العدد 22-2023

دراسات تطوير القطاع المالي

دور الذكاء الاصطناعي وتعلّم الآلة في تعزيز كشف الاحتيال على البطاقات الإئتمانية

إعداد: د.علي بن الضب

صندوق النقد العربي
ARAB MONETARY FUND

صندوق النقد العربي
ARAB MONETARY FUND

دراسة حول:

دور الذكاء الاصطناعي وتعلّم الآلة في تعزيز كشف الاحتيال على البطاقات الإئتمانية

د. علي بن الضب

صندوق النقد العربي

أغسطس 2023

يعد خبراء الدوائر الفنية بصندوق النقد العربي دراسات اقتصادية، وأوراقا بحثية، يصدرها الصندوق وينشرها على موقعه الرسمي بشبكة المعلومات العالمية. تتناول هذه الإصدارات قضايا تتعلق بالسياسات النقدية والمصرفية والمالية والتجارية وأسواق المال وانعكاساتها على الاقتصادات العربية.

الآراء الواردة في هذه الدراسات أو الأوراق البحثية لا تمثل بالضرورة وجهة نظر صندوق النقد العربي، وتبقى معبرة عن وجهة نظر معد الدراسة.

للاطلاع على الدراسة:

للاطلاع على الدراسات السابقة:

توجه جميع المراسلات إلى العنوان التالي:

الدائرة الاقتصادية

صندوق النقد العربي

ص.ب. 2818 – أبو ظبي – دولة الإمارات العربية المتحدة

هاتف: 97126171765+

البريد الالكتروني: economic@amfad.org.ae

Website: https://www.amf.org.ae

المحتويات

ملخص

أدى تطوّر التجارة الإلكترونية ونمو أنظمة الدفع الإلكتروني إلى زيادة كبيرة في استخدام بطاقات الائتمان للمعاملات عبر شبكة المعلومات العالمية (الإنترنت)، وصاحب هذا التطور ارتفاع كبير في عمليات الاحتيال على البطاقات الإئتمانية وما نجم عنها من تكاليف وخسائر للمؤسسات المالية وللأفراد. دفعت هذه التحديّات المؤسسات المالية وصانعي القرار إلى البحث عن طرق مبتكرة باستخدام التقنيات الحديثة، كالذكاء الاصطناعي وتعلّم الآلة وتطبيقاتها على البيانات الضخمة لكشف وتحليل عمليات الاحتيال، من خلال تصميم وتطوير طرق جديدة لكشف الاحتيال باستخدام بيانات المعاملات، وتحليل تفاصيل المعاملات السابقة وخصائص العملاء.

تهدف هذه الدراسة إلى إبراز أهم تطبيقات الذكاء الاصطناعي وتعلّم الآلة في تعزيز كشف الاحتيال على البطاقات الإئتمانية، والمقارنة بين نتائج خوارزميات تعلّم الآلة الخاضع للإشراف، بالتطبيق على لغة بايثون (Python) للبرمجة، باستخدام بيانات اصطناعية (Synthetic Data) تم إنشاؤها بطريقة عشوائية عن طريق المحاكاة للأرقام العشوائية لعينة تتكون من 200 ألف بطاقة إئتمانية، و20 متغير كخصائص لحامل البطاقة الإئتمانية باستخدام أربعة خوارزميات ممثلة في: خوارزمية الانحدار اللوجستي، أقرب الجيران (Nearest neighbours)، والتحليل التمييزي الخطي (Linear discriminant analysis) وشجرة القرار(Decision tree).

خلصت الدراسة إلى أن خوارزميات تعلّم الآلة تساهم في تعزيز كشف الاحتيال على البطاقات الإئتمانية بقدرة تنبؤية فاقت 94 في المائة، كما أن خوارزمية التحليل التمييزي الخطي كانت أفضل أداءً من بقية الخوارزميات المستخدمة، مما يدعم التوجّه نحو استخدام تقنيات تعلّم الآلة الحديثة، وفرص الاستفادة من العديد من الخوارزميات.

أوصت الدراسة بضرورة استخدام الذكاء الإصطناعي بصفة عامة، وتعلّم الآلة بصفة خاصة في تحليل عمليات الاحتيال على البطاقات الإئتمانية في الدول العربية، مما يساعد المؤسسات المالية والهيئات الإشرافية والتنظيمية والرقابية على إدارة المخاطر وتقليل التكاليف الناجمة عن هذه العمليات، خاصّة مع توجّه العديد من المحتالين إلى استخدام التقنيات الحديثة، مما يستدعي مواكبة التطورات العالمية الراهنة في هذا المجال.

الكلمات المفتاحية: بطاقات ائتمان، كشف احتيال، ذكاء اصطناعي، تعلّم الآلة.

Abstract

The use of credit cards for online purchases has significantly increased as a result of the growth of e-commerce and electronic payment systems. However, this rise has also resulted in an increase in credit card fraud and its cost, which has cost financial institutions and people a lot of money. Therefore, in order to identify and analyse fraud, financial institutions and decision-makers are under pressure to come up with novel solutions using cutting-edge technologies like artificial intelligence (AI) and machine learning (ML).

This paper aims to emphasize the key applications of artificial intelligence and machine learning in improving the detection of credit card fraud. Additionally, it aims to compare the outcomes of supervised machine learning algorithms implemented in the Python programming language. The study utilizes synthetic data, generated randomly through the simulation of random numbers, involving a sample of 200,000 credit cards and 20 variables representing credit card holder characteristics. Four algorithms, namely logistic regression, nearest neighbours, linear discriminant analysis, and decision tree, are applied for analysis and comparison purposes.

The study concluded that that machine learning algorithms significantly enhance the detection of credit card fraud, with a predictive accuracy exceeding 94 percent. Among the algorithms tested, the linear discriminant analysis algorithm outperformed the others, affirming the inclination towards employing modern machine learning techniques and leveraging various algorithmic opportunities in this domain.

The study recommended the adoption of AI, particularly ML, in analysing credit card fraud in Arab countries. This can help financial institutions and regulatory bodies to manage risks and reduce the costs associated with fraud, particularly with the increasing use of modern technologies by fraudsters. It is essential to keep up with global developments in this field to remain vigilant and prevent fraud.

Keywords: credit cards, fraud detection, machine learning, stander econometric model.

1. مقدمة

أدى نمو ثقافة الاعتماد المتزايد لشراء السلع والخدمات عن بُعد إلى تطوير التجارة الإلكترونية وأنظمة الدفع الإلكتروني عن بُعد. صاحب هذه التطورات ارتفاع كبير في عمليات الاحتيال على معاملات البطاقات الإئتمانية على المستوى العالمي، وما نجم عنها من تكاليف وخسائر للمؤسسات المالية وللأفراد (ECB, 2021)، حيث بلغ إجمالي خسائر الاحتيال على البطاقات الإئتمانية على مستوى العالم ما قيمته 32.34 مليار دولار أمريكي عام 2021، بزيادة قدرها 13.8 في المائة عن عام 2020 (Nilson, 2021). يحدث هذا النوع من النشاط الاحتيالي نتيجة الاستيلاء على معلومات بطاقة الائتمان بهدف شراء سلع أو خدمات أو سحب الأموال منها دون إذن صاحبها، لذلك أصبح من الضروري البحث عن أنظمة وطُرق فعّالة للكشف عن الأنشطة الاحتيالية الخاصة بالبطاقات الإئتمانية، وحماية المستخدمين والمؤسسات المالية من مخاطر هذه الأنشطة ذات الاتجاه المتزايد.

يشير الاحتيال على بطاقة الائتمان إلى الفقدان المادي للبطاقة البنكية، أو فقدان المعلومات الخاصة بها واستخدامها من قبل طرف أو أطراف أخرى دون إذن صاحبها (ECB, 2021). قرّرت العديد من البنوك والمؤسسات المالية تطوير منهجيات وطرق للتعامل مع عمليات الاحتيال على البطاقات الإئتمانية، وكيفية تجنب الاحتيال مسبقاً، وتم ابتكار العديد من الطرق والأفكار للحد من عمليات الاحتيال على هذه البطاقات حيث نجحت هذه الآليات بشكل جيّد لبعض الوقت، ولكن بمرور الوقت وفي ظل تكيّف المحتالين مع البيئة المتغيرة، تم كذلك ابتكارطرق جديدة للاحتيال، وأصبحت الأساليب التي تطبّقها بعض البنوك غير محدّثة خاصة في ظل تطور التقنيات الحديثة.

يُعدّ الاحتيال على البطاقة الائتمانية أحد القضايا الحاسمة، ويمثّل تحدّياً في مجال المعاملات عبر شبكة المعلومات العالمية، وبالتالي أصبحت هناك حاجة كبيرة لتطوير أفضل الطرق الممكنة استناداً إلى التقنيات الحديثة من أجل وضع حدٍّ لهذه المعاملات الاحتيالية.

دفعت هذه التحدّيات المؤسسات المالية إلى البحث عن طرق مبتكرة لكشف وتحليل عمليات الاحتيال على المعاملات المالية عن بُعد، من خلال تصميم وتطوير طرق جديدة لكشف الاحتيال باستخدام بيانات المعاملات، وتحليل تفاصيل المعاملات السابقة وخصائص العملاء. يتم استخدام عدة طرق لكشف الاحتيال، بما في ذلك، التحليل الإحصائي، والأنظمة المستندة إلى القواعد (Rules-based systems)، وتصنيف الاحتيال (Fraud scoring) والذكاء الاصطناعي وتعلم الآلة. يتم تحليل البيانات لتحديد الأنماط، واستخدام قواعد محددة مسبقًا للإبلاغ عن المعاملات المشبوهة، وتعيين درجات الاحتيال بناءً على عوامل الخطر، واستخدام خوارزميات تعلم الآلة للتعلم من البيانات التاريخية والتنبؤ بالاحتيال. يمكن من خلال هذه الطرق تقييم المعاملات بشكل شامل، مما يقلّل من احتمالية حدوث عمليات احتيال مفاجئة. تسمح هذه الطرق بتحديد الأنشطة الاحتيالية والحد منها بشكل استباقي، مما يضمن حماية مصالح الأفراد.

يهدف كشف الاحتيال على بطاقة الائتمان إلى تحديد ووضع حد للأنشطة الاحتيالية على بطاقة الائتمان أو أي بطاقة دفع أخرى، باستخدام طرق مختلفة للتنبؤ بالمعاملات المشبوهة ومراقبتها وايقافها. إضافة إلى ذلك، قد تستخدم المؤسسات المالية، وشركات بطاقات الائتمان أيضًا بيانات من مصادر خارجية مثل وكالات الاستعلام الائتماني للمساعدة في كشف الاحتيال والحد من آثاره.

أتاح عصر الذكاء الاصطناعي وتعلّم الآلة امتلاك أنظمة وخوارزميات وطرق قادرة على التعديل بصفة آلية وفقًا للبيئة المتغيرة، مع ضرورة توفر البيانات الجيّدة الخاصة بالبيئة الحالية في أقرب وقت ممكن. تم إنشاء وتطوير العديد من أنظمة الكشف عن الاحتيال الحديثة، وما زال البحث جارياً في ظل التطوّر السريع للتقنيات الحديثة وكذلك طرق الاحتيال (Kulatilleke, 2022).

يمكن استخدام العديد من خوارزميات تعلّم الآلة للكشف عن الاحتيال على البطاقات الائتمانية حيث تتمتع هذه الخوارزميات بالقدرة على "تعلم" الخصائص المعقدة من أجل تحديد عمليات الاحتيال في الوقت الفعلي، متجاوزة بذلك الطرق التقليدية (Alfaiz, & Fati, 2022). مع ذلك، كانت التطوّرات في خوارزميات الكشف عن الاحتيال صعبة وبطيئة بسبب الطبيعة غير المتوازنة بشكل كبير لبيانات الاحتيال، وغياب المعايير ومقاييس التقييم القياسية لتحديد الخوارزميات ذات الأداء الأفضل، وعدم مشاركة نتائج البحث والكشف عنها، والصعوبات الخاصة بالوصول إلى بيانات المعاملات الاحتيالية للبحث، والتي تعتبر سرية للغاية في أغلب الحالات.

