AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

استعمال الذكاء الاصطناعي للحد من الاحتيال المالي في عمليات الدفع الالكتروني

موسى كاظم ابو النص الياسري [1]
Musaqadm@gmail.com

فؤاد محمد عبد التميمي [2]
fouadabd523@uowasit.edu.iq

المديرية العامة لتربية واسط قسم تربية النعمانية

المستخلص

الهدف من هذا البحث، هو تقديم رؤى حول ماهية الذكاء الاصطناعي عبر وسائله وتقنياته وإسهاماته، في مواكبة التطور الحاصل في العمليات المالية والتحول الرقمي، وأثره في الحد من عمليات الاحتيال في عمليات الدفع الالكتروني المختلفة؛ إذ يبين أهم تقنيات الذكاء الاصطناعي المستعملة، كما يسعى إلى توضيح أهم وسائل الدفع الإلكتروني المستعملة في العراق التي أشار إليها البنك المركزي العراقي، مروراً بطرق الاحتيال الإلكتروني محدداً الأشكال المختلفة للأنشطة الاحتيالية التي يجب مراعاتها والحذر منها عند استعمال أي وسيلة دفع الكتروني، وكيفية استعمال تكنولوجيا الذكاء الاصطناعي في تحديد الانماط الشاذة التي غالباً ما تشير إلى عملية احتيالية يتوجب على متخذي القرار إيقافها والتحري منها ، كما يهدف البحث إلى تثقيف الجمهور وتعريفهُ بآليات الدفع الالكتروني وصور الاحتيال المتبعة من لدن المحتالين، وكيفية الحد منها مع بيان دور الذكاء الاصطناعي في الحدِّ من عمليات الاحتيال المالي، وبالخصوص عند التعامل مع كم هائل من البيانات التي في الغالب تشكل بعض التعقيد والتحديات للمدققين في ظل ازدياد العمليات الاحتيالية ، اعتمد الباحث في مجتمع بحثه، إحدى أهم الشركات العاملة في العراق في هذا المجال، وهي الشركة العالمية للبطاقة الذكية المحدودة المختلطة في العراق، وتوصل البحث إلى عدة استنتاجات أهمها: يمكن لتقنيات الذكاء الاصطناعي أن تعزز من إمكانيات الحماية والحد من عمليات الاحتيال المالي في عمليات الدفع الالكتروني إذا برمجت خوارزمياته بصورة تواكب الادوات الاحتيالية الحديثة المستخدمة من لدن المحتالين ، كذلك دائماً ما تكون عمليات الدفع الالكتروني رتيبة في حركاتها، فإن أي تغير شاذ في نمط تلك الحركات في الغالب يكون احتيالي يتوجب إيقاف العملية المالية، كما أن آليات وأدوات التدقيق المعتمدة من الدوائر لا تواكب التطور الحاصل في العمليات المالية، وهذا قد يكون أحد أهم أسباب تفشي ظاهرة الاحتيال المالي .

الكلمات المفتاحية: الذكاء الاصطناعي ،الاحتيال المالي، الدفع الإلكتروني.

Abstract

The aim of this research is to provide insights into the nature of artificial intelligence through its means, techniques and contributions to keeping pace with the development in financial operations and digital transformation and its role in reducing fraud in various electronic payment operations, as it shows the most important artificial intelligence techniques used, and seeks to clarify the most important electronic payment methods used in Iraq, which were referred to by the Central Bank of Iraq, passing through the methods of electronic fraud, specifying the different forms of fraudulent activities that must be taken into account and cautioned against when using any electronic payment method and how to use artificial intelligence technology to identify abnormal patterns that often indicate a fraudulent operation that decision-makers must stop and investigate. The research also aims to educate the public and familiarize them with the mechanisms of electronic payment and the forms of fraud followed by fraudsters and how to reduce them, while stating the role of artificial intelligence in reducing financial fraud operations, especially when dealing with a huge amount of data, which often poses some complexity and challenges for auditors in light of the increase in fraudulent operations. The researcher relied in his research community on one of the most important companies operating in Iraq in this field, which is the Global Company for Smart Cards Limited, mixed in Iraq, and the research reached several Conclusions: The most important of which is that artificial intelligence technologies can enhance the protection capabilities and reduce financial fraud in electronic payment operations if its algorithms are programmed in a way that keeps pace with the modern fraudulent tools used by fraudsters. Also, electronic payment operations are always monotonous in their movements, so any abnormal change in the pattern of those movements is often fraudulent and requires stopping the financial operation. Also, the auditing mechanisms and tools adopted by the departments do not keep pace with the development taking place in financial operations, and this may be one of the most important reasons for the spread of the phenomenon of financial fraud.

Keywords: Artificial Intelligence, Financial Fraud, Electronic Payment.

المحور الأول

منهجيةَ البحثِ والدراساتِ السابقةِ

1-1-مشكلة الدراسة:

وجود قصور في أمان عمليات الدفع الالكتروني، وفي آليات تدقيقها الأمر الذي يزيد من مخاوف مستخدمي بطاقات الدفع الالكتروني من الاحتيال المالي نتيجة الجهل بطرق الاحتيال والوقاية منها .

ويمكن تلخيص مشكلة البحث، في السؤال التالي: هل تؤثر تقنيات الذكاء الاصطناعي على زيادة نسبة الأمان لدى مستخدمي الدفع الالكتروني، وزيادة الاقبال على استعمال تلك الوسائل دون مخاوف حول ضياع اموالهم عن طريق الاحتيال؟

1-2-هدف الدراسة:

هدفت الدراسة إلى تحقيق عدد من الأهداف :

1. معرفة مفهوم تقنيات الذكاء الاصطناعي وأثرها في العمليات المالية .
2. بيان مفهوم الاحتيال المالي في بطاقات الدفع الالكتروني.
3. بيان الطرائق والآليات التي يمكنها أن تعطي أماناً كافياً للزبائن في نظام الدفع الإلكتروني.

1-3-أهمية الدراسة :

تنبع أهمية الدراسة من استعمال التقنيات الحديثة المتمثلة في تقنية الذكاء الاصطناعي في العمليات المالية والتدقيقية في البيئة العراقية، ولتحقيق نسبة عالية من الأمان في بطاقات الدفع الالكترونية الذي يقلل العزوف من استعمال تلك البطاقات ومغادرة الدفع النقدي نهائياً إسوةً بالدول الأخرى .

1-4-فرضية البحث

تقوم فرضية الدراسة على أن هنالك أثر لتقنية الذكاء الاصطناعي في الحد من الاحتيال المالي من خلال توفير وسائل أمان عالية في بطاقات الدفع الالكتروني.

الفرضية:- توجد علاقة ذات دلالة إحصائية بين تقنيات الذكاء الاصطناعي وتقليل نسبة الاحتيال المالي في عمليات الدفع الالكتروني.

المحور الثاني

الذكاء الاصطناعي

2-1-الذكاء الاصطناعي مفهومه وتعريفه:

2-1-1-مفهوم الذكاء الاصطناعي Artificial Intelligence

ارتبط مفهوم الذكاء الاصطناعي بالأجهزة الرقمية أو الإلكترونية مثل؛ اجهزة الكمبيوتر، أو الأجهزة الخلوية أو الروبوتات، كما يشير الذكاء الاصطناعي إلى قدرة هذه الأجهزة الرقمية على أداء المهمات المرتبطة بالكائنات الذكية وينطبق مصطلح الذكاء الاصطناعي على الأنظمة التي تتمتع بالعمليات الفكرية للإنسان مثل؛ المقدرة على التفكير، واكتشاف المعاني والتعلم من التجارب السابقة (عبادة ٢٠٢١، 1)

كما يعد مفهوم الذكاء الاصطناعي من المفاهيم المعاصرة التي أخذت حيزاً تطبيقياً في شتى العلوم والمجالات إلا إنَّ هذا المصطلح ليس جديداً، فقد بدأ تطويرهُ في الخمسينيات من القرن الماضي تقريباً، إذ صيغ هذا المصطلح لأول مرة من لدن McCarthy et al بوصفه علماً وهندسة لصنع آلات الذكية وتطور تعريفه جنبًا إلى جنب مع تطور استعمالاته، ويقوم الذكاء الاصطناعي بتطوير نظام قادر على أداء الوظائف التي تتطلب عادة ذكاء التفكير البشري، مثل الإدراك البصري واتخاذ القرار واللغة والتواصل وهو بطبيعة الحال متسارع جداً في عملية تطوره إلى الحد الذي يشبه فيه ذكاء البشر، فعلى الصعيد المالي كان من بين أهم تطورات الذكاء الاصطناعي هو التطور الهائل في معالجة البيانات الضخمة، الذي يصاحبه بالطبع زيادة في القدرة على تخزين البيانات وإدارتها، فضلاً عن ذلك، زيادة قوة معالجة البيانات (Ikhsan, et al. September 2022, 106) وعلى العموم فإن الذكاء الاصطناعي هو تقنية حاسوبية تعرض شكلاً مشابهاً للذكاء البشري بواسطة العديد من التقنيات المترابطة فيما بينها التي تتمثل باستخراج البيانات ومعالجة اللغات الطبيعية والتعلم الآلي والتعرف على الكلام و الصور، إضافة إلى تحليل المشاعر هذه التقنيات يمكنها أن تعطي الذكاء الاصطناعي القوة في قدرته على التعرف على الأنماط المختلفة وتقديم التنبؤات التي تساعد في اتخاذ القرارات (Seethamraju and Hecimovic 2022, 2).

