغلب الدول نحو التحول الرقمي، الذي أصبح ضرورة حتمية لمواكبة التطورات الراهنة وضمان التنافسية، أدى بالبنوك والمؤسسات المالية الانتقال من الطرق التقليدية الى الطرق الحديثة في معاملاتها المالية، لما توفره لها من جهد ووقت وتكاليف، الا انها كانت عرضة لعدة اختلاسات التي تعتبر وليدة هذا التطور، حيث تطورت اشكال الاحتيال بصفة عامة على المعاملات المالية وبصفة خاصة على وسائل الدفع الحديثة.

استنادا الى ما سبق يمكن الاجابة على إشكالية البحث بأن هنالك عدة طرق واجراءات كفيلة بأن **يساهم الذكاء الاصطناعي في الكشف والحد من الاحتيال على البطاقات الائتمانية سواء اكانت تشريعات قانونية او برامج تكنولوجية متقدمة أو أساليب مدعمة ببرامج الحماية والامن السيبيراني.**

اقتراحات الدراسة:

بناءا على ما تم التوصل اليه من نتائج يمكن اقتراح مجموعة من الاقتراحات المتمثلة في:

-على الدول خلق بيئة رقمية تسهل انتشار واستخدام الذكاء الاصطناعي، من خلال توفير بنية تحتية متينة قائمة على تكنولوجيا المعلومات والاتصال.

-تحديث القوانين تماشيا مع تطورات الذكاء الاصطناعي لضمان حماية الأطراف المعنية، وغرس الثقة في نفوس المتعاملين.

-العمل على انشاء مراكز بحث متخصصة في الذكاء الاصطناعي من اجل إعطاء برامج ذو كفاءة أعلى بمخاطر اقل.

-تثقيف افراد المجتمع بمفهوم الذكاء الاصطناعي واهمية تطبيقه وكذا توعيتهم للحذر من مختلف مخاطره، ونشر ثقافة الامن السيبراني لتفادي المخاطر المدركة خاصة في معاملاتهم المالية.

-توعية العملاء اصحاب البطاقات بإبلاغ فورا الجهات المصدرة للبطاقات في حالة التعرض للاحتيالالإيقاف جميع الخدمات المتعلقة بالحساب البنكي.

-ضرورة تطوير أدوات الامن واتخاذ إجراءات وتدابير تعتمد على الامن السيبراني، وابتكار أنظمة جديدة لكشف الاحتيال لحماية الخدمات المصرفية والمالية الالكترونية.

-اهمية الاستثمار في أفضل وسائل الحماية التقنية المعتمدة على أحدث التكنولوجيا، لجعل البنية التحتية متينة وقوية، والتأهب للمشاكل الفنية الممكن التعرض لها للتقليل من المخاطر.

-الاهتمام بالعنصر البشري لأنه رغم التطور يبقى هو الأساس في سير العمل المصرفي من خلال إقامة دورات تعليمية وتكوينية في المجال الالكتروني والذكاء الاصطناعي والامن السيبراني.

-إعطاء أهمية أكبر لإدارة المخاطر في البنوك، وتطبيق الحكومة البنكية، من اجل نشر روح المسؤولية بين الموظفين.

-تعزيز التعاون الدولي لمكافحة الاحتيال المالي، من خلال تبادل الخبرات والعمل على اعداد قوانيين وتشريعات ولوائح دولية، حرصا على مواجهة هذه الجرائم العابرة للحدود.

آفاق الدراسة: يمكننا اقتراح مواضيع بحثية مستقبلية ومن ضمنها:

- ✓ تعزيز تقنية الذكاء الاصطناعي المدمج بالأمن السيبيراني في المعاملات البنكية.

- ✓ تقييم استخدام أنواع البطاقات البنكية المستهدفة من الاحتيالفي الجزائر.
- ✓ المنظومة القانونية الدولية ودورها في الحد من الاحتيال الالكتروني في المعاملات الدولية.
- ✓ التوجه المعاصر في وسائل الدفع الحديثة للمعاملات المالية الدولية.