يوفر تعلم الآلة العديد من المزايا مقارنة بالطرق الأخرى لكشف الاحتيال على بطاقات الائتمان، كونه يعزز الدقة من خلال تحليل كميات هائلة من البيانات وتحديد الأنماط المرتبطة بالنشاط الاحتيالي، كما يمكن لخوارزميات تعلم الآلة التوسع للتعامل مع الكميات الكبيرة من المعاملات التي تتم معالجتها، مما يضمن التحليل الفعال وفي الوقت المناسب، إضافة لذلك تتكيف خوارزميات تعلم الآلة مع أنماط الاحتيال المتطورة مما يمكّن الشركات من البقاء في طليعة التقنيات الاحتيالية الجديدة. تعتبر القدرة على التكيف أمراً بالغ الأهمية حيث يبتكر المحتالون باستمرار أساليب جديدة. بالإضافة إلى ذلك، فعالية الحلول القائمة على تعلم الآلة من حيث التكلفة لأنظمة الكشف عن الاحتيال، والتخفيف بشكل فعال من المخاطر وحماية مصالح العملاء.

تعمل هذه الدراسة على إبراز دور وأهمية خوارزميات تعلّم الآلة الخاضع للإشراف باعتبارها أحد فروع الذكاء الاصطناعي في تعزيز كشف الاحتيال على البطاقات الإئتمانية. كما تعرض أهم الخوارزميات التي يمكن استخدامها في تصنيف المعاملات على أنها احتيالية أو غير احتيالية، والوقوف على أهم الإحصائيات الخاصة بالخسائر الناجمة عن عمليات الإحتيال على البطاقات الإئتمانية على المستوى الدولي، وتقديم بعض الإجراءات الاحترازية والتوصيات للجهات الإشرافية، والرقابية في الدول العربية من أجل المساهمة في تعزيز كشف العمليات الاحتيالية على بطاقة الائتمان باستخدام الذكاء الاصطناعي وتعلم الآلة، مما يعمل على تقليل المخاطر المالية الناجمة عن الأنشطة الاحتيالية، وما لها من تداعيات على القطاع المالي في الدول العربية.

تم تقسيم هذه الدراسة إلى ستة أقسام أساسيّة، بعد المقدمة، يستعرض القسم الثاني أهم الدراسات السابقة الخاصة باستخدام خوارزميات تعلّم الآلة في كشف الاحتيال على البطاقات الإئتمانية. يصف القسم الثالث الخلفية النظرية لعمليات الاحتيال على البطاقات الإئتمانية وأنواعها مع تقديم إحصائيات حديثة حول عمليات الاحتيال على بطاقات الائتمان على المستوى الدولي وتقديم أهم الإجرات الاحترازية، وكذلك طرق الكشف عن الاحتيال على البطاقات الإئتمانية في ظل التقنيات الحديثة. يتم في القسم الرابع تقديم الدراسة التطبيقية، بما في ذلك البيانات المستخدمة، والتعريف بأهم الخوارزميات المعتمدة في الدراسة ومعايير المفاضلة بينها. يناقش القسم الخامس نتائج الدراسة والمقارنة بين أداء ونتائج خوارزميات تعلّم الآلة. يتم في القسم السادس والأخير تقديم أهم الاستنتاجات والتوصيات.

2. الدراسات السابقة لاستخدام تعلّم الآلة في كشف الاحتيال على البطاقات الإئتمانية

نال موضوع تطوير آليات كشف الاحتيال على البطاقات الإئتمانية باستخدام التقنيات المالية الحديثة لاسيما خوارزميات تعلّم الآلة حيزاً معتبراً من اهتمامات المؤسسات الرائدة في الصناعة المالية والمصرفية، وكذلك الباحثين المهتمين بتطوير نماذج مختلفة للمساهمة في الكشف المبكر والحد من آثار الاحتيال على

البطاقة الائتمانية. في هذا الإطار قامت منظمة (IEEE-CIS[1]) بالشراكة مع شركة خدمات الدفع (Vesta)، بالإعلان عن جائزة معتبرة لمسابقة بعنوان "IEEE-CIS Fraud Detection" حيث طُلب من المتنافسين تقييم نماذج تعلّم الآلة على مجموعة بيانات صعبة وواسعة النطاق. من جهة ثانية، ناقش العديد من الباحثين موضوع الاحتيال على البطاقات الإئتمانية من أوجه مختلفة لتطبيقات تعلّم الآلة، فهناك دراسات اهتمت بخوارزميات التصنيف، ودراسات اهتمت بخوارزميات الانحدار والنمذجة، ودراسات أخرى جمعت بينهما، ونعرض فيما يلي أهم الدراسات الحديثة في هذا الموضوع.

استخدم الباحثون مناهج مختلفة لتعلّم الآلة لكشف الاحتيال على البطاقات الإئتمانية، خاصة في ظل زيادة التجارة الإلكترونية ونمو الدفع عبر شبكة المعلومات العالمية، والارتفاع المسجل في معدلات الاحتيال عبرها. اهتمت دراسة (Sandhya et al., 2023) بكشف الاحتيال على بطاقات الائتمان باستخدام خوارزميات تعلّم الآلة، من خلال بناء وإنشاء نهج جديد للكشف عن الاحتيال لتدفقات بيانات المعاملات، بهدف تحليل تفاصيل المعاملات التاريخية للعميل واستخراج الأنماط السلوكية. خلصت الدراسة إلى أن خوارزمية الغابة العشوائية (Random Forest) تتفوق في الأداء على خوارزمية "بايز" (Naive Bayes) في كشف الاحتيال على بطاقة الائتمان. كما أوصت الدراسة باستخدم استخدام الشبكة العصبية في المستقبل وفقًا لإعدادات محددة.

أشارت الدراسة الاستقصائية لـ (Berkmans & Karthick, 2023) إلى أهم الدراسات التي طبّقت تقنيات تعلّم الآلة وطرق إثبات المستخدم منها للكشف عن الاحتيال على بطاقات الائتمان، حيث تم تقسيم الدراسات السابقة في هذا الموضوع إلى جزأين أساسيين، تم في الجزء الأول التركيز على نماذج الذكاء الاصطناعي القديمة، والاستراتيجية القائمة على المعرفة (knowledge-based strategy) في الجزء الثاني، تم التركيز بشكل أكبر على إجراءات التحقق من العميل، وإجراء القياسات الحيوية (biometrics) لتمييز السلوك الفردي أثناء استخدام أدوات الدفع الإلكترونية. تتمثل الخطوط العريضة لهذه الدراسة في تطوير نموذج أكثر دقة يمكن الاعتماد عليه، متعدد الاستخدامات وفعّال لتحديد هوية المحتال على البطاقة الإئتمانية.

اقترحت دراسة (Van Belle et al. , 2023) طريقة جديدة تسمى (CATCHM)، بهدف الكشف عن الاحتيال على بطاقات الائتمان. تقوم هذه الطريقة على تحليل الشبكة باستخدام خوازميات التعلّم التمثيلي (representation learning). أبرزت الدراسة أهمية التعلم التمثيلي في الكشف عن الاحتيال من خلال التركيز على البنية العلائقية للمعاملات. يُظهر التقييم التجريبي الشامل لمجموعة بيانات بطاقة الائتمان الواقعية أن الطريقة المقترحة تتفوق في الأداء على أحدث الأساليب، مما يوضح الأهمية العملية لهذا النهج في الصناعة المالية ومواجهة تحديات عمليات الاحتيال على البطاقات الإئتمانية.

للوقوف على التحديات والتعقيدات في كشف الاحتيال القائم على تعلّم الآلة لبطاقات الائتمان، في ظل إسهامات تعلّم الآلة والذكاء الاصطناعي وتحليل البيانات الضخمة في إتاحة أدوات جديدة لمكافحة عمليات الاحتيال، سلّطت دراسة (Kulatilleke, 2022) الضوء على خصائص مجموعات بيانات الاحتيال النموذجية غير المتوازنة على نطاق واسع، ومدى توفرها، ومدى ملاءمتها للاستخدام البحثي أثناء استكشاف الطبيعة المتنوعة على نطاق واسع لتوزيعات الاحتيال. كما تم توضيح كيف تتراكم الأخطاء البشرية مع أخطاء تصنيف الجهاز. من خلال إجراء تجارب لتحديد تأثير تشويش تحليل المكوّنات الأساسية (PCA) على أداء خوارزمية التصنيف، وإبراز أن تحليل المكوّنات الأساسية لا يؤدي إلى تراجع الأداء

[1] IEEE Computational Intelligence Society هي منظمة تعمل عبر مجموعة متنوعة من مجالات الذكاء الاصطناعي وتعلم الآلة ، بما في ذلك الشبكات العصبية العميقة والأنظمة الضبابية والحسابات التطورية وذكاء السرب.

بشكل كبير، وعلى الرغم من ذلك ينبغي توخي الحذر عند استخدام حجم المكون الأساسي المناسب (تقليل الأبعاد) لتجنب أحد التحديات الرئيسة والمتمثلة في التثبيت الزائد (overfitting).

عملت دراسة (Jovanovic, et al. 2022) على ضبط نماذج تعلّم الآلة باستخدام خوارزمية البحث الجماعي (Firefly) للكشف عن الاحتيال الذي تتعرض له بطاقات الائتمان، وقدّمت نهجاً هجيناً لتعلّم الآلة مع خوارزمية سرب الأدلة العليا (swarm metaheuristic) لمواجهة تحدي كشف الاحتيال على بطاقات الائتمان. تم تصميم خوارزمية (Firefly) للبحث الجماعي، ثم تطبيقها على مجموعة بيانات كشف احتيال بطاقات الائتمان في العالم الحقيقي، والتي تخص معاملات مستخدمي بطاقات الائتمان الأوروبية، ونظراً لأن مجموعة البيانات الأصلية غير متوازنة للغاية، تم توسيع مجموعة البيانات من خلال استخدام طريقة أخذ العينات الاصطناعية. تمت مقارنة أداء الخوارزمية المقترحة باستخدام مؤشرات أداء تعلّم الآلة القياسية للتقييم (مثل دقة المصنف، والاستدعاء والدقة، والمنطقة الواقعة أسفل المنحنى). أظهرت النتائج التجريبية بوضوح أن النماذج التي تم ضبطها بواسطة الخوارزمية المقترحة حصلت على نتائج متفوقة مقارنة بالنماذج الأخرى المهجّنة.

اهتمت دراسة (Roseline et al., 2022) بكشف الاحتيال على بطاقات الائتمان بطريقة تلقائية باستخدام نهج تعلّم الآلة، بهدف معرفة كيفية كشف الاحتيال وتوقّع حدوثه، تم اقتراح إنشاء شبكة عصبية متكررة للذاكرة طويلة المدى (LSTM-RNN). بالإضافة إلى تضمين آلية التنبيه لزيادة الأداء أكثر. في حالات مثل كشف الاحتيال، حيث يتكون تسلسل المعلومات من نواقل ذات خصائص مترابطة معقدة، أثبتت النماذج التي تحتوي على هذا الهيكل أنها فعّالة بشكل خاص. تمت مقارنة نتائج الشبكة العصبية المتكررة للذاكرة طويلة المدى مع المصنفات الأخرى، مثل: خوارزمية "بايز"، وخوارزمية آلة المتّجه الداعم (Support Vector Machine)، والشبكات العصبية الاصطناعية (ANN)، حيث أبرزت النتائج أن النموذج المقترح ذو نتائج قوية ومستوى عالٍ من الدقة.