2-1-2-تعريف الذكاء الاصطناعي

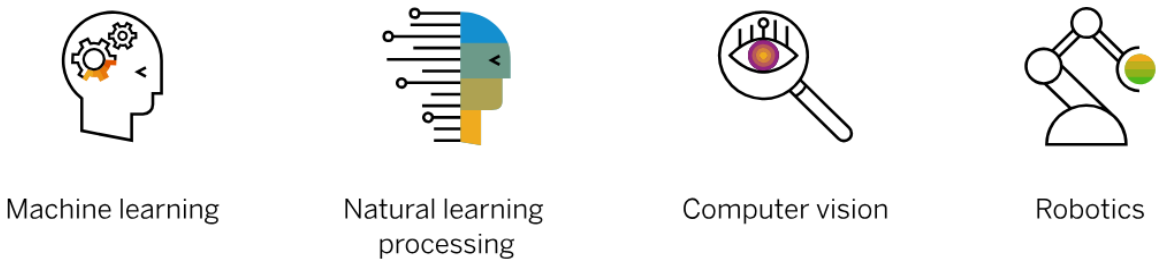
يعرف الذكاء الاصطناعي على أنه مجال علوم الكمبيوتر المتخصص في حل المشكلات المعرفية التي عادةً ما ترتبط بالذكاء البشري، كالتعلم والإبداع والتعرف على الصور، وعرِّفته منظمة التعاون الاقتصادي والتنمية على أنه نظام يقوم على الآلة بإمكانه تقديم تنبؤات أو إعطاء اقتراحات أو أحكام يمكنها أن تؤثر على البيئات الافتراضية أو الفعلية لمجموعة معينة من الأهداف المحددة (Azima Noordin, et al. 2022, 2) كما يشير Rikhardsson إلى أن الذكاء الاصطناعي هو تقنية متعددة الاستعمالات (عامة) تستعمل لتحسين وتغيير استعمال التقنيات والعمليات الأخرى، و الذكاء الاصطناعي في هذا السياق هو مصطلح شامل للتقنيات لجمع وتحليل ومراقبة البيانات المعقدة المنظمة وغير المهيكلة ، لأتمتة المهام والعمليات الرقمية والمادية، تشتمل الذكاء الاصطناعي التقنيات على أدوات وطرق للإدراك البصري والتفسير الصوتي وأنواع قواعد البيانات المختلفة والأساليب الاحتمالية والتعلم الآلي (Rikhardsson, et al. 2022) وعُرفَ الذكاء الاصطناعي أيضاً، بأنه تكنولوجيا معلومات جاهزة يمكنها جمع وتنظيم ومعالجة وتوزيع كميات كبيرة جداً من البيانات في دقائق لغرض إنتاج

معلومات موثوقة ودقيقة مما يساعد المحاسبين والمدققين في تفسير البيانات واتخاذ قرار بناءً على النتائج المترتبة (Adeoye, et al. 2023, 3).

2-2-تقنيات الذكاء الاصطناعي

لا يمكن الاستفادة من الذكاء الاصطناعي إلا اذا كان قابلاً للتطبيق ويمكن له من تحقيق قيمة حقيقية تقدم رؤى واضحة قابلة للتنفيذ، وعند وصف تطور الذكاء الاصطناعي بأنَّه مشابه للذكاء البشري فإن تقنياته هي تماثل مع ما موجود في العقل البشري مع ما يحتويه جسم الانسان من اعضاء ينفذ من خلالها افكاره ، فإن تقنيات الذكاء الاصطناعي تكون مثل اليدين والعينين وحركات الجسم - وكل ما يسمح بتنفيذ أفكار الدماغ، وفيما يلي بعض من تقنيات الذكاء الاصطناعي موضحة بحسب الشكل: (1).

شكل (1) تقنيات الذكاء الاصطناعي



تقنيات الذكاء الاصطناعي :(Pinadero 2024)

1-تعلم الآلة Machine Learning

هو أحد مكونات الذكاء الاصطناعي التي طبقت الخوارزميات على أشكال مختلفة من أساليب التعلم وتقنيات التحليل، التي تجيز للنظام بالتعلم والتحسين التلقائي من التجارب دون الحاجة إلى تدخل المبرمجين بذلك ، وعرف آرثر صموئيل ، التعلم الآلي على أنه مجال الدراسة الذي يمنح أجهزة الكمبيوتر القدرة والقابلية على التعلم دون أن تبرمج بشكل صريح من لدن المبرمجين، وهو على عدة أنواع منها (Mahesh 2018, 2):- وكما مبين في جدول رقم (1).

جدول (1) أنواع تعلم الآلة في الذكاء الاصطناعي

1- التعلم خاضع الإشراف	هو مهمة التعلم الآلي المتمثلة في تعلم وظيفة تقوم بتعيين المدخلات إلى المخرجات بناءً على أزواج المدخلات والمخرجات ، وبذلك فإن خوارزميات التعلم الآلي الخاضعة للإشراف هي تلك الخوارزميات التي تحتاج إلى مساعدة خارجية من قبل المبرمجين.
2-التعلم غير الخاضع	يُسمى هذا بالتعلم غير الخاضع للإشراف لأنه على عكس التعلم الخاضع للإشراف أعلاه لا

للإشراف	توجد إجابات صحيحة ولا يوجد معلم، تُترك الخوارزميات لأدواتها الخاصة لاكتشاف وتقديم البينة المثيرة للاهتمام في البيانات، تتعلم خوارزميات التعلم غير الخاضعة للرقابة بعض الميزات من البيانات، عند تقديم بيانات جديدة، فإنها تستعمل الميزات التي تم تعلمها مسبقًا للتعرف على فئة البيانات.
3-التعلم شبه الخاضع للإشراف	هو مزيج من أساليب التعلم الآلي الخاضعة للإشراف وغير الخاضعة للإشراف، يمكن أن يكون مثمرًا في مجالات التعلم الآلي واستخراج البيانات حيث تكون البيانات غير المسماة موجودة بالفعل ويكون الحصول على البيانات المصنفة عملية شاقة، باستعمال طرق التعلم الآلي الخاضعة للإشراف الأكثر شيوعًا، يمكن تدريب خوارزمية التعلم الآلي على مجموعة بيانات "مُصنفة" يتضمن كل سجل فيها معلومات النتيجة.

ويمكن أن تحدد متى يستعمل التعلم الآلي الخاضع للإشراف أو غير الخاضع للإشراف، بناءً على كمية البيانات، فإذا كانت كمية البيانات قليلة ومصنفة بوضوح للتدريب، فيتم اختيار التعلم الخاضع للإشراف، وفي حال كانت البيات كبيرة فيتم اختيار التعلم غير الخاضع للإشراف .

2- معالجة اللغة الطبيعية(Natural language processing (NLP

في قلب أي مهمة في البرمجة اللغوية العصبية، هناك مسألة مهمة وهي فهم اللغة الطبيعية، تتضمن عملية بناء برامج حاسوبية تفهم اللغة الطبيعية ثلاث مشكلات رئيسية: تتعلق الأولى بعملية التفكير، والثانية بتمثيل ومعنى المدخلات اللغوية، والثالثة بالمعرفة العالمية، وبالتالي؛ قد يبدأ نظام البرمجة اللغوية العصبية على مستوى الكلمة لتحديد البنية المورفولوجيا[1]، والطبيعة (مثل جزء من الكلام، والمعنى) وما إلى ذلك من الكلمة - وبعد ذلك قد ينتقل إلى مستوى الجملة - لتحديد ترتيب الكلمات والقواعد، ومعنى الجملة بأكملها، وما إلى ذلك - ثم إلى السياق والبيئة العامة أو المجال. قد يكون لكلمة أو جملة معينة معنى أو دلالة محددة في سياق أو مجال معين، وقد تكون مرتبطة بالعديد من الكلمات و/أو الجمل الأخرى في السياق المحدد ويمكن أن يستخدم NLP السياق لاستنتاج الموقف، والمزاج، وغيرها من الصفات الذاتية لتفسير المعنى بدقة (Chowdhury 2020, 4).

3-رؤية الكمبيوتر(Computer vision)

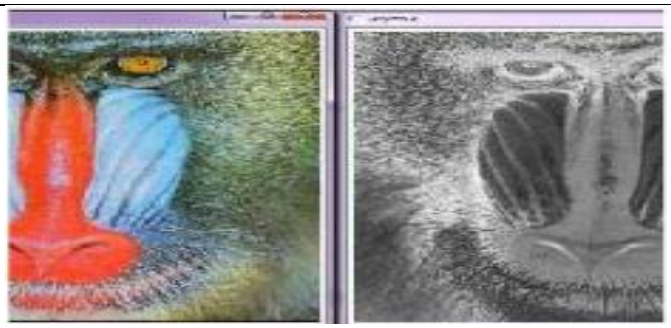
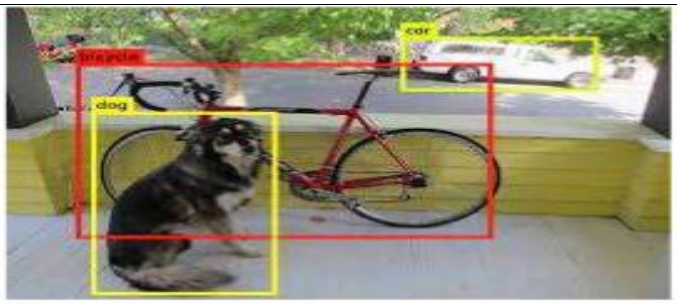
يتم تعريف رؤية الكمبيوتر على أنها مجال الدراسة الذي يركز على تطوير التقنيات لمساعدة أجهزة الكمبيوتر على رؤية وفهم محتوى الصور الرقمية مثل الفيديو والصور، في سياق رؤية الكمبيوتر، هناك طرق مختلفة تكون فيها الآلات قادرة على فهم واستشعار محيطها، اكتشاف كائن واحد مع اكتشاف الكائن، تستطيع الآلة استشعار عناصر الصورة عن طريق

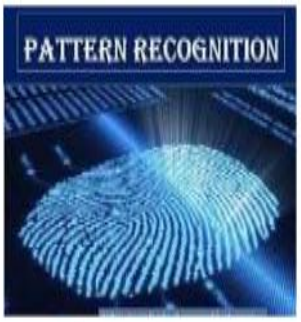
[1] لمورفولوجيا(**Morphology**) العلم الذي يبحث في طرائق بناء الكلمة، وما يطرا على هذا البناء من تغيرات لفظية.