VI. المراجع

المراجع العربية :

1. آسية بن عزوز، و ميلود بن عبد العزيز. (2022). جريمة الاحتيال المالي في ظل تكنولوجيا المعلومات. مجلة الدراسات المالية والمحاسبية والادارية، 9(1)، الصفحات 1364-1378.
2. البنك المركزي الاردني. (2023). دليل التوعية في الاحتيال المالي باستخدام الوسائل الالكترونية. (البنك المركزي الاردني، المحرر) الاردن: دائرة حماية المستهلك المالي ووجدة الاستجابة للحوادث السيبرانية للقطاع المالي و المصرفي. تاريخ الاسترداد 25 مارس, 2024، من https://www.jordanislamicbank.com/ar/awareness-guide-on-methods-of-financial-fraud
3. الهام شيلي. (2023). تسيير الموارد البشرية في ظل تحديات تطبيق الذكاء الاصطناعي. مجلة ارصاد للدراسات الاقتصادية و الادارية، 6(1)، الصفحات 79-94.
4. جميلة جغل، و زقرير عادل. (2023). الامن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (تهديدات سيبرانية،اليات التحوط). مجلة التنمية الاقتصادية، 8(1)، الصفحات 303-319.
5. خديجة امان عماروش. (2017). بطاقات الائتمان في الجزائر-دراسة حالة بطاقة فيزا للدفع المسبق لبنك التنمية المحلية BDL.مجلة الادارة والتنمية للبحوث والدراسات، 12(24)، الصفحات 204-220.
6. سعاد بوبحة. (2022). الذكاء الاصطناعي تطبيقات وانعكاسات. مجلة اقتصاد المال والاعمال، 6(4)، الصفحات 85-108.
7. سليمان قطاف، و عبد الحليم بوقرين. (2022). الامن السيبراني والمضامين المفاهيمية المرتبطة به. مجلة طبنة للدراسات العلمية الاكاديمية، 5(2)، الصفحات 37-56.
8. سليمان يعقوب الفرا. (2012). الذكاء الاصطناعي. مجلة البدر، 4(1)، الصفحات 3-6.
9. سمية بن علي. (2023). مساهمة الذكاء الاصطناعي في الكشف عن الاحتيال في القطاع المصرفي باستخدام الامن السيبراني بنك Danskeالدنماركي نموذجا. مجلة ابعاد اقتصادية، 13(2)، الصفحات 39-63.
10. شهيرة بولحية، و دنيازاد سويح . (2019). الاحتيال الالكتروني. مجلة الدراسات القانونية والاقتصادية، 2(2)، الصفحات 37-46.
11. عبد القادر صواق، بومدين بوداود ، و عبد اللطيف حيمودة. (2023). اثر جاهزية الامن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة-دراسة حالة بنك BDLبغرداية-. مجلة ابحاث اقتصادية معاصرة، 6(1)، الصفحات 353-372.
12. عبد الله بن عبد الله الحميدي. (2023). تقرير الاستقرار المالي في الدول العربية. الامارات العربية المتحدة: صندوق النقد العربي. تاريخ الاسترداد 20 مارس, 2024، من

https://www.amf.org.ae/ar/publications/tqryr-alastqrar-almaly/tqryr-alainstqrar-almaly-fy-aldwl-alrbyt-lam-2023

13. عبدالرحمان محمد قدري حسن. (2011). جرائم الاحتيال الالكتروني. مجلة الفكر الشرطي، 20(79)، الصفحات 55-147.

14. عبدالغني حريري، و هاجرة ديدوش. (2022). تطبيق الصيرفة الالكترونية والذكاء الاصطناعي في بنك التوفير والاحتياط -دراسة حالة المديرية االجهوية بالشلف-. مجلة الادارة والتنمية للبحوث والدراسات، 11(1)، الصفحات 305-325.