اقترحت دراسة (Esenogho et al. 2022) طريقة للكشف عن الاحتيال على بطاقة الائتمان باستخدام مصنّف مجموعة الشبكة العصبية وطريقة إعادة تشكيل البيانات المختلطة، حيث يُعد تطوير خوارزميات فعّالة للكشف عن الاحتيال أمراً حيوياً في تقليل هذه الخسائر، ولكنه يمثل تحدياً لأن معظم مجموعات بيانات بطاقات الائتمان غير متوازنة إلى حد كبير، كما أن استخدام خوارزميات تعلّم الآلة التقليدية للكشف عن الاحتيال على بطاقات الائتمان يُعد غير فعّال بسبب تصميمها، والذي يتضمن تعييناً ثابتاً لمتجه الإدخال إلى متجهات الإخراج. ونتيجة لذلك لا يمكن لهذه التقنيات التكيف مع سلوك التسوّق الديناميكي لعملاء بطاقات الائتمان. في هذه الدراسة تم الحصول على مصنف المجموعة باستخدام شبكة عصبية للذاكرة طويلة المدى (LSTM) كمُتعلم أساسي في تقنية التعزيز التكيفي (AdaBoost). وفي الوقت نفسه يتم تحقيق إعادة التشكيل الهجينة باستخدام تقنية زيادة عينات اصطناعية وتعديل خوارزمية أقرب الجيران (SMOTE-ENN). تم إثبات فعالية الطريقة المقترحة باستخدام مجموعة بيانات معاملات بطاقات الائتمان الواقعية المتاحة للجمهور. وتم قياس أداء النهج المقترح مقابل الخوارزميات التالية: آلة متجه الدعم (SVM) المستقبلات متعددة الطبقات (MLP)، شجرة القرار، تقنية التعزيز التكيفي (AdaBoost) التقليدية والذاكرة الطويلة والقصيرة (LSTM). أظهرت النتائج التجريبية أن خوارزميات التصنيف (المصنّفات) كان أداؤها أفضل عند تدريبها باستخدام البيانات المعاد تشكيلها، وأن الطريقة المقترحة تفوّقت على الخوارزميات الأخرى.

حاولت دراسة (Alharbi et al., 2022) تقديم آلية جديدة تقوم بتحويل النصوص إلى صورة (text2IMG) للكشف عن الاحتيال على بطاقة الائتمان، حيث قدّمت العديد من الدراسات الحديثة حلولاً قائمة على تعلّم الآلة للكشف عن معاملات بطاقات الائتمان الاحتيالية، لكن نتائج الكشف عنها لا تزال

بحاجة إلى التحسين بسبب عدم توازن الفئات في مجموعة البيانات. تم تطوير نهج قائم على التعلّم العميق (DL) لحل مشكلة البيانات النصية، واقتراح تقنية جديدة لتحويل النصوص لتوليد صور صغيرة، وتم إدخال الصور في بنية الشبكة (CNN) باستخدام أوزان الفئة باستخدام طريقة التردد العكسي لحل مشكلة عدم توازن الفئة، من خلال تطبيق نهج التعلّم العميق وتعلّم الآلة للتحقق من متانة وصلاحية الطريقة المقترحة. تم تحقيق دقة في التنبؤ بقيمة 99.87 في المائة باستخدام خوارزمية (Coarse-KNN) بالاعتماد على الميزات العميقة لشبكة (CNN) المقترحة. توفر هذه الطريقة بُعدًا جديدًا للكشف عن الاحتيال على بطاقات الائتمان باستخدام تقنيات الرؤية الحاسوبية، وتقدم اتجاهات مستقبلية لتحويل أنواع أخرى من البيانات النصية إلى صورة، مما يتيح تصنيف البيانات بأنماط مختلفة، كما أوصت الدراسة بتطبيق طريقة التصنيف المستندة إلى هذه الطريقة في كشف الاحتيال على بطاقات الائتمان المماثلة أو مجموعات البيانات النصية الأخرى، كما يمكن استخدام طرق عدم توازن الفئات الأخرى وتطبيق الميزات العميقة على طرق التصنيف القائمة على تعلّم الآلة.

تم في دراسة (Alfaiz, & Fati, 2022) تقديم نموذجٍ محسّنٍ للكشف عن الاحتيال على بطاقة الائتمان باستخدام تعلّم الآلة من خلال دراسة 66 نموذجاً لتعلّم الآلة بناءً على مرحلتين من التقييم. تهدف المرحلة الأولى إلى ترشيح أفضل ثلاث خوارزميات لتعلّم الآلة من بين تسعة خوارزميات، والمرحلة الثانية تهدف إلى دمج أفضل ثلاث خوارزميات مع 19 تقنية إعادة تشكيل. تم استخدام مجموعة بيانات كشف احتيال بطاقات الائتمان في العالم الحقيقي لحاملي البطاقات الأوروبية. تشير النتائج إلى أن النموذج المقترح يتفوق على النماذج السابقة، ولديه قدرة على التنبؤ بنسبة 97.94 في المائة، كما أوصت الدراسة باستخدام مجموعة بيانات أخرى، وخوارزميات تحسين أخرى، مثل: (MBO)، (EWA)، (EHO)، (MS)، (SMA)، و(HHO)[2].

قارنت دراسة (Khatri et al., 2020) بين خوارزميات تعلّم الآلة الخاضع للإشراف في الكشف عن الاحتيال على بطاقات الائتمان للتمييز بين المعاملات الحقيقية والاحتيالية. تم الاعتماد على معايير الحساسية، والدقة، والوقت كمعلمات حاسمة للوصول إلى نتيجة أحسن. تم استخدام خمسة خوارزميات لتعلّم الآلة الخاضع للإشراف بغرض التنبؤ بفرص حدوث معاملة بطاقة ائتمان احتيالية من عدد معين من المعاملات. خلصت الدراسة أن النموذج الأنسب للتنبؤ بمثل هذه العمليات الاحتيالية هو نموذج شجرة القرار. يُظهر التحليل أن حساسية خوارزمية أقرب الجيران (kNN) أكبر من حساسية شجرة القرار، ولكن نظرًا لأن الوقت الذي تستغرقه خوارزمية أقرب الجيران لاختبار البيانات كبير جدًا، لذلك تم اختيار شجرة القرار لكشف الاحتيال على البطاقات الإئتمانية، كونها تستغرق الحد الأدنى من الوقت للتنبؤ وبالتالي هي النموذج الأفضل. أوصت الدراسة في هذا المجال بتطبيق تقنيات إعادة التشكيل على مجموعات البيانات المستخدمة كونها تساعد في تقليل نسبة عدم التوازن لمجموعة البيانات، والتي بدورها تنتج نتائج تصنيف أفضل. كما ينبغي أيضًا تقييم أداء نموذج شجرة القرار بمساعدة نماذج تعلّم الآلة غير الخاضعة للإشراف في المستقبل لإنتاج نتيجة أكثر شمولية.

ما يُميّز هذه الدراسة عن الدراسات السابقة كونها تُقارن أداء خوارزميات تعلّم الآلة من جهة، ومن جهة ثانية تعتمد على بيانات اصطناعية، تمت محاكاتها بطريقة عشوائية، وهذا في ظل عدم توفر بيانات خاصة بالاحتيال على البطاقات الائتمانية في المنطقة العربية، حيث يمكن تحقيق هدف الدراسة لإبراز أهمية خوارزميات تعلّم الآلة، مع توفير خلفية نظرية وتطبيقية حول الموضوع للهيئات الإشرافية والرقابية في

[2] Monarch Butterfly Optimization (MBO) , Earthworm Optimization Algorithm (EWA) , Elephant Herding Optimization (EHO) , Moth Search (MS) algorithm , Slime Mold Algorithm (SMA), and Harris Hawks Optimization (HHO).

الدول العربية، ويمكن إعادة تطبيق هذه التقنيات الحديثة على بيانات حقيقية، بالرجوع إلى هذه الدراسة والاستفادة من الخطوات واستخدام برمجية "Python".

3. أنواع الاحتيال على البطاقات الإئتمانية والإجراءات الاحترازية

يشير الاحتيال على البطاقات الإئتمانية إلى أي نشاط غير قانوني يتضمن الاستخدام غير المصرح به لبطاقة بنكية أو معلومات بطاقة الائتمان لإجراء عمليات شراء أو سحب نقود أو إجراء معاملات مالية أخرى. يمكن أن يتم ذلك بعدة طرق وأنشطة مثل التصيد الاحتيالي أو سرقة البطاقة أو غيرها من الطرق. يمكن أن تؤدي هذه الأنشطة إلى خسائر مالية لكل من جهة إصدار بطاقة الائتمان، وحامل البطاقة، كما يمكن أن تلحق الضرر بالتصنيف الائتماني لحامل البطاقة، كما يمكن أن تؤثر هذه العمليات على ثقة الأفراد في المؤسسات المالية، مما ينعكس على متانة النظام المالي واستقراره في الأخير. يمثل الاحتيال على البطاقات الإئتمانية أحد أشكال سرقة الهوّية التي تنطوي على أخذ معلومات بطاقة ائتمان شخص ما بشكل غير مصرح به لغرض تحصيل رسوم المشتريات من الحساب أو سحب الأموال منه، كما يمثل الاحتيال أي فعل متعمّد أو غير متعمّد يهدف إلى خداع الآخرين، مما يؤدي إلى تحميل الضحية لخسارة و/أو تحقيق المحتال لمكاسب، على الرغم من أن بعض الدول تحد من مسؤولية حالمي البطاقة الإئتمانية، فمثلا وفق القانون الاتحادي في الولايات المتحدة الأمريكية ((Richards, et al., (n.d)، وبموجب القانون 15 (U.S.C. §1643)، يتم تحميل مسؤولية الخسائر لحاملي البطاقات في حدود 50 دولاراً أمريكياً في حالة سرقة بطاقة الائتمان، ولكن في بعض الحالات تتنازل البنوك عن هذا المبلغ إذا وقع حامل البطاقة على إفادة خطية تشرح عملية فقدان البطاقة.

1.3.أنواع الاحتيال على البطاقات الإئتمانية

يمكن تقسيم أنواع الاحتيال على بطاقات الائتمان بصفة عامّة إلى صنفين: (1) المعاملات الاحتيالية بالاستخدام المادي للبطاقات البنكية (الاحتيال باستخدام البطاقة)، مثل عمليات السحب النقدي ببطاقات مزيفة أو مسروقة، وهذا النوع ليس شائعًا بصورة كبيرة في الوقت الحاضر(Delamaire, et al., 2009)، و(2) المعاملات الاحتيالية التي يتم إجراؤها عن بُعد (الاحتيال بدون وجود البطاقة (Card not present "CNP")، وهو النوع الأكثر شيوعًا في الوقت الحالي (ECB, 2021). يشمل النوع الثاني كل ما يقوم به المحتالون بإجراء مدفوعات عبر شبكة المعلومات العالمية باستخدام تفاصيل البطاقة التي يتم الحصول عليها من خلال التصيد الاحتيالي، أو خرق البيانات، أو طرق أخرى، وتتم التسوية بعدة طرق، ويمكن أن تحدث عادة دون علم صاحب البطاقة. يأخذ الاحتيال على البطاقات الإئتمانية العديد من الأشكال والأحجام، يمكن أن يحدث ذلك عبر شبكة المعلومات العالمية، أو عبر الهاتف، أو يمكن استخدام رسائل البريد الإلكتروني المزيفة، أو يتم سرقة معلومات من خلال اختراق البيانات، (Alharbi et al., 2022) أو يتم ُسرقة بطاقة الائتمان من صندوق البريد. نعرض فيما يلي بعض الأنواع الشائعة لعمليات الاحتيال على بطاقات الائتمان وطرق الحماية منها.