استخراج وحدات البيكسل وتشغيلها على التعلم الآلي أو التعلم العميق، الخوارزمية هي أحد الأمثلة الأكثر شيوعًا لاكتشاف الكائنات وهي التعرف على الوجه. التي تستعمل لتأمين الوصول إلى الهواتف الذكية، يمكن لخوارزميات رؤية الكمبيوتر لإعادة بناء المشهد ثلاثي الأبعاد إعادة بناء كائنات ثلاثية الأبعاد من صور ثنائية الأبعاد مأخوذة من العديد من التطبيقات الأكثر شيوعًا لهذه التقنية في الهندسة المعمارية والتصميم الداخلي ثلاث معالجات مسبقة للصور والفيديو المتقدمة لرؤية الكمبيوتر تكنولوجيًا (Gavari 2022, 1-2). وكما مبين في جدول رقم (2)

جدول (2)

أشكال رؤية الكمبيوتر

1-تجزئة الصورة: - في تجزئة الصورة هي طريقة لتقسيم الصورة الرقمية إلى مجموعات فرعية تسمى أجزاء الصورة، مما يقلل من تعقيد الصورة ويتيح المزيد من المعالجة أو التحليل لكل جزء من الصورة.	
2-اكتشاف الكائنات:- اكتشاف الكائنات هو تقنية رؤية حاسوبية لتحديد مواقع الكائنات في الصور أو مقاطع الفيديو.	
3-التعرف على الوجه: - في التعرف على الوجه للتحقق من وجهنا ثم فتح الهواتف المحمولة الخاصة بك ولأغراض أمنية أخرى لاستعمال هذه الرؤية.	

التعرف على الأنماط: - في هذه الرؤية هناك نوعان الأول هو التعرف على الأنماط والثاني هو التعرف المسبق على الأنماط.	 i) Pattern  ii) fingerprint advance

المصدر: (Gavari 2022)

4-علم التحكم الآلي Robotics

هي فرع من فروع التكنولوجيا التي تتعامل مع تصميم الروبوتات وبنائها وتطبيقاتها، والروبوتات هي آلات تستعمل للقيام بوظائف معينة، إذاً تقوم معظم الروبوتات بعملها بنفسها؛ ويجب أن يكون لدى الروبوتات الأخرى شخص يخبرها بما يجب عليها فعله، ويعرّف معهد الروبوت الأمريكي الروبوتات بأنها "الربط الذكي بين الإدراك والعمل" إذاً هو آلة قادرة على الحصول على المعلومات من محيطها واستعمال المعرفة حول عالمها للتحرك بأمان والعمل بطريقتها الخاصة دون مساعدة الإنسان ، إذ صُممتْ الروبوتات بأجهزة استشعار مغناطيسية قوية، تشبه الدماغ البشري، لغرض استشعار البيئة المحيطة بها والشعور بها ورؤيتها حيثما ينطبق ذلك (Adeoye, et al. 2023, 7).

المحور الثالث

الاحتيال المالي في عمليات الدفع الالكتروني

1-3-مفهوم وتعريف الاحتيال المالي

تعد ظاهرة الاحتيال المالي واحدة من الظواهر المنتشرة عالمياً ، وهو مصطلح عام يتمثل بالحيَل التي يلجأ إليها المجرمين لاستغلال ثقة شخص معين بهدف الحصول على المال، أو على معلومات سرية تمكّنهم من ارتكاب جريمة مالية حالية أو لاحقة ويكون بطرق مختلفة ومحترفة، أخذ الاحتيال بالتطور الديناميكي وفقاً للتطور الحاصل في البيئة المالية حتى وصل إلى طرق تواكب الانتقال من عمليات الدفع التقليدية النقدية إلى عمليات الدفع الالكتروني، ونظراً للنمو السريع في التجارة الإلكترونية الأمر الذي أدى إلى زيادة كبيرة في استعمال أنظمة الدفع الإلكتروني وبالخصوص بطاقات الائتمان في المعاملات اليومية وعبر الإنترنت ونتيجة هذا الارتفاع في المدفوعات الإلكترونية جعل من بطاقات الائتمان هدفًا جذابًا للمحتالين، إذ أشارت البيانات والدراسات المتعلقة بالاحتيال على بطاقات الائتمان أنها أصبحت متنوعة وواسعة الانتشار مع ظهور التسوق عن طريق الإنترنت، ويمكن يكون الاحتيال على بطاقات الائتمان بشكلين: الاحتيال خارج الإنترنت ،والاحتيال عبر الإنترنت (Loukil and Messaoudi 2024, 4).

وعرف الاحتيال بأنه خداع غير مشروع وإجرامي يتم من خلال استعمال طرق ووسائل غير قانونية بهدف تحقيق مكاسب مالية أو شخصية (Diadiushkin, et al. 2019, 74) . والاحتيال المالي هو نشاط إجرامي خفي له تأثير خطير على استقرار الأسواق المالية وثقة المستثمرين (Wang 2024, 1).

1-الاحتيال الاحتيال خارج الإنترنت

يتمثل بسرقة محفظة تحتوي على أشياء ثمينة مثل بطاقات الدفع ووثائق تعريفية أخرى؛ إذ تستعمل بيانات ومعلومات الوثائق المسروقة للابتزاز وسرقة الأموال .

2-الاحتيال عبر الإنترنت

يكون ذلك عندما يستخدم المحتالون منصات عبر الإنترنت أو يقوموا بإنشاء مواقع ويب مزيفة الغرض منها جمع بيانات شخصية حساسة على حساب الزبائن وإجراء معاملات غير مصرح بها ، إذ يقوم المحتالون باستعمال مجموعة متنوعة من الطرق والأساليب لغرض الوصول إلى البيانات الشخصية أو سرقتها، بما في ذلك القرصنة والتصيَد الاحتيالي والاحتيال في الهوية وبرامج التجسس واستنساخ المواقع، واستنساخ البطاقات، والمواقع التجارية المشكوك فيها وغيرها من الطرق الاحتيالية (Dayyabu, et al. 2023, 2).

2-3- طرق الاحتيال

يرجح المختصون أن هنالك ست طرق أساسية يستخدمها المحتالون لارتكاب عمليات الاحتيال في نظام الدفع الإلكتروني (Alabi and David 2023):

1-**الاحتيال الحقيقي (الكلاسيكي):** سرقة معلومات بطاقة الائتمان الخاصة بالضحية أو شرائها عن طريق الإنترنت وهذا هو النوع الأساسي من عمليات الاحتيال.

2- احتيال التثليث بوجود محتال ومتسوق شرعي وأعمال التجارة الإلكترونية، يقوم المحتال بإنشاء متجر على الإنترنت ويوفر عناصر رائعة بأقل التكاليف، يقوم بشراء الأشياء من شركة مشروعة ويرسلها إلى العملاء بعد الحصول على معلومات بطاقة الائتمان من أولئك الذين اشتروا.

3- الاحتيال في الاعتراض عندما يقدم المحتالون طلبًا يتضمن عناوين إرسال الفواتير والشحن المطابقة لعنوان البطاقة سيحاول المحتال بعد ذلك سرقة عنوان البطاقة سيحاول المحتال بعد ذلك اختطاف الطرد من خلال مطالبة ممثل خدمة العملاء بإجراء تعديلات على عنوان التسليم؛ طلب تغيير عنوان الطلب إلى موقع يمكن من خلاله اعتراض المادة المسروقة.

4-الاحتيال في اختبار صلاحية البطاقة عندما يقوم المحتال بتقييم بيانات البطاقة المختلفة لتحديد ما إذا كانت بيانات الاعتماد مشروعة أم لا ثم يستخدمها لإجراء معاملات غير مشروعة على موقع ويب آخر.

5- احتيال رد المبالغ المدفوعة عندما يشتري العميل سلعًا عبر الإنترنت، ثم يطلب رد المبالغ المدفوعة مدعيًا أن بطاقة الائتمان الخاصة به قد سُرقت، من المرجح أن يحدث هذا بعد تسليم العناصر، يعد هذا النوع من الاحتيال أكثر شيوعًا بين المستهلكين منه بين المحتالين المحترفين، ويصعب اكتشافه.

6-الاستيلاء على الحساب

تحدث هذه الحالة من الاحتيال عندما يسرق المحتالون تفاصيل حامل البطاقة الشرعي، ويحصل المحتال على السيطرة على حساب صالح من خلال تقديم أرقام حساب العميل أو أرقام بطاقة الائتمان ثم يتصل المحتالون ببنك حامل البطاقة، متظاهرين بأنهم حامل البطاقة الحقيقي، لطلب إعادة توجيه البريد إلى عنوان جديد ويبلغ المحتال عن فقدان البطاقة ويطلب إرسال بطاقة بديلة.

ويرى الباحث ان هنالك طرقاً أخرى غير التي ذكرت يمكن أن تضاف إلى طرق الاحتيال وهي :

أ-عن طريق التاجر يحدث هذا النوع من الاحتيال عندما يتآمر التجار أو موظفوهم لارتكاب عمليات احتيال باستعمال حسابات أصحاب البطاقات أو المعلومات الفردية، وتقديم تفاصيل حامل البطاقة إلى المحتالين.