15. علي بن الضب. (2023). دور الذكاء الاصطناعي وتعلم الالة في كشف الاحتيال على البطاقات الائتمانية. الامارات العربية المتحدة: صندوق النقد العربي. تاريخ الاسترداد 10 افريل, 2024، من https://www.amf.org.ae/ar/publications/drasat-ttwyr-alqta-almaly-walmsrfy/dwr-aldhka-alastnay-wtlwm-alat-fy-tzyz-kshf

16. ليندة صيمود، و سهيلة دهماني . (2022). الذكاء الاصطناعي تقنية رقمية تقود الى ابتكار تجربة تعليمية ناشئة في الجزائر-شركة انكيديا نموذجا-. مجلة رقمنة للدراسات الاعلامية والاتصالية، 2(2)، الصفحات 87-97.

17. محمد شايب، و نعيمة بارك. (2011). الوقاية من تزوير بطاقات الدفع الالكترونية كالية للحد من الفساد المالي في البنوك والمؤسسات المالية -حالة فرنسا-. مجلة دفاتر اقتصادية، 2(1)، الصفحات 68-94.

18. مريم عبدالكافي، و صورية بورابة. (2022). جريمة الاحتيال المعلوماتي الواقعة على البطاقات المالية الالكترونية. مجلة القانون والعلوم السياسية، 8(1)، الصفحات 406-427.

19. مصطفى عمراني. (2017). جريمة تزوير البطاقات البنكية. مجلة الدرسات والبحوث القانونية، 2(5)، الصفحات 298-330.

20. هدى برابح. (2021). مزايا ومخاطر استخدام العامل لبطاقة الائتمان البنكية. مجلة قانون العمل والتشغيل، 6(1)، الصفحات 243-260.

21. هدى برابح. (2022). بطاقة الائتمان البنكية والجرائم المتعلقة بها (اطروحة دكتوراه). كلية الحقوق والعلوم السياسية، مستغانم: جامعة عبد الحميد بن باديس .

22. هدى بوحنك. (2024). اثر تبني البنوك لتقنيات الذكاء الاصطناعي دراسة حالة بنك ICIC. مجلة الرسالة للدراسات والبحوث الانسانية، 8(4)، الصفحات 169-184.

23. وهيبة حنان عزوز. (2022). الذكاء الاصطناعي نحو افاق جديدة. مجلة وهران2، 7(1)، الصفحات 56-65.

المراجع الأجنبية:

1. rebertson, D. (2022, december). card fraud worldwide. Etats-unis: Nilson report. Retrieved Avril 1, 2024, from https://nilsonreport.com/newsletters/1232/
2. rebertson, D. (2023). card fraud worldwide. Etats-unis: Nilson report. Retrieved Avril 1, 2024, from https://nilsonreport.com/newsletters/1254/
3. robertson, D. (2021, December). card fraud worldwide. Etats-unis: Nilson report. Retrieved Avril 1, 2024, from http://nilsonreport.com/newsletters/1209/

References translated from Arabic:

1. Asiya Benaazouz, & Miloud Ben Abdel Aziz. (2022). Financial fraud crime in the shadow of information technology. Journal of Financial, Accounting and Administrative Studies, 9(1), pp. 1364-1378.
2. Central Bank of Jordan. (2023). Awareness guide on financial fraud using electronic means. (Central Bank of Jordan, Ed.) Jordan: Department of Consumer Financial Protection and Financial and Banking Sector Cyber Incident Response Unit. Retrieved March 25, 2024, from https://www.cbj.gov.jo/Pages/viewpage.aspx?pageID=176
3. Elham Chelly. (2023). Human resource management in the face of the challenges of applying artificial intelligence. Journal of Orasd for Economic and Administrative Studies, 6(1), pp. 79-94.
4. Djamila Djahel, & Adel Zaghrir. (2023). Cybersecurity and financial inclusion in the digital transformation of the financial sector (Cyber threats, hedging mechanisms). Journal of Economic Development, 8(1), pp. 303-319.
5. Khadija Amane Amarouche. (2017). Credit cards in Algeria: A case study of the BDL prepaid Visa card. Journal of Management and Development for Research and Studies, 12(24), pp. 204-220.
6. Souad Boubah. (2022). Artificial intelligence applications and reflections. Journal of Money and Business Economics, 6(4), pp. 85-108.
7. Slimane Kattaf, & Abdelhalim Bouguerine. (2022). Cybersecurity and its related conceptual contents. Tabine Journal of Academic Scientific Studies, 5(2), pp. 37-56.
8. Slimane Yacoub Al-Fara. (2012). Artificial intelligence. Al-Badr Journal, 4(1), pp. 3-6.
9. Samia Ben Ali. (2023). The contribution of artificial intelligence to fraud detection in the banking sector using cybersecurity: The case of Danske Bank in Denmark. Economic Dimensions Journal, 13(2), pp. 39-63.
10. Chahira Boualiha, & Djeniazad Souaih. (2019). Electronic fraud. Journal of Legal and Economic Studies, 2(2), pp. 37-46.
11. Abdelkader Saouak, Boumediene Boudoudou, & Abdelatif Haimouda. (2023). The impact of cybersecurity readiness on electronic banking services by reducing perceived risks: A case study of BDL Bank in Ghardaïa. Journal of Contemporary Economic Research, 6(1), pp. 353-372.
12. Abdullah bin Abdullah Al-Hamidi. (2023). Financial stability report in Arab countries. United Arab Emirates: Arab Monetary Fund. Retrieved March 20, 2024, from https://www.amf.org.ae/en
13. Abdelrahman Mohamed Kadry Hassan. (2011). Electronic fraud crimes. Journal of Police Thought, 20(79), pp. 55-147.
14. Abdelghani Hariri, & Hager Didouche. (2022). Application of electronic banking and artificial intelligence in the Savings and Investment Bank: A case study of the regional directorate in Chlef. Journal of Management and Development for Research and Studies, 11(1), pp. 305-325.
15. Ali Ben Dhib. (2023). The Role of Artificial Intelligence and Machine Learning in Detecting Credit Card Fraud. United Arab Emirates: Arab Monetary Fund. Retrieved April 10, 2024, from https://www.amf.org.ae/ar/publications/drasat-ttwyr-alqta-almaly-walmsrfy/dwr-aldhka-alastnay-wtlwm-alat-fy-tzyz-kshf
16. Linda Semaoudi, & Sahila Dahmani. (2022). Artificial intelligence: A digital technology leading to the innovation of an emerging educational experience in Algeria

- Enkydia Company as a model -. Digital Journal of Media and Communication Studies, 2(2), pp. 87-97.
17. Mohamed Shaib and Naïma Bark. (2011). Prevention of Electronic Payment Card Forgery as a Measure to Reduce Financial Corruption in Banks and Financial Institutions - The Case of France. Journal of Economic Notebooks, 2(1), pp. 68-94.
18. Maryam AbdulKafi and Soumeya Bouraba. (2022). Cyber Fraud on Electronic Financial Cards. Journal of Law and Political Science, 8(1), pp. 406-427.
19. Mustafa Omrani. (2017). Crime of Counterfeiting Bank Cards. Journal of Legal Studies and Research, 2(5), pp. 298-330.
20. Huda Brabah. (2021). Advantages and Risks of Using the Employee for Bank Credit Card. Journal of Labor Law and Employment, 6(1), pp. 243-260.
21. Huda Brabah. (2022). Bank Credit Card and Related Crimes (Ph.D. Thesis). Faculty of Law and Political Science, Mostaganem: Abdelhamid Ibn Badis University.
22. Huda Bouhnak. (2024). The Impact of Banks' Adoption of Artificial Intelligence Technologies: A Case Study of ICIC Bank. Journal of Al-Risalah for Humanities Studies and Research, 8(4), pp. 169-184.
23. Hanan Azouz Wahba. (2022). Artificial Intelligence Towards New Horizons. Journal of Oran 2, 7(1), pp. 56-65.