1.1.3. المعاملات الاحتيالية بالاستخدام المادي للبطاقات البنكية

يشمل هذا النوع ثلاث حالات، سواءً عن طريق استخدام البطاقة ذاتها أو الحصول على نسخة ثانية من البطاقة، أو تزويرها، وفيما يلي عرض لهذه الأصناف:

أ. الاحتيال الناجم عن فقدان أو سرقة البطاقات الإئتمانية

يحصل المحتالون وفق هذا النوع من الاحتيال على بطاقات الائتمان عن طريق السرقة، أو بالحصول على بطاقة مفقودة. يحاول المحتال في هذه الحالة استخدام معلومات بطاقة الائتمان في المعاملات عبر شبكة المعلومات العالمية أو عمليات الشراء الأخرى، واحدة من أكثر مخططات الاحتيال الأساسية لبطاقات الائتمان هي ببساطة سرقة بطاقة ائتمان لشخص ما، أو استخدام بطاقة فقدها شخص ما. يمكن أيضًا سرقة بطاقات الائتمان المرسلة إلى أصحابها عبر البريد (ECB, 2021).

ب. الاحتيال من خلال طلب نسخة من البطاقة الإئتمانية

يستخدم المحتالون وفق هذا النوع المعلومات الشخصية المسروقة (الإسم والعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وغيرها من البيانات) لتقديم طلب للحصول على بطاقة الائتمان. يمكن أن يستمر هذا النوع من الاحتيال دون أن يتم كشفه حتى يتقدم الضحية بطلب للحصول على الائتمان بنفسه أو يتحقق من تقرير الائتمان الخاص به. في حين أن الضحية لن يكون عادةً مسؤول عن أي مشتريات تتم باستخدام حسابات بطاقة ائتمان احتيالية بسبب الحماية التي توفرها البطاقات، لذلك هذا النوع من الاحتيال قد يضر بدرجة ائتمان الضحية والتصنيف الإئتماني له.

ت. الاحتيال من خلال إنشاء نسخة من البطاقة الأصلية

يعتمد المحتالون في هذه الحالة على أجهزة احتيال للحصول على معلومات بطاقة الائتمان بشكل غير قانوني مثل "scrapers". تستطيع هذه الأجهزة التقاط معلومات بطاقة الائتمان من الشريط المغناطيسي المتصل بالبطاقة عندما يتم تمرير البطاقات دون علم حامل البطاقة بهذا الجهاز. يمكن للمحتالين بعد ذلك نسخ هذه المعلومات لإنشاء بطاقات مزيفة واستخدامها، أو بيع بيانات البطاقة لجهات إحتيالية أخرى (Delamaire et al., 2009).

2.1.3. الاحتيال بدون وجود البطاقة الإئتمانية (CNP)

ينجُم هذا النوع من الاحتيال عن طريق وصول المحتالين إلى البيانات الشخصية لحامل البطاقة الإئتمانية، ومن ثمة يستخدمونها لإجراء عمليات الشراء عبر شبكة المعلومات العالمية أو عبر الهاتف. يعتبر هذا النوع صعباً في منعه نظراً لعدم وجود بطاقة فعلية لفحصها، ويصعب على الجهات التي تتلقى المدفوعات باستخدام البطاقة التحقق من هوية المشتري (ECB, 2021). ويكون هذا النوع من الاحتيال بعدة طرق منها:

أ. الاحتيال عبر البريد الإلكتروني

يقوم المحتالون وفق هذه الطريقة بإرسال رسائل عبر البريد الإلكتروني لأشخاص مستهدفين للحصول على البيانات الشخصية، مثل تاريخ ميلادهم، والأسماء الكاملة، وتفاصيل العنوان وما إلى ذلك، ومن خلال سرقة أكبر قدر ممكن البيانات والوثائق الداعمة قدر الإمكان لتنفيذ عملهم، واختراق جهاز الكمبيوتر ومن ثمة يتم استخدام هذه البيانات لاختراق الحساب البنكي أو بيانات البطاقة لاستخدامها في عمليات الشراء وتحويل الأموال.

ب. عمليات الاحتيال عبر الهاتف

أصبح هذا النوع من الاحتيال على بطاقات الائتمان أكثر شيوعاً، حيث يتصل المحتال بحامل البطاقة الإئتمانية ، ويحصل على معلومات شخصية حسّاسة مثل تاريخ الميلاد وكلمات المرور وتفاصيل البطاقة. غالباً ما يتم إجراء مثل هذه المكالمات من المحتال متظاهراً بأنه الفريق الفني للبنك، ويقوم المتصل بعملية تمثيلية مقنعة تجعل صاحب البطاقة يفشي معلومات حسّاسة.

ت. الاحتيال باستخدام أجهزة قراءة بيانات البطاقة

يعتبر جهاز قارئ البطاقة الاحتيالي "scrapers" أحد أجهزة الاستيلاء على معلومات بطاقة الائتمان من الشريط المغناطيسي الموجود على ظهر البطاقة، ويتم ذلك من خلال إرفاق المحتالين أجهزة قراءة بجانب أجهزة الصراف الآلي، أومتاجر البيع بالتجزئة، أومحطات الوقود أوغيرها. ثم يقومون إما ببيع المعلومات إلى محتالين آخرين، أو استخدامها لتحصيل مبالغ من البطاقة المستهدفة.

إضافة إلى الأنواع السالفة يوجد نوع آخر وهو الاحتيال المتعلق بالإفلاس، ويعتبر من أصعب أنواع الاحتيال التي يمكن توقعها. توجد بعض الأساليب والتقنيات للمساعدة في الوقاية منه. يعني الاحتيال المتعلق بالإفلاس استخدام بطاقة ائتمان لأفراد في حالة عسر مالي، حيث يستخدم حامل بطاقة الائتمان وهو يعلم أنه غير قادر على دفع المستحقات، ويقوم البنك بإرسال أمراً بالدفع، لكنه يعترف بأنه في حالة إفلاس شخصي وغير قادر على سداد ديونه. يتحمل البنك في الأخير تغطية الخسائر، خاصة وأن هذا النوع الخسائر ليس مشمولاً في الحساب المخصص للخسائر المحتملة. تتمثل الطريقة الأحسن لمنع الاحتيال المتعلق بالإفلاس في إجراء فحص مسبق مع مكاتب الاستعلام الائتماني (credit bureau) من أجل الحصول على المعلومات والتقارير الإئتمانية للعملاء[3].

3.1.3. الاحتيال باستخدام الذكاء الاصطناعي وتعلّم الآلة لتزييف الهوية السمعية والمرئية

تلجأ العديد من المصارف والمؤسسات المالية إلى استخدام الهوية الصوتية كأداة لمنع المحتالين من الوصول إلى البيانات المالية للأفراد والمؤسسات، ويتم إنشاء بصمة صوت فريدة لاستخدامها بطرق متعددة للتحقق من الهوية، حيث يمكن التعرّف على أنماط الكلام والتحقق من الهوية بعد التحدث بحرية إلى أحد الوكلاء بالمصرف، كما يمكن استخدام كلمة مرور للحساب من خلال نطق عبارة محددة. توجد أنظمة تقوم بعمليات الفحص اللازمة لضمان أن الصوت المسموع ليس مقلدًا أو مسجلاً، لكن على الرغم من ذلك يستخدم المحتالون التقنيات الحديثة مثل ""deep voice"" لاستنساخ خطاب شخص ما متاح على شبكة المعلومات العالمية للاحتيال. يعتبر هذا النوع من الاحتيال من أخطر الأنواع، حيث تمثل التزييفات السمعية والمرئية العميقة التطور المذهل للتقنيات الحديثة، لكنها أيضاً من المحتمل أن تكون خطرة بشكل غير متوقع، وتشكّل تهديداً للبيانات في قطاع الأعمال عموماً والقطاع المالي خصوصاً (Euronews, 2023).

2.3. الإجراءات الإحترازية للحد من الاحتيال على البطاقات الإئتمانية

أصبح الاحتيال من بين أهم التحديات التي تواجه المدفوعات الرقمية في ظل تطور التقنيات الحديثة، وعلى الرغم من عدم إمكانية القضاء على هذه الأنشطة بصفة كاملة، يمكن أن تؤدي الإجراءات المتخذة في الوقت المناسب إلى التقليل من عمليات الاحتيال وآثارها (Bai, & Chen, 2013)، وكشف المخاطر الناجمة عنها وتجنّبها. هناك حاجة إلى تقنيات مختلفة نظراً لوجود أنواع مختلفة من الاحتيال على بطاقات الائتمان (Sybersource, 2022).

تشمل أهم الإجراءات الإحترازية ما يلي:

[3] في ألمانيا ، على سبيل المثال ، بعض مكاتب الائتمان الأكثر استخدامًا هي SCHUFA و CEG. يقدم SCHUFA ، باعتباره مكتب الائتمان الرائد في ألمانيا حلول لعملائها خلال عملية إدارة المخاطر بأكملها ؛ يتم تخزين 62 مليون سجل في قاعدة بياناتهم. عادة ما تقدم مكاتب الائتمان تقارير عن قطاعات متنوعة ، مثل البنوك الخاصة ، وبنك الادخار ، البنوك التعاونية ومعاهد الائتمان الخاصة وما إلى ذلك ، وشركات بطاقات الائتمان.

1.2.3. من قبل الجهات الحكومية والتنظيمية

نفّذت الحكومات في جميع أنحاء العالم تدابير احترازية مختلفة، تم تصميم هذه الإجراءات لحماية كل من المستهلكين والشركات من الأنشطة الاحتيالية ولضمان نزاهة النظام المالي (Bai, & Chen, 2013).

تعاملت الحكومات بالعديد من الطرق مع الاحتيال على بطاقات الائتمان من خلال تنفيذ التشريعات واللوائح التي تتطلب من الشركات الامتثال لتدابير أمنية محددة، كأن تطلب من الشركات استخدام تقنية الشريحة والرقم السري لمعاملات بطاقات الائتمان والخصم، والتي توفر طبقة إضافية من الأمان مقارنة بالبطاقات التقليدية ذات الشريط المُمغنط. بالإضافة إلى ذلك، قد تطلب الحكومات من الشركات الامتثال لمعايير محددة لأمن البيانات لمنع اختراق البيانات، والتي يمكن أن تؤدي إلى معاملات احتيالية (SEON, 2023).

تتعاون بعض الحكومات أيضاً مع المؤسسات المالية وشركات بطاقات الائتمان لتنفيذ أدوات الكشف عن الاحتيال والوقاية منه. تستخدم هذه الأدوات الخوارزميات وتعلّم الآلة لتحليل المعاملات وكشف الأنماط غير العادية التي قد تشير إلى نشاط احتيالي. في بعض الحالات، قد تقدّم المؤسسات المالية أيضاً ميزات أمان إضافية، مثل التنبيهات للمعاملات المشبوهة أو القدرة على تجميد البطاقة في حالة فقدها أو سرقتها.

توفر بعض الحكومات حملات تثقيفية وتوعوية لمساعدة المستهلكين على حماية أنفسهم من الاحتيال على بطاقات الائتمان. قد تتضمن هذه الحملات نصائح حول التسوّق الآمن عبر شبكة المعلومات العالمية، ونصائح لحماية المعلومات الشخصية والمالية، وإرشادات لما ينبغي القيام به في حالة الاشتباه في الاحتيال.