ب-عن طريق الوسيط : المتمثل بموظفي شركات الدفع الالكتروني الاخرى كونهم على دراية تامة بمعلومات الزبائن فبعض الشركات تقوم بتسريح موظفيها نتيجة طلب اجور أعلى وبذلك تضطر إلى تسريحهم متناسيةً ان هؤلاء الموظفين على اطلاع تام بمعلومات الزبائن والتي بالإمكان استعمالها او بيعها .

جـ عن طريق موظف الخدمة وهو الموظف الذي يقوم برفع المبالغ على بطاقات الماستر كارد من قبل الشركات أو الدوائر الحكومية لحاملي بطاقات الدفع الالكتروني فهو ايضاً على دراية تامة بمعلومات الزبون .

3-3-أسباب الاحتيال المالي

لا بد لجريمة الاحتيال المالي من أن تتوافر فيها مجموعة من العناصر المشتركة التي توجد على المستويات كافة التي يطلق عليها مثلث الاحتيال، وهي كالآتي: (السهلي 2023، 10):

1. **الضغوط/الحوافز:** إدارة المنشأة أو الموظفون على استعداد لارتكاب عمليات احتيال أو التلاعب بالبيانات المالية بسبب حاجتهم إلى المال، قد يكون المحتال غارقاً في الديون أو يريد تحسين أسلوب حياته أو إنفاقه على ملذاته.

2. الفرص: ضعف نظام الرقابة الداخلية مع ضعف الرقابة من لدن الإدارة والآخرين يخلق الفرصة لارتكاب عمليات الاحتيال، حيث يجب أن يكون لدى المحتال أو الموظف القدرة على إدارة إجراءات الرقابة والاستفادة من المسؤوليات والصلاحيات التي تتيح لك فرصة لارتكاب عمليات احتيال.

3. المبررات/الاتجاهات: تشير إلى اتجاهات الأفراد نحو تبرير أو إقناع أنفسهم بالموافقة على ارتكاب عمليات احتيال أو التلاعب بالبيانات المالية .

ويرى الباحث أن أحد اسباب الاحتيال الالكتروني هو الجهل بالتكنلوجيا الحديثة ومعرفة كيفية استعمالها؛ إذ يجب أن يكون هنالك حملات تثقيفية في كيفية استعمال التقنيات وطرق الاحتيال وكيفية تجنبها ووضع قوانين صارمة للحد من تلك العمليات.

المحور الرابع

الدفع الإلكتروني

4-1- الدفع الالكتروني مفهومه وتعريفه

الدفع الالكتروني هو أحد ابتكارات الدفع التي أنشأها الذكاء الاصطناعي في مجال التكنولوجيا تبدء عملية الدفع الرقمي بتخزين الأموال ومعالجتها واستلامها، مما يؤدي إلى توليد معلومات رقمية ويتم التحويل إلكترونيًا، لذلك لم يعد المشترون مضطرين إلى الدفع نقدًا. وباستعمال المدفوعات الرقمية، يمكن للنظام أن يجعل المعاملات أسهل وأكثر آلية، هناك عدة طرق لإجراء الدفعات الرقمية؛ على سبيل المثال من خلال التطبيقات المتاحة وبطاقات الدفع والأموال الإلكترونية، و بيَن (مهدي) إن الدفع الإلكتروني هي عملية تحويل سعر السلعة أو الخدمة إلكترونياً باستعمال إحدى طرق الدفع الإلكتروني، إذ يتم استعمالهُ كأداة وفاء بديلة لطرق الدفع التقليدية مثل النقود والشيكات، وذلك عن طريق دفع وتسوية الالتزامات المالية من شخص إلى آخر الكترونياً ، ومن جانبه عَرَفَ المشرع العراقي نظام الدفع الإلكتروني بأنه " مجموعة الوسائل والإجراءات والقواعد الخاصة بعملية تحويل الأموال بين المشاركين ضمن النظام، على أن تتم عملية تحويل الأموال من خلال استعمال البنية التحتية لنظام الدفع (مهدي 2024، 3) كما عرف ايضاً بأنه عبارة عن دفع لمعاملة إلكترونياً دون استعمال النقد ، عبر استعمال المشترون والبائعون نظامًا إلكترونيًا للمعاملات، يمكن أيضًا تفسير الدفع على أنه تحويل مبلغ من المال من المشتري إلى المستلم (Sardjonor, et al. 2021).

4-2-طرق الدفع الالكتروني

بعد الانتقال العالمي في العمليات المالية عبر استعمال تقنيات الدفع الالكتروني واكب البنك المركزي العراقي ذلك التطور ففي عام 2004 بدء البنك بتهيئة الارضية المناسبة لعمليات الدفع الالكتروني وفي عام 2006 بدء الاستعمال الفعلي لتلك التقنيات مما انعكس ذلك إيجاباً على العمليات المالية في السوق العراقية كما وحدد البنك المركزي طرق الدفع الالكتروني والتي منها (الدفع الإلكتروني POS، البطاقات الإلكترونية، المحافظ الإلكترونية، الخدمات المصرفية عبر تطبيق الهاتف النقال).

1-الدفع الإلكتروني POS: مجموعة من الأجهزة والبرامج المتصلة والتي تعمل معًا لتمكين إعداد الفواتير السريعة لبيانات المخزون، غالبًا ما تحتوي البرامج الموجودة في أنظمة نقاط البيع على أزرار أو اختصارات وصول سريعة تمكن من تسريع العمليات، وتعدُّ المكون الأساسي للأنشطة التجارية ويتم من خلالها الدفع مقابل شراء أي منتج في كافة المحلات التجارية باستعمال البطاقات الإلكترونية بكافة أنواعها، وهو متوفر في الدوائر الحكومية ومراكز التسوق والمتاجر والمطاعم والصيدليات ومحطات الوقود.

2- البطاقات الإلكترونية:

أ. بطاقات الائتمان (Credit Card) هي بطاقات تصدر من المصارف للزبائن وتستعمل داخل البلد وخارجه لتمكين الزبائن من إجراء عملياتهم المالية وتوفر بطاقات الائتمان سهولة إجراء المعاملات غير النقدية وتسمح أيضًا بإجراء عمليات شراء عبر الهاتف، وبشكل متزايد عبر الإنترنت، كما توفر بطاقات الائتمان للمستهلكين مرونة تأجيل الدفع إلى تاريخ مستقبلي، وبالتالي يمكن أن تسمح للمستهلكين بتيسير الإنفاق على النقص المؤقت في السيولة، ومع ذلك فإن استعمال خيار الائتمان المتجدد لبطاقة الائتمان يؤدي عادة إلى دفع معدلات فائدة عالية ليس فقط على الرصيد الحالي ولكن أيضًا على أي رسوم جديدة يتم فرضها على البطاقة أيضًا، وبالتالي يعد شكلاً من أشكال الائتمان مكلفًا إلى حد ما، خاصة إذا كان الخيار الائتماني المتجدد يتم استعمال ميزة الائتمان بشكل متكرر (Bertaut and Haliassos 2006, 2)

ب. بطاقات الخصم (Debit Card) بطاقة الخصم هي بطاقة دفع بلاستيكية تسمح لعميل البنك بإجراء الدفعات وإجراء المعاملات أثناء تحصيل الرسوم مباشرة من حسابه المصرفي وتمكن الزبون من إجراء عملياتهُ المالية ؛ سحب نقدي من أجهزة الصراف الالي ATM ، دفع قيمة المشتريات عند الشراء من خلال نقاط البيع pos ، والتسوق عبر الانترنت، ويختلف هذا النوع من الخدمة عن بطاقة الائتمان، لذا فقد اعتمدت العديد من البلدان هذه التكنولوجيا التي أصبحت تحل محل استعمال الشيكات والحوالات المصرفية، تتميز الخدمات المقدمة عن طريق بطاقة الخصم بالمرونة حيث تم تصميمها لتناسب خصوصيات كل دولة على عكس بطاقات الائتمان، مما أدى إلى زيادة عدد شركات الخدمات التي تتعامل مع بطاقة الخصم وأصبحت بطاقاتها غير متوافقة مع بطاقات أخرى حول العالم، وقد بدأت بعض التغييرات ظهرت منذ منتصف العقد الأول من القرن الحادي والعشرين حيث يمكن لبطاقات البلدان المختلفة إجراء عمليات شراء عبر الإنترنت وتحويل الأموال إلكترونيًا (Igboanusi 2024, 3).

ج. بطاقات الدفع المسبق (Prepaid Card) توفر بطاقات الدفع المسبق للمستهلكين ومقدمي الخدمات والبنوك المصدرة في زيادة اعتماد تطبيقات الدفع فباستعمال هذه البطاقات يمكن للمستهلكين دفع الفواتير وإجراء عمليات الشراء والحصول على النقد من أجهزة الصراف الآلي، إذ يكون الرصيد المتوفر في البطاقة عند استلامها (صفر) ويجب ان يتم ايداع مبلغ محدد في حساب البطاقة وعند كل عملية تتم باستعمال البطاقة يتم الخصم من الرصيد المتوفر فيها وتكون على أنواع متعددة ؛ فبعضها يمكن ان تتم تعبئتها لمرة واحدة فقط وتستعمل لأغراض التسوق عبر الانترنت او الالعاب والبعض الاخر يمكن اعادة تعبئتها ويمكن استعمالها عن طريق أجهزة الصراف الالي ATM ونقاط البيع POS وكذلك للتسوق الالكتروني داخل وخارج البلاد.