بشكل عام، تلعب الحكومات دوراً هامّاً في حماية المستهلكين والشركات من الاحتيال على بطاقات الائتمان من خلال تنفيذ التشريعات، والشراكة مع المؤسسات المالية، وتعزيز التعليم والتوعية، والتعاون المحلي والدولي Wikipedia (2022, March 16). يمكن تقليل المخاطر المرتبطة بالاحتيال على بطاقات الائتمان وضمان نظام مالي أكثر أماناً نعرض فيما يلي أهم الأنشطة الاحترازية المقترحة:

- سن قوانين لحماية المستهلك المتعلقة بالاحتيال على البطاقات الإئتمانية.
- إجراء فحوصات منتظمة وتقييمات للمخاطر لمصدري بطاقات الائتمان.
- نشر المعايير والمبادئ الإرشادية والتوجيهية لحماية معلومات حامل البطاقة ومراقبة النشاط الاحتيالي.
- إعداد ونشر اللوائح التنظيمية وتحديثها بصفة مستمرة.
- الاستفادة من مزايا وتطبيقات التقنيات الحديثة كالذكاء الاصطناعي والبيانات الضخمة في بناء أنظمة إنذار حديثة ومتطورة ومحدّثة بصفة دورية.
- سن وتحديث قوانين ولوائح واضحة تعالج الاحتيال على بطاقات الائتمان وتفرض عقوبات صارمة على المحتالين.
- إنشاء نظام مركزي للإبلاغ عن حالات الاحتيال المتعلقة ببطاقات الائتمان والتحقيق فيها.
- تنفيذ بروتوكولات فعّالة للتحقق من الهوية للمعاملات عبر شبكة المعلومات العالمية لتقليل مخاطر انتحال الهوية.

2.2.3. من قبل البنوك والمؤسسات المالية

تعتبر البنوك والمؤسسات المالية الهدف الرئيس للاحتيال على بطاقات الائتمان، حيث إنها مسؤولة عن معالجة المعاملات والموافقة عليها. لحماية عملائها وأعمالهم، نفّذت العديد من البنوك والمؤسسات المالية تدابير احترازية مختلفة للحد من مخاطر الاحتيال على بطاقات الائتمان. تم تصميم هذه الإجراءات لمنع الوصول غير المصرح به إلى المعلومات الحساسة، وكشف ومنع المعاملات الاحتيالية وتوفير ميزات أمان إضافية لعملائها.

يمكن للبنوك والمؤسسات المالية تقليل مخاطر الأنشطة الاحتيالية، من خلال اتخاذ تدابير استباقية، وحماية المعلومات الشخصية والمالية لعملائها، والحفاظ على ثقة عملائها. تتضمن بعض الإجراءات الاحترازية التي تستخدمها البنوك والمؤسسات المالية والأكثر شيوعاً للحد من الاحتيال على بطاقات الائتمان ما يلي:

أ. **تنفيذ إجراءات قوية لأمن البيانات:** يمكن للبنوك والمؤسسات المالية وضع تدابير صارمة لأمن البيانات مثل التشفير والتخزين الآمن لحماية المعلومات الحساسة من الوصول غير المصرح به.

ب. **استخدام أدوات الكشف عن الاحتيال والوقاية منه:** ينبغي على البنوك والمؤسسات المالية استخدام أدوات متطورة للكشف عن الاحتيال والوقاية منه، مثل تعلّم الآلة والذكاء الاصطناعي، لمراقبة المعاملات في الوقت الفعلي وكشف الأنشطة المشبوهة.

ت. **توفير تنبيهات للعملاء:** يمكن للبنوك والمؤسسات المالية تقديم تنبيهات لعملائها، مثل إشعارات الرسائل النصية أو البريد الإلكتروني، لتنبيههم بالمعاملات المشبوهة أو الاحتيال المحتمل.

ث. **توفير الحماية من الاحتيال:** يمكن للبنوك والمؤسسات المالية توفير الحماية من الاحتيال لعملائها من خلال تعويضهم عن المعاملات غير المصرح بها وتزويدهم بفريق دعم عملاء مخصص لمساعدتهم في تجاوز التحديات التعلقة بالاحتيال.

ج. **تثقيف العملاء:** ينبغي على البنوك والمؤسسات المالية تزويد عملائها بالموارد التعليمية والإرشادات حول كيفية حماية أنفسهم من الاحتيال، مثل المشورة بشأن إنشاء كلمات مرور قوية واليقظة بشأن رسائل البريد الإلكتروني أو المكالمات الهاتفية المشبوهة.

يلعب مصدرو البطاقات بشكل عام دوراً هامّاً في حماية عملائهم من الاحتيال على بطاقات الائتمان، ومن خلال تنفيذ هذه الإجراءات الاحترازية وغيرها ، يمكن لمصدري البطاقات تقديم خدمة مالية آمنة وموثوقة تلبي احتياجات عملائهم مع حمايتهم من الأنشطة الاحتيالية. كما ينبغي ينبغي على مصدري البطاقات الإئتمانية تبني سياسات احترازية للكشف عن الاحتيال والوقاية منه، من خلال تحليل السلوك الطبيعي وغير الطبيعي للمعاملات الفردية من أجل التنبؤ بالاحتيال المحتمل، بالاعتماد على الملفات والمعلومات التعرفية. من بين السياسات الاحترازية لمصدري البطاقات Wikipedia (2022, March 16) نذكر ما يلي:

- الاتصال بحامل البطاقة لغرض التحقق.
- وضع ضوابط وقائية على الحسابات التي قد تكون مستهدفة.
- إيقاف البطاقة حتى يتم التحقق من المعاملات من قبل حامل البطاقة.
- التحقيق في الأنشطة الاحتيالية.
- التعاون وتبادل المعلومات حول المحتالين المعروفين ونواقل التهديدات الناشئة.

3.2.3. من قبل التجار ومستلمي المدفوعات

توجد العديد من الإجراءات الاحترازية التي يمكن للتجار ومستلمي المدفوعات اتخاذها لتجنب الاحتيال بالبطاقات المصرفية. بعض هذه التدابير تشمل:

أ. **استخدام نظام دفع آمن:** ينبغي على التجار ومستلمي الدفع استخدام أنظمة دفع آمنة مصممة للحماية من الاحتيال. ينبغي أن تستخدم هذه الأنظمة التشفير والتدابير الأمنية الأخرى لمنع المتسللين من اعتراض المعلومات الحساسة.

ب. **التحقق من هوية حامل البطاقة:** ينبغي على التجار ومستلمي الدفع التحقق من هوية حامل البطاقة قبل إتمام المعاملة. يمكن القيام بذلك عن طريق طلب التعريف أو مطالبة حامل البطاقة بإدخال رقم التعريف الشخصي.

ت. **استخدام أدوات الكشف عن الاحتيال:** ينبغي على التجار ومستلمي الدفع استخدام أدوات الكشف عن الاحتيال لتحديد المعاملات المشبوهة. يمكن لهذه الأدوات وضع علامة على المعاملات التي تقع خارج النمط الطبيعي لسلوك حامل البطاقة، مثل المعاملات في مواقع مختلفة أو لمبالغ كبيرة بشكل غير عادي.

ث. **مراقبة المعاملات:** ينبغي على التجار ومستلمي المدفوعات مراقبة معاملاتهم بانتظام لتحديد أي نشاط مشبوه. ينبغي عليهم أيضًا التحقق من بياناتهم المصرفية بانتظام للتأكد من أن جميع المعاملات مشروعة.

ج. **تدريب الموظفين:** ينبغي على التجار ومتلقي المدفوعات تدريب موظفيهم على التعرف على الاحتيال ومنعه. ينبغي تدريب الموظفين على كيفية التحقق من هوية حامل البطاقة، وكيفية استخدام أدوات الكشف عن الاحتيال، وكيفية الإبلاغ عن أي نشاط مشبوه.

ح. **الاحتفاظ بالسجلات:** ينبغي على التجار ومستلمي المدفوعات الاحتفاظ بسجلات لجميع المعاملات، بما في ذلك هوية حامل البطاقة وأي معلومات أخرى ذات صلة.

خ. **تأمين المعدّات الخاصة بهم:** ينبغي على التجار ومستلمي الدفع تأمين معدات الدفع الخاصة بهم ، مثل قارئات البطاقات وأجهزة الكمبيوتر، لمنع الوصول غير المصرح به. يمكن أن يشمل ذلك استخدام كلمات مرور قوية وبرامج الحماية من الفيروسات.

باتباع الإجراءات الاحترازية، يمكن للتجار ومستلمي الدفع المساعدة في منع الاحتيال على البطاقة المصرفية وحماية أنفسهم وعملائهم من الخسائر المالية، بالإضافة لما سبق يمكن تبني الإجراءات الاحترازية التالية:

- عدم عرض رقم الحساب الأساسي الكامل على الإيصالات (PAN truncation).
- الترميز واستخدام رمز مميز لرقم البطاقة بدلاً من الرقم الحقيقي للبطاقة.
- طلب معلومات إضافية، مثل رقم التعريف الشخصي، أو الرمز البريدي، أو رمز أمان البطاقة.
- إجراء التحقق من تحديد الموقع الجغرافي، مثل عنوان (Postal Index Number "PIN").
- استخدام مصادقة الاعتماد Wikipedia (2022, March 16).

4.2.3. من قبل حاملي البطاقات

يعتبر حاملو بطاقات الائتمان المستهدف الأساس في عمليات الاحتيال على بطاقات الائتمان، حيث يمكن للمحتالين استخدام معلوماتهم الشخصية والمالية لإجراء عمليات شراء غير مصرح بها أو سرقة هويتهم.

لحماية أنفسهم من الاحتيال على بطاقات الائتمان ، ينبغي على حاملي البطاقات اتخاذ تدابير احترازية مختلفة لحماية معلوماتهم وتقليل مخاطر المعاملات غير المصرح بها. تم تصميم العديد من الإجراءات لمنع الوصول غير المصرح به إلى المعلومات الحساسة، وكشف النشاط الاحتيالي والإبلاغ عنه، وتحسين أمن البيانات. كما أن اتخاذ تدابير استباقية، يمكن لحاملي البطاقات تقليل مخاطر الأنشطة الاحتيالية، وحماية معلوماتهم الشخصية والمالية، والحفاظ على ثقة مؤسساتهم المالية. تتضمن بعض الإجراءات الاحترازية الأكثر التي يمكن لحاملي البطاقات اتخاذها للحد من الاحتيال على بطاقات الائتمان ما يلي:

أ. **حماية المعلومات الحساسة:** ينبغي على حاملي البطاقات حماية معلومات بطاقة الائتمان الخاصة بهم، مثل رقم البطاقة وتاريخ انتهاء الصلاحية ورمز الأمان، من خلال عدم مشاركتها مع أي شخص وتخزينها في مكان آمن.

ب. **مراقبة المعاملات:** ينبغي على حاملي البطاقات مراقبة معاملات بطاقات الائتمان الخاصة بهم بانتظام من خلال التحقق من نشاط حساباتهم عبر شبكة المعلومات العالمية أو عبر تطبيق جوال ومراجعة بياناتهم الشهرية بحثاً عن أي معاملات غير مصرح بها أو مشبوهة.

ت. **إعداد التنبيهات:** يمكن لحاملي البطاقات إعداد تنبيهات المعاملات، مثل إشعارات الرسائل النصية أو البريد الإلكتروني أو تطبيقات البنوك على الجوّال لتنبيههم بأي نشاط مشبوه أو غير عادي.

ث. **استخدام كلمات مرور قوية:** ينبغي على حاملي البطاقات استخدام كلمات مرور قوية وفريدة من نوعها لحساباتهم عبر شبكة المعلومات العالمية وتحديثها بصفة دورية.

ج. **توخي اليقظة:** ينبغي على حاملي البطاقات توخي الحذر بشأن الاحتيال المحتمل، مثل توخي الحذر من المكالمات الهاتفية المشبوهة أو رسائل البريد الإلكتروني التي تطلب معلومات بطاقة الائتمان الخاصة بهم والتحقق من وجود أجهزة القشط في أجهزة الصراف الآلي.