3- المحافظ الإلكترونية

هي إحدى وسائل الدفع الإلكتروني والتي تتم عبر الهاتف النقال ويتم تسجيلها لدى مزود الخدمة المرخص من قبل البنك المركزي بالاعتماد على المبادئ معرفة الزبون ورقم هاتفهُ الشخصي لتمكينه من تنفيذ حركات العمليات المالية ، **ومن اهم مميزاتها :-**

أ- يمكن تحويل المبالغ مباشرة من محفظة إلى محفظة اخرى

ب- دفع قيمة المشتريات مباشرةً

جـ- السحب النقدي

د- تسديد كل أنواع الفواتير

هـ- شحن أرصدة الهواتف النقالة

و- شراء بطاقات خدمات ترفيهية من العاب وتطبيقات

4-الخدمات المصرفية عبر تطبيق الهاتف النقال

تتضمن الخدمات المصرفية عبر تطبيق الهاتف النقال الخدمات المصرفية المسموح بها قانونا مثل تمكين خدمة تحويل الأموال الكترونياً بين المصارف عن طريق الهاتف النقال وطلب كشف للعمليات المصرفية والحركات التي يقوم بها الزبون، وكذلك عمليات تحويل الاموال بين حسابات الزبائن، والاطلاع على الخدمات المقدمة والقروض والمنتجات وكذلك الاسعار والعروض المصرفية، بالإضافة إلى الاستعلام عن مواقع أجهزة الصراف الالي ، و التواصل مع خدمة الزبائن بطريقة سهلة وفعالة.

المحور الخامس

الحد من الاحتيال المالي عبر الذكاء الاصطناعي.

5-1- دور الذكاء الاصطناعي في كشف الاحتيال

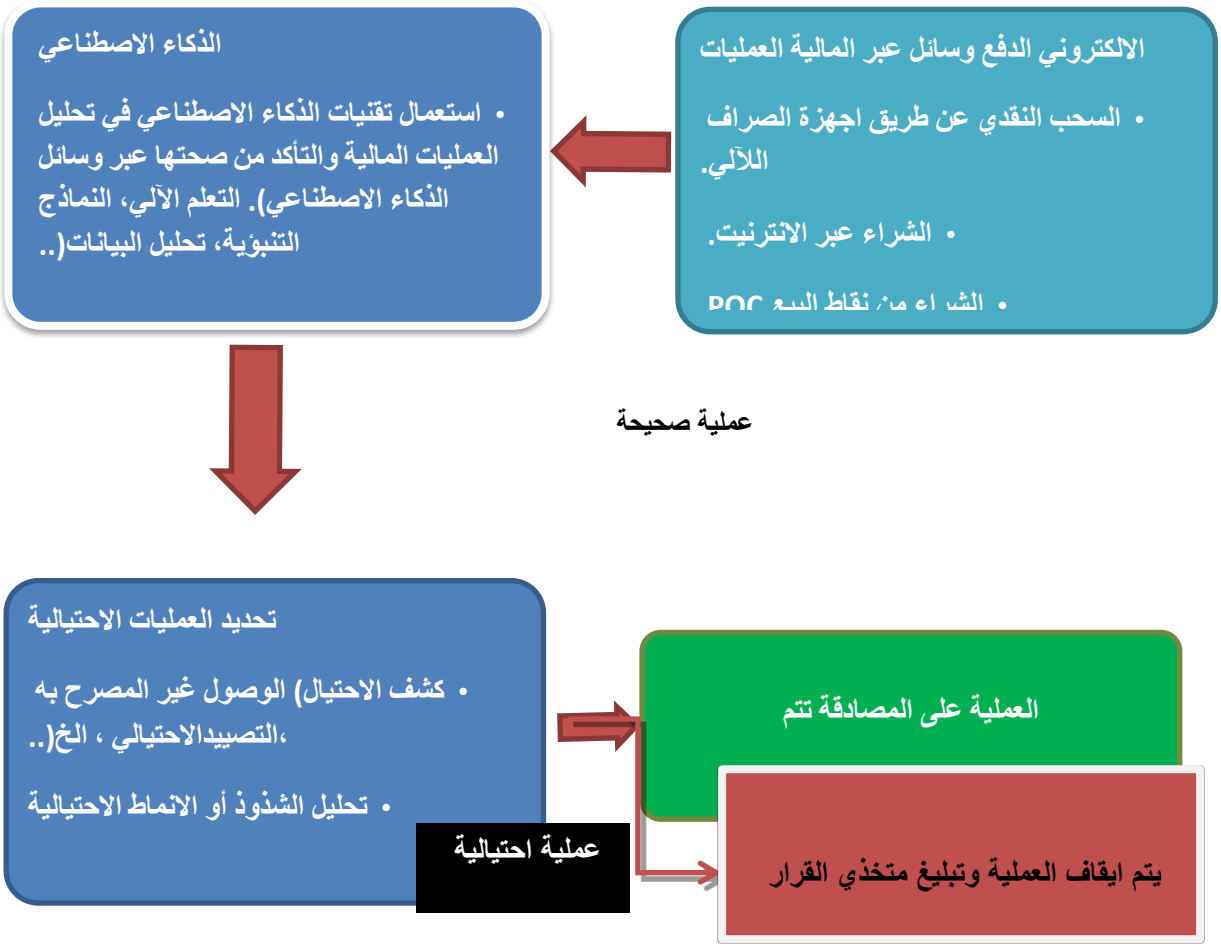
تطلب ظهور الاحتيال المالي في العصر الرقمي الحديث نقلة نوعية في استراتيجيات الكشف عن الاحتيال، لكون الأساليب التقليدية أصبحت غير كافية على نحو متزايد في سياق مخططات الاحتيال المعقدة والسريعة في التغير، واستجابة لذلك وجهت صناعة التكنولوجيا المالية اهتمامها إلى التقنيات المتقدمة، وخاصة الذكاء الاصطناعي (AI) والتعلم الآلي (ML)، بهدف صياغة حدود جديدة في الكشف عن الاحتيال، أحدثت هذه التقنيات ثورة في قدرات الكشف عن الاحتيال، إذ يمكن لها من توفير القدرة على تحليل كميات كبيرة من بيانات المعاملات في الوقت الفعلي، وكذلك تحديد الأنماط المعقدة التي تشير إلى أي نشاط احتيالي ممكن، والتنبؤ بمحاولات الاحتيال ومنعها قبل وقوعها وتسببها بضرر ما (Shoetan and Familo 2024, 3). ويبدأ تطبيق تقنية الذكاء الاصطناعي في الكشف عن الاحتيال المالي بتحليل الاحتياجات المختلفة، ويشمل ذلك فهم تعقيد الأسواق المالية وطرق الاحتيال المتغيرة باستمرار، فضلاً عن الوعي بانخفاض كفاءة طرق الكشف عن الاحتيال التقليدية، ويعد كشف السلوك الاحتيالي والوقاية منه في الوقت المناسب أمراً بالغ الأهمية بالنسبة للمؤسسات المالية والمستخدمين، إذ يسهم في الحفاظ على استقرار السوق المالية وحقوق ومصالح المستخدمين، وفي هذه الحالة أصبح تطبيق تقنية الذكاء الاصطناعي خيارًا لا غنى عنه (Wang 2024, 2). تقوم أنظمة وتقنيات الذكاء الاصطناعي بفحص البيانات

للتعرف عليها وتحديد الأنماط والمعاملات الاحتيالية، مما يوفر أداةً قيمة لصناع ومتخذي القرارات في مكافحة الاحتيال وكذلك لتحديد الخروقات، كما يتطلب التعلم التكيفي بأن تكون تقنيات الكشف عن الاحتيال ديناميكية وليست ثابتة أي تتغير وسائلها في الكشف عن الاحتيال مع التجديد في طرق الاحتيال كون المحتالون في العادة يبتكرون طرقاً جديدة في الاحتيال كلما عرفت طرقهم السائدة وبذلك يتكيف الذكاء الاصطناعي مع الأنماط الجديدة للنشاط الاحتيالي، ويتعلم باستمرار من كل معاملة، ويتطلب تحليل سلوك المستخدم أن يستخدم الذكاء الاصطناعي نموذج التعلم العميق لدراسة أنماط سلوك المستخدم واكتشاف أي سلوك يمكن ان يكون غير عادياً أو غير متسقاً، وهذا مفيدًا بشكل خاص على الأنظمة الأساسية عبر الإنترنت، حيث يمكن أن يكون السلوك غير الطبيعي مؤشراً بعلامة حمراء فورية (Ezeji 2024, 69).