يؤدي حاملو بطاقات الائتمان دوراً مهماً في حماية أنفسهم من الاحتيال على بطاقات الائتمان من خلال تنفيذ هذه الإجراءات الاحترازية وغيرها، كما يمكنهم تقليل مخاطر الأنشطة الاحتيالية وحماية معلوماتهم الشخصية والمالية والحفاظ على ملف ائتماني سليم، من خلال ما يلي:

- الإبلاغ عن البطاقات المفقودة أو المسروقة للجهات المصدرة في أقرب وقت ممكن.
- مراجعة المدفوعات بانتظام والإبلاغ عن المعاملات غير المصرح بها على الفور.
- الاحتفاظ ببطاقة الائتمان في متناول يد حامل البطاقة في جميع الأوقات، خاصة في الأماكن العامّة كالمطاعم وسيارات الأجرة.
- تثبيت برنامج الحماية من الفيروسات على جهاز الحاسبوب الشخصي والهواتف الذكية.
- توخي الحذر عند استخدام بطاقات الائتمان لعمليات الشراء عبر شبكة المعلومات العالمية، خاصة على مواقع الويب غير الموثوق بها، والتأكد من أن الموقع يتمتع بسمعة طيبة.
- الاحتفاظ بسجل لأرقام الحسابات، وتواريخ انتهاء صلاحيتها، ورقم هاتف وعنوان كل شركة في مكان آمن Wikipedia (2022, March 16).
- عدم إرسال معلومات بطاقة الائتمان عن طريق البريد الإلكتروني غير المشفر.
- عدم الاحتفاظ الرمز السري للبطاقة مكتوباً على بطاقة الائتمان.
- عدم إرسال أرقام بطاقات الائتمان وغيرها من المعلومات عبر شبكة المعلومات العالمية.
- الاشتراك في تنبيهات المعاملات عند استخدام البطاقة.
- الإطلاع الواسع على مخططات التصيّد.

- الالتزام بالتعليمات الصادرة عن الجهات الرقابية والإشرافية، والمصارف، والجهات المصدرة للبطاقات الإئتمانية.
- وضع مبلغ كحد أقصى لاستخدام البطاقة بشكل دوري، واستخدام التنبيهات عن كل استخدام للبطاقة مع توخي الحذر عند السفر والتنقل، وأوقات الإجازة.
- استخدام التطبيق الخاصة بالبنك على الهاتف الجوّال لمتابعة المعاملات، ووضع سقف لقيمة المعاملات والسحب اليومي أوالأسبوعي، والشهري.

3.3. تطور حجم عمليات الاحتيال على البطاقات الإئتمانية على المستوى الدولي

عرفت عمليات الاحتيال على البطاقات الإئتمانية على المستوى العالمي نمواً متزايداً في السنوات الماضية سواء من حيث العدد أو الحجم. تكبّد مصدرو البطاقات والتجار ومتلقو المدفوعات من التجار، بالإضافة إلى معاملات البطاقات من أجهزة الصراف الآلي، خسائر احتيال إجمالية بلغت 32.34 مليار دولار أمريكي عام 2021، بزيادة قدرها 13.8 في المائة مقارنة بعام 2020. في الولايات المتحدة في عام 2021 ارتبطت خسائر الاحتيال البالغة 11.91 مليار دولار أمريكي بإجمالي حجم المعاملات بالبطاقات البنكية الذي بلغ 11.269 تريليون دولار أمريكي، نمت هذه العمليات الاحتيالية بنسبة 18.1 في المائة مقارنة بعام 2020 الذي بلغ فيه حجم الاحتيال 10.09 مليار دولار أمريكي مقابل إجمالي حجم التعاملات بالبطاقات البالغ 9.403 تريليون دولار أمريكي عام 2020 (Nilson, 2021).
تتركز 23.02 في المائة من حجم معاملات البطاقات العالمية في عام 2021 في الولايات المتحدة الأمريكية، كما أنها تتكبد ما قيمته 36.83 في المائة من الخسائر العالمية الناجمة عن الاحتيال على البطاقات الائتمانية. يرجع ارتفاع خسائر الاحتيال في الولايات المتحدة في عام 2021 إلى الارتفاع في حجم الشراء باستخدام بطاقات الائتمان البالغ نسبة 25.0 في المائة، بعد انخفاض بنسبة 8.8 في المائة في عام 2020 بالإضافة إلى النمو المستمر في معاملات البطاقة غير الموجودة (CNP)، والتي تكون أكثر عرضة للاحتيال. والشكل التالي يبرز تطور حجم الخسائر الناجمة عن الاحتيال على البطاقات الإئتمانية (Nilson, 2021).

الشكل (1): تطور تكلفة الاحتيال على البطاقات الإئتمانية على المستوى العالمي داخل وخارج الولايات المتحدة الأمريكية للفترة (2014-2021).

المصدر: (Nilson, 2021)

تشير التوقعات إلى وصول حجم صناعة بطاقات الدفع إلى 79.14 تريليون دولار أمريكي في عام 2030، مع خسائر احتيال تقدر بحوالي 49.32 مليار دولار أمريكي (6.23 سنت لكل 100 دولار أمريكي). كما أنه من المتوقع أن يبلغ الحجم الإجمالي لصناعة بطاقات الدفع في الولايات المتحدة 18.953 تريليون دولار أمريكي، مع خسائر احتيال تبلغ 17.00 مليار دولار أمريكي (8.97 سنت لكل 100 دولار أمريكي). على مدى السنوات العشر المقبلة، من المتوقع أن تبلغ خسائر صناعة البطاقات بسبب الاحتيال 408.50 مليار دولار أمريكي. يتحمّل المصدرون 65.40 في المائة من إجمالي الخسائر الناجمة عن الاحتيال في جميع أنحاء العالم في عام 2020، بينما يتكبد التجار ومقتنيو أجهزة الصراف الآلي والمستحوذون التجار نسبة 34.60 في المائة الأخرى. شهد الاحتيال على بطاقات الخصم زيادة في عام 2020. يُشار الآن إلى الاحتيال الودي باسم "إساءة استخدام الطرف الأول" للبطاقة، مما يعكس الوعي المتزايد بأن الادعاءات الاحتيالية تنطوي على نية وتتجاوز التحديات الرقمية، حيث استغل بعض المستهلكون وسائل الحماية في المسؤولية ضد الاحتيال، كما أن صناعة بطاقات الدفع لم تجعل بعد إساءة استخدام الطرف الأول فئة رسمية للاحتيال، ولكنها تتحرك في هذا الاتجاه. لا تزال هجمات الهندسة الاجتماعية على المستهلكين التي تهدف إلى الحصول على معلومات التعريف الشخصية (PII) والاحتيال الاصطناعي تحديات كبيرة كذلك (Nilson, 2021). نعرض الجدول التالي الذي يبرز نمو حجم الخسائر الناجمة عن الاحتيال على البطاقة الإئتمانية المتوقع حتى عام 2030:

الجدول (1): حجم خسائر الاحتيال على البطاقة الإئتمانية والمتوقع حتى عام 2030

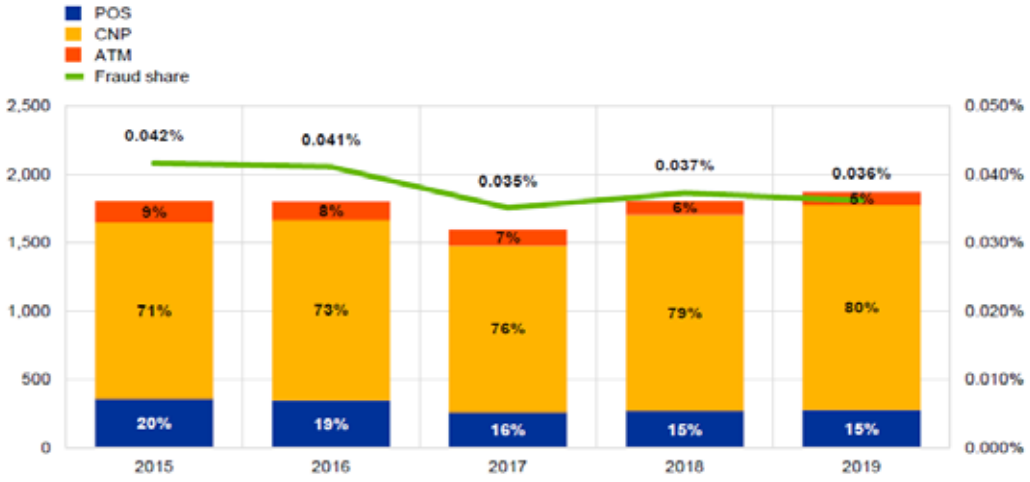
الخسائر بالسنت لكل $100	خسائر الإحتيال (مليون)	حجم الصفقات للبطاقات الإئتمانية (ترليون)	السنوات
6.81	$28.58	$41.962	2020
6.82	$32.20	$47.229	2021
6.75	$34.36	$50.868	2022
6.68	**$36.13**	**$54.061**	**2023**
6.64	$38.07	$57.323	2024
6.58	$39.89	$60.583	2025
6.52	$41.73	$64.038	2026
6.48	$43.76	$67.570	2027
6.39	$45.54	$71.221	2028
6.32	$47.50	$75.111	2029
6.23	$49.32	$79.140	2030

المصدر: (Nilson, 2021).

على مستوى دول الاتحاد الأوربي، بلغت القيمة الإجمالية للمعاملات باستخدام البطاقات الصادرة في منطقة منطقة المدفوعات اليورو الموحدة (SEPA[4]) 5.16 ترليون يورو في عام 2019، منها 1.87 مليار يورو خسائر ناجمة عن العمليات الاحتيالية على البطاقات الإئتمانية (ECB, 2021)، والشكل التالي يبرز ذلك.

[4] SEPA: The Single Euro Payments Area.

الشكل (2): تطور خسائر ناجمة عن العمليات الاحتيالية على البطاقات الإئتمانية الصادرة داخل منطقة (SEPA) خلال الفترة 2015-2019



المصدر: (ECB, 2021).

ارتفعت قيمة الخسائر الناجمة عن العمليات الاحتيالية على البطاقات الإئتمانية في منطقة النظام الموحد للمدفوعات الأوربية (SEPA) في عام 2019 بنسبة 3.4 في المائة مقارنة بعام 2018، في حين نمت قيمة حجم معاملات البطاقة الإئتمانية الإجمالية بنسبة 6.5 في المائة. وبالتالي نمت قيمة المعاملات الإجمالية للبطاقات بشكل أسرع من الخسائر الناجمة عن الاحتيال، مما أدى إلى انخفاض طفيف في الاحتيال كحصة من القيمة الإجمالية للمعاملات التي انتقلت من 0.037 في المائة في 2018 إلى 0.036 في المائة في 2019. سجلت خسائر الاحتيال أدنى مستوى في عام 2017 (0.035 في المائة). تظل أرقام 2018 و 2019 أقل بشكل ملحوظ من أعلى مستوى لها في خمس سنوات في عام 2015 (0.042 في المائة). من منظور أوسع على مدى السنوات العشر الماضية، ازداد الاحتيال على البطاقات الإئتمانية من الناحيتين المطلقة والنسبية حتى منتصف العقد، لكنه أظهر تحسينات كبيرة من الناحية النسبية في السنوات الأخيرة (ECB, 2021).

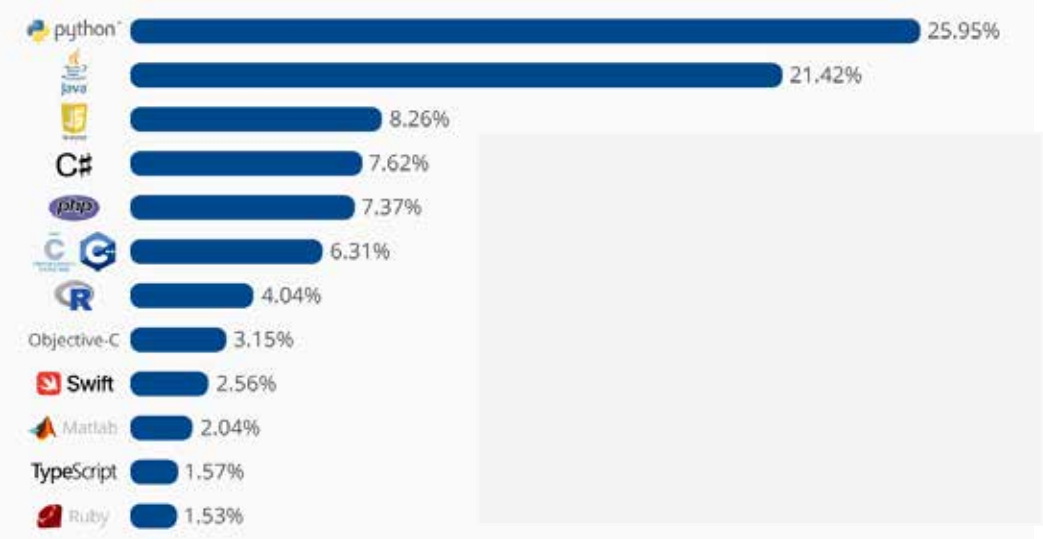
تستمر أهمية الاحتيال في الاحتيال بدون وجود بدون بطاقة (CNP) في الزيادة، حيث تمثل 80 في المائة من إجمالي قيمة الخسائر الناجمة عن العمليات الاحتيالية على البطاقات الإئتمانية في عام 2019. وفي المقابل، انخفضت نسبة الاحتيال في أجهزة الصراف الآلي ومحطات نقاط البيع إلى 5 في المائة و 15 في المائة من إجمالي قيمة الاحتيال على التوالي (ECB, 2021).

4.3. طرق الكشف عن الاحتيال على البطاقات الإئتمانية في ظل التقنيات الحديثة

يمتاز الاحتيال على بطاقات الائتمان بصعوبة كبيرة في كشفه خاصة في ظل البيانات الضخمة والتطور التقني الكبير الذي تشهده المعاملات المالية، مما يقلل من فعالية الطرق التقليدية، لذلك تم تطوير استخدامات الذكاء الاصطناعي من أجل جعل الآلات تحاول القيام بمهام نيابة عن الأفراد، ونظراً للتقدم في الذكاء الاصطناعي، لذلك توجد العديد من الطرق المقترحة للكشف عن الاحتيال على بطاقات الائتمان (Delamaire et al., 2009) بما في ذلك خوارزميات استقراء القواعد، وشجرة القرار، والشبكات العصبية، وآلات ناقلات الدعم، والانحدار اللوجستي، والاستدلال الفوقي. يواجه كشف الاحتيال على بطاقة الائتمان من باستخدام الذكاء الاصطناعي وتعلّم الآلة بعض التحديات مثل التصنيفات الخاطئة، وكذلك الكشف عن الاحتيال على بطاقة ائتمان ذات حد متاح أكبر.

تتمثل أشهر لغات البرمجة المستخدمة في الذكاء الاصطناعي وتعلّم الآلة في (Python)، و(Java). يعتبر (Python) أحد لغات البرمجة الأكثر استخداما على مستوى العالم، نعرض الشكل التالي الذي يبرز ذلك:

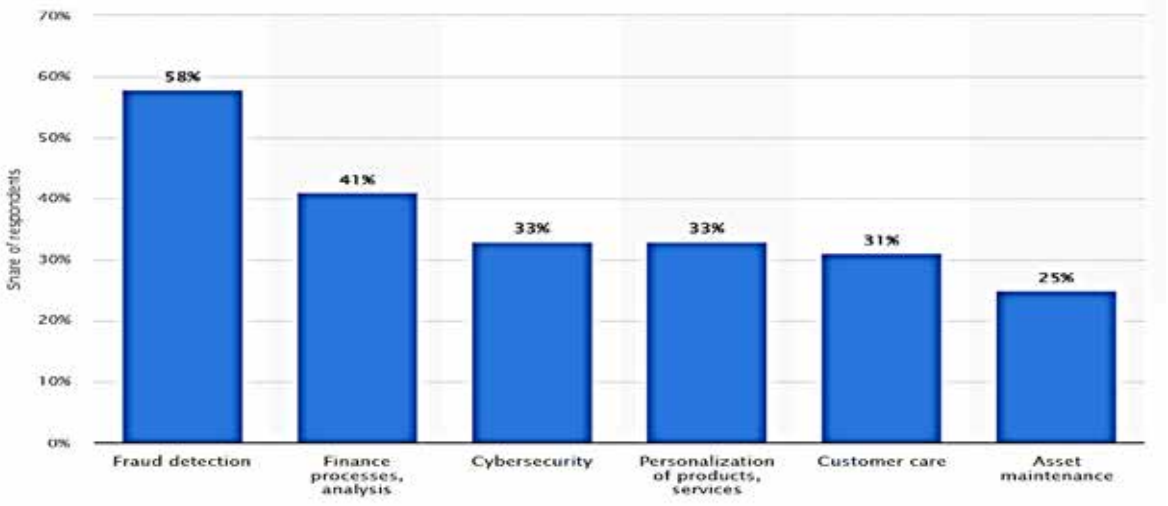
الشكل(3): أشهر لغات البرمجة استخداماً بشكل عام في العالم في عام 2022



Source: https://www.statista.com/chart/16567/popular-programming-languages/ (16/03/2023)

تشير العديد من الدراسات إلى أهمية استخدام تقنيات الذكاء الاصطناعي في الكشف عن الاحتيال على بطاقة الائتمان، ووفقا لنتائج الاستبيان الذي أجراه موقع (statista)، على استخدام الذكاء الاصطناعي في صناعة الخدمات المالية، ذكر معظم المستجيبين أن التحسينات في الكشف عن الاحتيال هي الأكثر استخداماً للذكاء الاصطناعي نسبة 58 في المائة، والشكل التالي يبرز ذلك.

الشكل(4): استخدامات الذكاء الاصطناعي في صناعة الخدمات المالية على مستوى العالم في عام 2020



Source: https://www.statista.com/statistics/1197955/ai-financial-services-global/ (16/03/2023)

يعمل الذكاء الاصطناعي على تحسين طرق كشف الاحتيال على بطاقات الإئتمان من خلال عدة أوجه لتعلّم الآلة، سواء عن طريق التعلم الخاضع الإشراف أو غير الخاضع للإشراف، والتعلم العميق، بالإضافة

إلى التعلم المعزّز وفهم اللغة الطبيعية بهدف اكتساب فهم سلوك العملاء، حيث يسمح الفهم الأفضل لسلوكيات العملاء للمؤسسات بتحديد ومنع النشاط الاحتيالي بشكل أفضل (Gangwar, & Ravi. 2019).

يتمثل أحد الأساليب الشائعة في استخدام أساليب تعلّم الآلة غير الخاضعة للإشراف، مثل خوارزميات التجميع و/أو التصنيف للكشف عن التشوهات، ولتحديد الأنماط في البيانات التي تنحرف عن القاعدة. يمكن بعد ذلك استخدام هذه الأنماط لتحويل المعاملات للمراجعة اليدوية أو لرفض المعاملات التي يُحتمل أن تكون احتيالية تلقائياً. يوجد نهج آخر يتمثل في استخدام أساليب تعلّم الآلة الخاضعة للإشراف، مثل شجرة القرار أو الشبكات العصبية، لتصنيف المعاملات على أنها احتيالية أو غير احتيالية بناءً على البيانات التاريخية. يمكن تدريب هذه الأساليب على البيانات الضخمة، ويمكن أن توفر دقة عالية في كشف الاحتيال (Gangwar, & Ravi. 2019).

عند التطرق إلى الصعوبات التي تواجه كشف الاحتيال على بطاقات الائتمان (Kulatilleke, 2022)، خاصة في ظل التقدم الحاصل في التعلم والتقنيات الحديثة كل يوم، لا تقبل العديد من الشركات مشاركة خوارزمياتها وتقنياتها. بالإضافة إلى ذلك، لا تمثل معاملات الاحتيال سوى ما نسبته بين 0.01-0.05 في المائة من المعاملات اليومية على الرغم من أهمية الخسائر كمبلغ، مما يجعل كشفها أكثر صعوبة. في هذا الإطار يمثل تعلّم الآلة مجالاً فرعياً للذكاء الاصطناعي، ويكمن الهدف منه في العثور على نموذج قائم على الخوارزميات ويُنتج مستوى أعلى من الدقة في التنبؤ.

4. الدراسة التطبيقية لكشف الاحتيال على البطاقة باستخدام خوارزميات تعلّم الآلة الخاضع للإشراف

يمكن استخدام خوارزميات تعلّم الآلة للكشف عن الاحتيال على بطاقة الائتمان من خلال تدريب نموذج على البيانات التاريخية للمعاملات الاحتيالية وغير الاحتيالية. يمكن بعد ذلك استخدام النموذج لكشف السلوك غير المعتاد في المعاملات الجديدة، مثل أنماط الإنفاق غير العادية أو المعاملات من مواقع غير معروفة، كما يمكن استخدام هذه التوقعات للإشارة إلى المعاملات للمراجعة أو لرفض وإيقاف المعاملات التي يُحتمل أن تكون احتيالية تلقائيًا. تتضمن بعض خوارزميات تعلّم الآلة الشائعة المستخدمة لهذا في هذا المجال الإنحدار اللوجستي، شجرة القرار، الغابة العشوائية والشبكات العصبية وغيرها.

1.4.بيانات الدراسة

تعتبر البيانات الخاصة بالاحتيال أحد البيانات الحسّاسة في القطاع المصرفي، وعلى الرغم من وجود بعض البيانات المنشورة، مثل البيانات الخاصة بالمعاملات التي أجراها حاملو البطاقات الأوروبيون على مدار يومين في سبتمبر 2013، والبالغة 284807 معاملة، منها 492 حالة احتيال، وتم إخفاء هوية مجموعة البيانات لأسباب تتعلق بالخصوصية، ولم يتم توفير أسماء المتغيرات ولا طبيعتها، ما يجعلها لا تعطي التصور والنظرة الثاقبة لسلوك النموذج والتفسير المالي والاقتصادي للنتائج. كما أن مجموعة البيانات تعاني من تحدّي معروف باسم "عدم توازن الفئة"، حيث تميل البيانات نحو فئة واحدة (في هذه الحالة ينتمي أكثر من 99 في المائة من البيانات إلى فئة الأغلبية). وتستخدم عدة طرق لمحاولة التغلب على هذا التحدي (Salekshahrezaee, et al, 2023)، من بينها إنشاء بيانات اصطناعية والمحاكاة وغيرها من الطرق.

لذلك، بغية تحقيق أهداف الدراسة المتمثلة في إبراز خوارزميات تعلّم الآلة، تم الاعتماد على بيانات إصطناعية (Synthetic Data)، حيث استخدمت بعض الدراسات البيانات الاصناعية (Kaur & Gosain, 2018). تم في دراستنا هذه الاعتماد على المحاكاة وإنشاء الأرقام العشوائية[5] ، لعينة عشوائية

[5] For more detail see: Alamri & Ykhlef, (2022).