5-2-آليات الذكاء الاصطناعي للحد من الاحتيال في عمليات الدفع الالكتروني

يُحدِثْ دمج الذكاء الاصطناعي في التدابير الأمنية التقنية التقليدية ثورة في أنظمة كشف الاحتيال ومنعهُ، حيث أصبحت الخوارزميات قادرة على معالجة كميات كبيرة من المعلومات بسرعة ودقة للعثور على المعاملات المشبوهة وأنماط النشاط الاحتيالي، إذ يمكن أن يساعد الذكاء الاصطناعي المطبق على التحليل التلقائي، واكتشاف التطفل من خلال تحديد وصول المستخدم تلقائيًا واكتشاف البريد العشوائي، واكتشاف الروبوتات، والبرامج الضارة على الأجهزة المحمولة، وتطوير برامج مكافحة الفيروسات المتقدمة ، والتنبؤ بالانتهاكات الأمنية، والمصادقة وحماية كلمة المرور، واكتشاف التصيد الاحتيالي، ومراقبة حركة مرور الشبكة لتحديد الحالات الشاذة، ومع ذلك، هناك أيضًا القيود المستندة إلى نقص أو عدم كفاية مجموعات البيانات المتعلقة بالمخططات المبتكرة لمجرمي الإنترنت، فضلاً عن استعمال تكنولوجيا الذكاء الاصطناعي في عملية منع الاحتيال عبر الإنترنت، حول الشروط التشريعية المتعلقة بمعالجة البيانات الشخصية، وغالبًا ما يتم استعمال الذكاء الاصطناعي والتعلم التلقائي، من أجل تحسين قدرات اكتشاف الاحتيال بشكل كبير، إذ توفر آليات الاحتيال لجميع المعاملات المصرفية والبطاقات عبر الإنترنت ميزة يمكن أن تساعد في اكتشاف الاحتيال، مثل موقع بدء الدفع، أو تواريخ الدفع أو سلوك صاحب الحساب أثناء معاملات الدفع أو الخصائص المختلفة للمدفوعات كالمدفوعات الكبيرة بشكل غير عادي، أو التحويلات إلى ولايات أخرى، أو البيانات التاريخية ذات الصلة حول المعاملات الإلكترونية من الأنظمة والمنصات المشاركة في عملية الدفع أو المعاملة وبالتالي يمكن للخوارزميات التعرف على الماضي ومعرفة السلوك الاحتيالي أو اكتشاف أنواع جديدة من الاحتيال، تعد كمية البيانات ودقتها أمرًا بالغ الأهمية لفعالية أدوات متخذي القرار والتي تمنع الاحتيال عبر الإنترنت، كما تعد النمذجة التنبؤية واحدة من أقوى تطبيقات الذكاء الاصطناعي والتعلم الآلي الميزة الأكبر هي أنه يحدد الاحتيال قبل حدوثه كما في الشكل (**2**) يبين كيفية منع الاحتيال بواسطة الذكاء الاصطناعي (NIȚĂ, et al. 2023, 99). ويرى الباحث ضرورة اضافة ميزات جديدة لعمليات الدفع الالكتروني بكافة صورها كإضافة كامرة للأجهزة المرتبطة بعمليات الدفع او اضافة التوقيع الالكتروني أو البصمة للإتمام العمليات المالية بشكلٍ آمن وتقليل فرص الاحتيال مما يوفر أمان اكثر لمستخدمي الدفع الالكتروني .

شكل (5) مخطط عمل تقنيات الذكاء الاصطناعي للحد من الاحتيال في عمليات الدفع الالكتروني



الشكل من اعداد الباحث بالاعتماد على المصادر

المحور السادس

الجانب العملي

6-1-وصف مجتمع البحث وقائمة الفحص والمحاور الرئيسة المستخدمة

في هذا المبحث، وصفٌ لمجتمع البحث المتمثل في الشركة العالمية للبطاقة الذكية المحدودة المختلطة :-

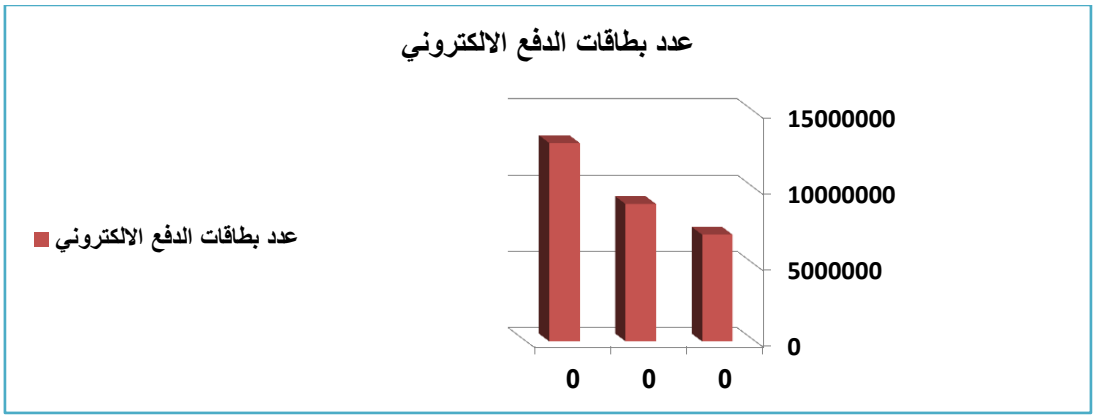
حيث تأسست الشركة العالمية للبطاقة الذكية في عام 2007م بالشراكة بين القطاع العام والقطاع الخاص، إذ عملت الادارة على طرح مشروع بطاقة "كي كارد" البايومترية على مصرفي الرافدين والرشيد بهدف وضع حلول للتحديات التي كانت تواجه موظفي الدولة والمتقاعدين وغيرهم من الفئات الأخرى، إذ أدخلت الشركة تقنيات الدفع الالكتروني للعراق ووفرت أكثر من 10 آلاف نقطة من نقاط استلام الرواتب بعد ما كانت في السابق محصورة بالمصارف والتي تقدر بحوالي 250 فرعاً لمصرفي الرشيد والرافدين والتي لم تكن كافية لتغطية الاعداد الكبيرة من الموظفين والمستفيدين، وكان لتقنيات تقاطع البصمات البايومتري في بطاقات "كي كارد" الدور الفعال في كشف الفساد وتحديد آلاف حالات التزوير وكذلك سرقة الهوية ومنعت حالات تعدد الرواتب لنفس الشخص وتطورت في اعتماد المؤشرات الحيوية المتعددة كبصمات الأصابع وبصمات العين و بصمة الوجه لمعرفة الزبائن، لم تتوقف الشركة من التطور فهي تعمل على إطلاق جيل من الخدمات الجديدة بين الحين والآخر ، إضافة إلى توفير حلول القيمة المضافة للزبائن من أفراد أومؤسسات وهذا واضح جداً من مؤشرات النمو الموضحة في جدول رقم (3)

جدول (3) مؤشرات نمو الدفع الإلكتروني لمصرف الرافدين في العراق

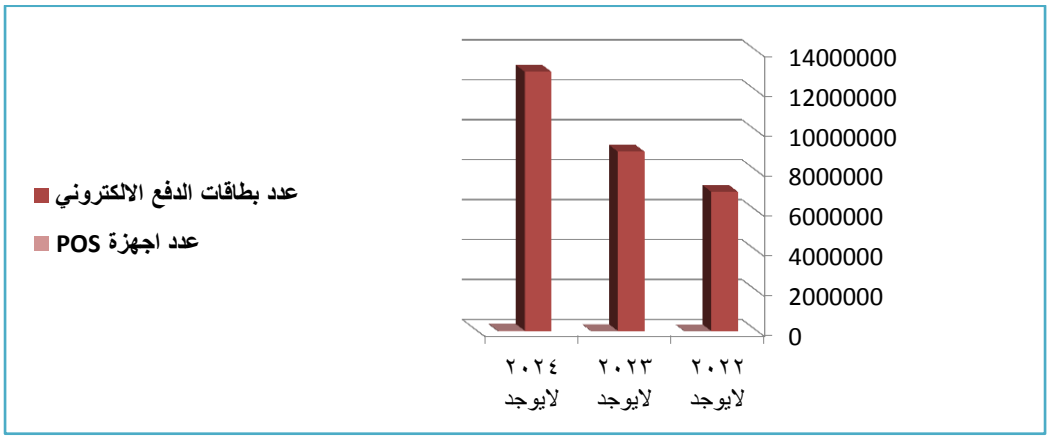
السنة	اجهزة ATM	بطاقات الدفع الالكتروني	اجهزة POS	المحافظ الالكترونية	دفع الكتروني بواسطة الموبايل
2022	لا يوجد	7000000	21000	لا توجد	4000000
2023	لا يوجد	9000000	23000	لا توجد	12000000
2024	لا يوجد	13000000	35000	لا توجد	25000000

المصدر : الشركة العالمية للبطاقة الذكية المحدودة المختلطة

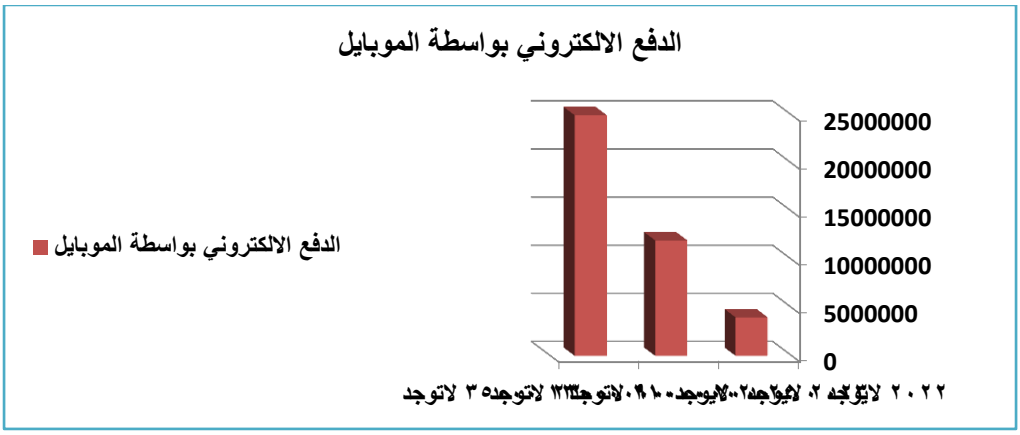
شكل (2) مؤشر بطاقات الدفع الإلكتروني لمصرف الرافدين في العراق



شكل (3) مؤشر أجهزة P OS لمصرف الرافدين في العراق



شكل (4) مؤشر الدفع الالكتروني بواسطة الموبايل لمصرف الرافدين في العراق



2-6-تطوير قائمة الفحص:

طور الباحث قائمة الفحص (Checklist) معتمداً على محوريين رئيسين:

1. الأول، **استعمال الذكاء الاصطناعي في عمليات الدفع الالكتروني**
2. المحور الآخر: الحد من الاحتيال المالي بواسطة الذكاء الاصطناعي

وتم اختبار صدق (Checklist) بعد عرضها على المحكمين من اساتذة الجامعات العراقية والأخذ بالملاحظات والتوصيات التي وجهت حول التعديلات اللازمة بالاستمارة، وقد ملئت قائمة الفحص من قبل الباحث بعد اجراء عدد من الزيارات إلى مجتمع البحث المتمثل بالشركة العالمية للبطاقة الذكية والاقسام ذات العلاقة بموضوع البحث والاستفسار عن بعض المعلومات والبيانات والجداول والتقارير ذات العلاقة ، بالإضافة إلى الملاحظات التي شوهدت من لدن الباحث خلال هذه الزيارات لبعض مراكز الشركة.

جدول (4) المصادر المعتمدة في بناء قائمة الفحص

ت	محاور قائمة الفحص	عدد الفقرات	المصادر
1	استعمال الذكاء الاصطناعي في عمليات الدفع الالكتروني	8	بالاعتماد على الأدبيات المحاسبية
2	المحور الثاني الحد من الاحتيال المالي بواسطة الذكاء الاصطناعي	8	

المصدر: من اعداد الباحث

بالاعتماد على الوسط الحسابي المرجح والنسبة المئوية لمدى المطابقة للوصول إلى مقدار الفجوة في ممارسات تطبيق وسائل الامان ، حيث اعتمد الباحث على مقياس (Likert) السباعي بهدف الحصول على مرونة ودقة عالية في المعلومات التي سيتم الحصول عليها.

3-6-عرض وتحليل وتفسير البيانات على ضوء نتائج قائمة الفحص:

يعرض هذا المبحث نتائج إجابات أسئلة قائمة الفحص، وتحليل بياناتها للوصول إلى نتائج البحث بالاعتماد على (الوصفي التحليلي) وهو أحد الاساليب الاحصائية المعتمدة باستخراج التكرار والوسط الحسابي والنسب المئوية لبيان مدى مطابقة المتغيرات الفرعية ولتحديد حجم الفجوة مع ما مطبق في الشركة العالمية للبطاقة الذكية عينة البحث ومن خلال الإجابات على قائمة الفحص ذات المقياس السباعي (غير مطبق وغير موثق، مطبق جزئيا غير موثق، مطبق جزئيا موثق جزئيا، مطبق جزئيا موثق كليا، مطبق كليا غير موثق، مطبق كليا موثق جزئيا، مطبق كليا موثق كليا) والأوزان المقابلة لها 0,1,2,3,4,5,6 على التوالي، وفيما يلي تحليل نتائج قائمة الفحص :

الجدول (5) قائمة الفحص (استعمال الذكاء الاصطناعي في عمليات الدفع الالكتروني)

الفرضية الأولى : هناك دور ايجابي لتقنيات الذكاء الاصطناعي في عمليات الدفع الالكتروني

ت	أولا: **استعمال الذكاء الاصطناعي في عمليات الدفع الالكتروني**	مطبق كلياً وموثق كلياً	مطبق كلياً وموثق جزئياً	مطبق كلياً و غير موثق	مطبق جزئياً وموثق كلياً	مطبق جزئياً وموثق جزئياً	مطبق جزئياً غير موثق	غير مطبق و غير موثق
1	تعمل الشركة على دمج الذكاء الاصطناعي في عمليات الدفع الالكتروني بهدف تحسين العمليات المالية وزيادة أمانها.	✓						
2	تستعمل الشركة ادوات الذكاء الاصطناعي لمراقبة عمليات الدفع الالكتروني واكتشاف الانماط غير الاعتيادية (الشاذة) .	✓						
3	لدى الشركة فريق تقني مختص للاستجابة السريعة حول اي عملية احتيالية واردة عبر نظام الدفع الالكتروني .	✓						

4	تستعمل الشركة خوارزميات التعلم الآلي لتحديد سلوك مستخدمي وسائل الدفع الالكتروني.		✓					
5	تقوم الشركة بدراسة التحديات والمشاكل التي تواجه عمليات الدفع الالكتروني بصورة دورية بهدف تطوير وسائل أمان ذات كفاءة عالية.	✓						
6	تستعمل الشركة وسائل أمان وفق معايير اخلاقية ووصول محدد لحماية خصوصية بيانات الزبائن.	✓						
7	تقوم الشركة وبشكل دوري بتعريف الزبائن بماهية الدفع الالكتروني وطرق الاحتيال الشائعة والوقاية منها.		✓					
8	تحرص الشركة على تعيين موظفين اكفاء في قسم الدفع الالكتروني ومنح مكافئات مالية لهم مع الحرص على عدم تسريحهم .	✓						
	الوزن	**6**	**5**	**4**	**3**	**2**	**1**	**0**
	التكرارات	**6**	**2**	**0**	**0**	**0**	**0**	**0**
	التكرارات) xالنتيجة(الوزن	**36**	**10**	**0**	**0**	**0**	**0**	**0**
	الوسط الحسابي المرجح **(مج النتيجة / عدد الاسئلة)**	**5.75**						
	النسبة المئوية لمدى المطابقة **(الوسط الحسابي / 6)X %**	**%.95**						
	حجم الفجوة(100 – النسبة المئوية)	**99.05**						

الجدول (6) قائمة الفحص (الحد من الاحتيال المالي بواسطة الذكاء الاصطناعي)

الفرضية الثانية: تؤثر تقنيات الذكاء الاصطناعي في الحد من الاحتيال المالي في عمليات الدفع الالكتروني.

ت	ثانياً: الحد من الاحتيال المالي بواسطة الذكاء الاصطناعي	مطبق كلياً وموثق كلياً	مطبق كلياً وموثق جزئياً	مطبق كلياً و غير موثق	مطبق جزئياً وموثق كلياً	مطبق جزئياً وموثق جزئياً	مطبق جزئياً غير موثق	غير مطبق وغير موثق
1	تستعمل الشركة خوارزميات التعلم الآلي المتمثل في الشبكات العصبية وشجرة القرار في تحليل الانماط غير الاعتيادية .		✓					
2	تقنية التعلم العميق هي احدى التقنيات المستعملة من قبل الشركة في التعرف على الصور والنصوص وكشف الاحتيال قبل وقوعه.	✓						
3	تستعمل الشركة تقنيات حديثة من شأنها فحص وتحليل البيانات الضخمة واكتشاف التحايل ان وجد.	✓						
4	لدى الشركة برامج خاصة يمكنها ربط المعاملات بالزبون وتأكيد الاعمال المتكررة (المعتادة) من الاعمال الشاذة في عمليات الدفع الالكتروني.	✓						
5	لدى الشركة كادر وظيفي متخصص اكاديمياً ومهنياً يشرف على اعداد الخوارزميات الخاصة بعمليات الدفع الالكتروني فيما يخص الجانب الحسابي والتدقيقي.	✓						
6	تمتلك الشركة تقنيات الانذار المبكر في حال حدوث اي عملية شاذة تنذر باحتيال مالي في عمليات الدفع الالكتروني .	✓						
7	تستعمل الشركة خاصية التعرف على الوجه في تأكيد	✓						

	عمليات الدفع الالكتروني.							
8	تستعمل الشركة في عمليات الدفع الالكتروني خاصية التعرف على الانماط كالتوقيع الالكتروني او البصمة الالكترونية في عمليات تأكيد الدفع من قبل الزبائن.	✓						
	الوزن	**6**	**5**	**4**	**3**	**2**	**1**	**0**
	التكرارات	**7**	**1**	**0**	**0**	**0**	**0**	**0**
	النتيجة(الوزن x التكرارات)	**42**	**5**	**0**	**0**	**0**	**0**	**0**
	الوسط الحسابي المرجح (مج النتيجة / عدد الاسئلة)	**5.875**						
	النسبة المئوية لمدى المطابقة (الوسط الحسابي / 6)X %	**%.97**						
	حجم الفجوة(100 – النسبة المئوية)	**99.03**						

4-6-تحليل النتائج

اولاً : تحليل المتغير الثابت استعمال الذكاء الاصطناعي في عمليات الدفع الالكتروني وفقاً لنتائج مقياس ليكرت السباعي:

1. مطبق كلياً وموثق كلياً : حصل هذا المقياس على ستة تكرارات بنتيجة 36 درجة مما يدل على أن هناك تقارب كبير مع مفردات المتغير الثابت
2. مطبق كلياً وموثق جزئياً **:** حصل هذا المقياس على تكراران بنتيجة 10 درجة مما يدل على أن هناك تقارب جيد مع مفردات المتغير الثابت.
3. مطبق كلياً وغير موثق **:** صفر و النتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة.
4. مطبق جزئياً وموثق كلياً **:** صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة.

5. مطبق جزئياً وموثق جزئياً **:** صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة

6. مطبق جزئياً غير موثق **:** صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة

7. غير مطبق وغير موثق **:** صفر وهنا النتيجة تكون مؤيدة لما ورد في المتغيرات السابقة

وهنا حصل هذا المتغير المستقل على وسط حسابي مرجح بنسبة (5.75)وبنسبة مئوية وصلت إلى 95.% مما جعل حجم الفجوة يصل إلى 99.05%

ثانيا : تحليل المتغير التابع الحد من الاحتيال المالي بواسطة الذكاء الاصطناعي وفقاً لنتائج مقياس ليكرت السباعي:

1. مطبق كلياً وموثق كلياً : حصل هذا المقياس على سبعة تكرارات بنتيجة 42 درجة مما يدل على ان هناك تقارب كبير مع مفردات المتغير التابع
2. مطبق كلياً وموثق جزئياً : حصل هذا المقياس على تكرار واحد بنتيجة 5 درجة مما يدل على ان هناك تقارب جيد مع مفردات المتغير الثابت.
3. مطبق كلياً وغير موثق : صفر و النتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة.
4. مطبق جزئياً وموثق كلياً : صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة.
5. مطبق جزئياً وموثق جزئياً : صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة
6. مطبق جزئياً غير موثق : صفر والنتيجة هنا تكون مؤيدة لما ورد في المتغيرات السابقة
7. غير مطبق وغير موثق : صفر وهنا النتيجة تكون مؤيدة لما ورد في المتغيرات السابقة

وهنا حصل هذا المتغير التابع على وسط حسابي مرجح بنسبة **5.875**% وبنسبة مئوية وصلت إلى 97.% مما جعل حجم الفجوة يصل إلى 99.03

نستنتج من ذلك قبول فرضية العدم H0: توجد علاقة ذات دلالة إحصائية بين تقنيات الذكاء الاصطناعي وتقليل نسبة الاحتيال المالي في عمليات الدفع الالكتروني.

المحور السادس

سادساً: الاستنتاجات والتوصيات

6-1-الاستنتاجات

توصل الباحث إلى عدة نقاط هامة وهي كالتالي:

1-يمكن لتقنيات الذكاء الاصطناعي أن تعزز من امكانيات الحماية والحد من عمليات الاحتيال المالي في عمليات الدفع الالكتروني إذا تمت برمجة خوارزمياته بصورة تواكب الادوات الاحتيالية الحديثة المستخدمة من قبل المحتالين .

2-في العادة تكون عمليات الدفع الالكتروني رتيبة في حركاتها فإن أي تغير شاذ في نمط تلك الحركات في الغالب يكون احتيالي يوجب ايقاف العملية المالية.

3- آليات وأدوات التدقيق المعتمدة من قبل الدوائر المستفيدة لا تواكب التطور الحاصل في العمليات المالية وهذا قد يكون احد أهم اسباب تفشي ظاهرة الاحتيال المالي .

4-ضعف الجانب التوعوي حول عمليات الدفع الالكتروني فيما يخص طرق الاستعمال ووسائل الأمان والمخاطر الملازمة لعمليات الدفع الالكتروني جعل الزبائن هدفاً سهلاً للمحتالين .

5- غالباً ما يتم السحب من بطاقات الدفع الالكتروني من دون الحاجة إلى الباسور ولمبلغ معين في عمليات الشراء عن طريق نقاط POS مما يسهل هذا الامر عملية الاحتيال خصوصاً عند فقدان البطاقة.

6-2-التوصيات

1-ضرورة استعمال تقنيات الذكاء الاصطناعي تماشياً مع التطور الحاصل في عمليات الدفع الالكتروني إضافة إلى تدريب المدققين على آلياته والمشاركة في اعداد بياناته الخاضعة للأشراف.

2-ضرورة مراقبة الحالات الشاذة وغير المعتادة في عمليات الدفع الالكتروني بوساطة مقارنة الحالات المالية السابقة عبر موائمة عمليات السحب المتكرر غير النمطي أو التحويل الدولي أو المشتريات الكبيرة المفاجئة وغيرها من عمليات الاحتيال .

3-تعزيز آليات وأدوات التدقيق بما يتلاءم مع العمليات المالية الحديثة وأنظمة الدفع الإلكتروني فحداثة التطبيقات يجب ان يقابلها حداثة في عمليات التدقيق مما يؤدي إلى تضيق فرص الاحتيال المالي بتلك الوسائل.

4- ضرورة إقامة حملات توعوية توضح آلية عمل وسائل الدفع الإلكتروني وطرق الاحتيال المعتادة وكيفية الوقاية منها والتعريف بالمواد القانونية التي تطال المحتالين جراء عملية الاحتيال المالي.

5- ضرورة إضافة بعض الميزات للوسائل الدفع الالكتروني لزيادة الامان وتقليل فرص الاحتيال كإضافة المصادقة عبر الكامرة والتوقيع الإلكتروني أو البصمة الالكترونية وغيرها من الميزات عالية الامان.

المراجع

1. Adeoye, Oluwasegun Isaiah, Rufus Ishola Akintoye, Theophilus Anaekenwa Aguguom, and Olubusola Ayoola Olagunju. "Artificial intelligence and audit quality: Implications for practicing accountants." *Asian Economic and Financial Review*, August 28, 2023: 18.

2. Alabi, O.F., and , A.A David. "Framework for Detection of Fraud at Point of Sale on Electronic Commerce sites using Logistic Regression." *EAI Endorsed Transactions on Scalable Information Systems*, 2023: 8.

3. Azima Noordin, Nora , Khaled Hussainey, Ahmad Faisal Hayek, and . . "The Use of Artificial Intelligence and Audit Quality: An Analysis from the Perspectives of External Auditors in the UAE." *Risk Financial Manag.*, 2022: 14.

4. Bertaut , Carol C, and Michael Haliassos. *SSRN Electronic Journal*, October 2006: 53.

5. Chowdhury, Gobinda G. "Natural Language Processing ." *The Annual Review of Information Science and Technology*, 2020: 37.

6. Dayyabu, Yusuf Yusu, Dhamayanthi Arumugam, Suresh Balasingam, and . "The application of artificial intelligence techniques in credit card fraud detection: a quantitative study." *E3S Web of Conferences 389, 07023*, 2023: 19.

7. Diadiushkin, Alexander, Kurt Sandkuhl, Alexander Maiatin, and . "Fraud Detection in Payments Transactions: Overview of Existing Approaches and Usage for Instant Payments." *Complex Systems Informatics and Modeling Quarterly (CSIMQ)*, October 2019: 72–88.

8. Ezeji, Chiji Longinus. "Artificial Intelligence for detecting and preventing procurement fraud." ***International*** *Journal of Business Ecosystem & Strategy, 6(1)*, 2024: 63-73.

9. Gavari, Kushal. "Computer Vision in Artificial Intelligence." *International Journal of Research Publication and Reviews Vol 3, no 10,*, October 2022: pp 1229-1231.

10. Igboanusi , Mirian O. "Factors Affecting the Preference of Debit cards to Credit cards in Nigeria." *International Journal of Advances in Engineering and Management (IJAEM)Volume 6, Issue 03*, Mar 2024: 14.

11. Ikhsan, Wishmy Meinawa, Elzami Haqie Ednoer, Winanda Setyaning Kridantika, and Amrie Firmansyah. "FRAUD DETECTION AUTOMATION THROUGH DATA ANALYTICS AND ARTIFICIAL INTELLIGENCE." *Jurnal Aplikasi Ekonomi, Akuntansi dan Bisnis Vol. 4 No. 2,*, September 2022.

12. Lai , Guangsheng. "Artificial Intelligence Techniques for Fraud Detection." *www.preprints.org*, December 15, 2023: 12.

13. Loukil, Manal , and Fayçal Messaoudi. "Defending against digital thievery: a machine learning approach to predict E-payment fraud." *International Journal of Management Practice* , January 2024: 1-18.

14. Mahesh, Batta. "Machine Learning Algorithms." *International Journal of Science and Research (IJSR),* 2018: 6.

15. NIȚĂ, Gabriel, Larisa GĂBUDEANU, Cosmin Constantin CERNAEANU, Gabriel Mărgărit RAICU, and Mircea Constantin ȘCHEAU. "ARTIFICIAL INTELLIGENCE AND KEY RISK INDICATORS IN CYBER FRAUDS PREVENTION." *Journal of Financial and Monetary Economics, Centre of Financial and Monetary Research "Victor Slavescu", vol. 11(1),*, October. 2023: pages 92-111.

16. Pinadero, Unai Pinadero. "Inteligencia Artificial en SAP." *eiposgrados.* August 28, 2024. https://eiposgrados.com/consultor-sap/inteligencia-artificial-en-sap (accessed December الاثنين, 2024).

17. Sardjonor, Wahyur, Wowon Priatna, Mohammad Tohir, and . "ARTIFICIAL INTELLIGENCE AS THE CATALYST OF DIGITAL PAYMENTS IN THE REVOLUTION INDUSTRY 4.0." *ICIC International*, 2021: 34.

18. Shoetan, Philip Olaseni, and Babajide Tolulope Familo. "TRANSFORMING FINTECH FRAUD DETECTION WITH ADVANCED ARTIFICIAL INTELLIGENCE ALGORITHMS." *Finance & Accounting Research Journal, Volume 6, Issue 4*, April 2024: 24.

19. Wang, Ziyue. "Research on the Application of Artificial Intelligence and Big Data Technology in Financial Fraud Detection." *urnal of Theory and Practice of Engineering Science ISSN: 2790-1505 Journal of Theory and Practice of Engineering Science ISSN: 2790-1505*, 4 2024: 4.

20. Rikhardsson, Pall , Kristinn R. Thórisson, Gudmundur Bergthorsson, and Catherine Batt. "Artificial intelligence and auditing in small- and medium-sized firms: Expectations and applications." *AI Magazine*, 2022: 323–336.

21. Seethamraju, Ravi , and Angela Hecimovic . "Impact of Artificial Intelligence on Auditing – An Exploratory Study." *Australian Journal of Management*, July 2022: 10.

22. حسين رضا مهدي . "البنك المركزي العرقي دائرة الرقابة على المصارف."*تطور الدفع الالكتروني في العراق*. بغداد: البنك المركزي لعراقي دائرة الرقابة على المصارف، 2024.

23. نافع بن عوض الله السهلي. "International Journal of Research and Studies Publishing ISSN: 2709-7064." *جريمة الاحتيال المالي والتعامل معها وفق القواعد القانونية في النظام السعودي*، 2023: 29.

24. ناهد عبادة.موضوع . ٢ ديسمبر، ٢٠٢١.
https://mawdoo3.com/%D8%AA%D8%B9%D8%B1%D9%8A%D9%81_%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1_%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A (تاريخ الوصول 01 jun, 2024).