تشمل 200000 معاملة، ولكل معاملة خصائص مختلفة تتمحور حول 20 عاملا من العوامل المفسرة، وتم اختيارها على سبيل الذكر لا الحصر، وهي معروضة في الجدول التالي:

الجدول (2): متغيرات الدراسة ورموزها

المتغير	رمز المتغير في الدراسة	المتغير	رمز المتغير في الدراسة
العمر	AGE	طبيعة الفرد (أنثى/ذكر)	MALFAMEL
الراتب السنوي	ANNUAL_SLAR	الحالة الاجتماعية (متزوج أعزب)	MARR
استخدام تطبيق البنك	BANKAPPUSE	الحد الأقصى للبطاقة الائتمانية	MAXCREDIT
نوع البطاقة الائتمانية	CARDTYPES	عدد الحسابات في بنوك مختلفة	NBANKS
عدد الأولاد	CHIN	عدد البطاقات الائتمانية	NCARD
نوع البريد الإلكتروني	EMAILTYPE	عدد الصفقات الدولية	NINTERTRANS
الثقافة المالية	FINLITERACY	عدد مرات التأخر عن السداد	NONLPY
امتلاك مسكن	HOME	عدد مرات تغيير الجوال	PHONECHA
نوع المهنة	JOBTYPE	مكان الإقامة	STATE
حجم القرض	LONVOL	المستوى التعليمي	STUDYLEV

المصدر: الباحث.

توفّرالعديد من البرامج بما في ذلك (Excel) دوال مختلفة لتوليد أرقام عشوائية، نعرض فيما يلي بعض الدوال شائعة الاستخدام لإنشاء أرقام عشوائية على (Excel):

الدالة (RAND): تُنشئ هذه الدالة عددًا عشريًا عشوائيًا بين 0 و 1. في كل مرة يتم فيها إعادة حساب ورقة العمل، يتم إنشاء رقم عشوائي جديد، ولإنشاء أرقام عشوائية نختار أي خانة ونكتب: "RAND () ="

الدالة (RANDBETWEEN): تُنشئ هذه الدالة عددًا صحيحًا عشوائيًا بين الحد الأدنى والحد الأقصى للقيمة المحددة. فعلى سبيل المثال : "RANDBETWEEN=(100 ,1)"

الدالة (RANDARRAY): تقوم هذه الدالة بإنشاء صفيف (Array) من الأرقام العشرية العشوائية بين 0 و1، وعلى سبيل المثال: "RANDARRAY = (3 ,5) "

إنشاء أرقام عشوائية ذات الحدين، يمكن استخدام الدالة (BINOM.DIST.RANGE) لحساب دالة الكتلة الاحتمالية للتوزيع ذي الحدين، مما يسمح بإنشاء نطاق من الأرقام العشوائية ذات الحدين بناءً على معلمات محددة. يكون بناء الدالة كما يلي: "=BINOM.DIST.RANGE(A1:B1, C1, D1, FALSE) " كما يمكن استخدام "=BINOM.INV(1, 0.1, RAND()) " لإنشاء أرقام عشوائية ثنائية الحد بنسبة 10 في المائة للرقم 1، و90 في المائة للرقم 0.

تجدر الإشارة على أنه من المهم معرفة أن قيم هذه الدوال سيتم إعادة حسابها في كل مرة يتم فيها إعادة فتح أي خانة في ورقة العمل، مما قد ينتج عنه أرقام عشوائية مختلفة، وعند الحاجة إلى إنشاء مجموعة من الأرقام العشوائية التي تظل ثابتة، فيمكنك نسخ ولصق القيم المُنشأة كقيم ثابتة.

بالإضافة إلى ذلك، عند الحاجة إلى إنشاء أرقام عشوائية أكثر تقدمًا أو محددًا ، فيمكن التفكير في استخدام إمكانات البرمجة VBA (Visual Basic for Applications) من (Excel) لإنشاء دوال مخصصة أو وحدات ماكرو لإنشاء أرقام عشوائية بمزيد من المرونة والتحكم.

2.4. منهجية الدراسة وأهم خوارزميات تعلّم الآلة المستخدمة

يُمثل تعلّم الآلة مجموعة فرعية من الذكاء الاصطناعي، يركّز على تطوير الخوارزميات والنماذج التي يمكن أن تتعلم من البيانات وتقوم بالتنبؤات أو القرارات دون أن تتم برمجتها بشكل صريح. يتضمن تدريب النموذج على مجموعة بيانات معنونة واستخدامها لعمل تنبؤات بشأن بيانات جديدة غير مرئية[6]. يوجد هناك نوعين رئيسين من تعلّم الآلة: التعلم الخاضع للإشراف والتعلم غير الخاضع للإشراف (Tatsat, 2020).

يُعد التعلّم غير الخاضع للإشراف نوعاً من تعلّم الآلة، حيث يتم تدريب النموذج على البيانات غير المسمّاة، مما يعني أن البيانات تتضمن فقط ميزات الإدخال دون أي قيم أو تسميات مستهدفة. يهدف التعلّم غير الخاضع للإشراف إلى كشف الأنماط أو بنية البيانات دون أي معرفة مسبقة بالتسميات. تتضمن أمثلة خوارزميات التعلم غير الخاضعة للإشراف التجميع، وتقليل الأبعاد، وكشف الحالات الشاذّة .من ناحية أخرى، يعتبر التعلّم الخاضع للإشراف أحد أنواع تعلّم الآلة، حيث يتم تدريب النموذج على البيانات المصنفة، مما يعني أن البيانات تتضمن ميزات الإدخال وتسميات الإخراج الصحيحة أو القيم المستهدفة. الهدف من التعلم الخاضع للإشراف هو تعلّم رسم الخرائط بين ميزات الإدخال وتسميات المخرجات، بحيث يمكن للنموذج التنبؤ بدقة بمخرجات البيانات الجديدة غير المرئية. وباختصار يُعد تعلّم الآلة أداة قوية للتحليل والتنبؤ بناءً على البيانات، يحتوي كلا النوعين من تعلّم الآلة على مجموعة واسعة من التطبيقات في مجالات مثل التمويل والرعاية الصحية والتسويق (Le Borgne, et al., 2021).

تتطلب خوارزميات تعلّم الآلة الخاضع للإشراف بيانات تدريب مصنفة، يهدف التعلم الخاضع للإشراف إلى تعلّم دالة (أو نموذج) يمكنها تعيين المدخلات إلى المخرجات المرغوبة، بناءً على الأمثلة الموجودة في بيانات التدريب، وهو محور الاهتمام في هذه الورقة، كما يوجد نوعين رئيسيين من التعلم الخاضع للإشراف وهما التصنيف والانحدار.

تُستخدم خوارزميات التصنيف للتنبؤ بالمخرجات الفئوية، مثل ما إذا كان البريد الإلكتروني بريدًا عشوائياً أم لا، أو نوع العنصر الموجود في الصورة، أو معاملة مالية على أنها احتيالية أم لا. تتضمن أمثلة خوارزميات التصنيف الانحدار اللوجستي، وشجرة القرار، وآلات ناقلات الدعم. بينما تُستخدم خوارزميات الانحدار للتنبؤ بالمخرجات المستمرة، مثل سعر السهم أو درجة الحرارة. تتضمن أمثلة خوارزميات الانحدار الانحدار الخطي والانحدار اللوجستي والغابة العشوائية. توجد أنواع أخرى من خوارزميات التعلم الخاضع للإشراف هي التنبؤ بالسلاسل الزمنية، وهي حالة محددة من التعلم الخاضع للإشراف والتي تستخدم للتنبؤ بالقيم المستقبلية لمتغير ما بناءً على القيّم التاريخية، من بين خوارزميات التنبؤ بالسلاسل الزمنية هي خوارزمية الذاكرة الطويلة والقصيرة (LSTM).

هناك مجموعة متنوعة من خوارزميات تعلّم الآلة الخاضعة للإشراف، ويتم تطويرها بصفة مستمرة تتضمن القائمة التالية أهم الخوارزميات المعروفة (Tatsat, 2020)، وهي:

- الانحدار اللوجستي (Logistic regression).
- التحليل التمييزي الخطي (Linear Discriminant Analysis).

[6] لمزيد من التفصيل أنظر : https://coursee.org/blog/artificial-intelligence/top-10-machine-learning-algorithms/

- أقرب الجيران ("k-NN " k-Nearest Neighbors).
- شجرة القرار (Decision Tree).
- الغابة العشوائية (Random forests).
- دعم آلات المتجهات (SVMs).
- تصنيف بايز(Bayesian classification).
- الشبكات العصبية (Neural networks).
- آلات تعزيز التدرج (GBM).
- تعزيز التدرج الشديد XGBoost .
- خوارزميات تعزيز التدرج القائمة على الأشجار(LightGBM).

لا تشمل هذه القائمة جميع الخوارزميات، بل توجد العديد من الخوارزميات الأخرى الموجودة والتي يجري تطويرها (Tatsat, 2020). يعتمد اختيار الخوارزمية على المسألة المُراد حلّها وخصائص البيانات والموارد المتاحة ومعايير أخرى سيتم عرضها في القسم الموالي.

نعرض فيما يلي بعض التفاصيل حول الخوارزميات الأربعة المستخدمة في الدراسة، مع الوقوف على مزايا وعيوب كل منها (Le Borgne, et al., 2021).

1.2.4. خوارزمية الانحدار اللوجستي

تمثّل خوارزمية الانحدار اللوجستي (LR) من بين خوارزميات تعلّم الآلة الخاضع للإشراف، تُستخدم لمهام التصنيف والانحدار، كما تهدف إلى التنبؤ باحتمالية أن ينتمي أحد المدخلات إلى فئة أو فئة معينة. يتم ذلك عن طريق استخدام دالة لوجستية (تسمى أيضاً الدالة السينية) لتعيين المدخلات إلى قيمة بين 0 و1، والتي يمكن تفسيرها على أنها احتمال أن ينتمي الإدخال إلى الفئة الإيجابية (Kulatilleke, 2022).
يتم تدريب خوارزمية الانحدار اللوجستي باستخدام البيانات المصنّفة، حيث يتم تعريف المدخلات والمخرجات المقابلة لها. تتعلم الخوارزمية من العلاقة بين المدخلات والمخرجات من خلال إيجاد أفضل مجموعة من المعلمات للدالّة اللوجستية. يتم اختيار هذه المعلمات لتعظيم احتمالية البيانات المرصودة في ضوء النموذج.
بمجرد تدريب خوارزمية نموذج الانحدار اللوجستي، يمكن استخدامه للتنبؤ باحتمالية وجود مدخلات جديدة تنتمي إلى الفئة الإيجابية. عادةً ما يتم اختيار قيمة العتبة (مثل 0.5) لتحويل الاحتمال المتوقع إلى تصنيف ثنائي. يتم تصنيف المدخلات ذات الاحتمالية الأكبر من الحد على أنها موجبة، ويتم تصنيف المدخلات ذات الاحتمالية الأقل من الحد على أنها سلبية.
يُستخدم الانحدار اللوجستي على نطاق واسع في العديد من مسائل التصنيف مثل تصنيف الصور ومعالجة اللغة الطبيعية والتشخيص الطبي، وكذلك في كشف الاحتيال، كما تعتبر خوارزمية بسيطة يسهل تنفيذها وتفسيرها، كما أنها لا تتطلب الكثير من القدرة الحسابية لتشغيلها.
من حيث المزايا، تعتبر خوارزمية الانحدار اللوجستي سهلة التنفيذ، ولها قابلية تفسير جيدة، وتعمل بشكل جيد للغاية في الفئات القابلة للفصل خطياً. يكمن لنتائج النموذج ان توفّر مزيداً من التشخيص. يحتوي النموذج على عدد قليل من المعلمات المستقلة، على الرغم من أنه قد يكون هناك خطر حدوث فرط في

التخصيص، إلا أنه قد تتم معالجة ذلك باستخدام بعض طرق فرط التخصيص لنماذج الانحدار الخطي. أما من حيث العُيوب، قد يكون النموذج متحّيزاً عند تزويده بعدد كبير من المتغيرات المستقلة، كما أن هذه الخوارزمية تتعامل فقط مع الدوال الخطية (بعد ادخال اللوغاريتم الطبيعي) وهي أقل ملاءمة للعلاقات المعقدة بين الميزات والمتغير المستهدف. أيضًا، قد لا تتعامل هذه الخوارزمية بشكل جيد مع المتغيرات المرتبطة ذاتياً، كما تقوم هذه الخوارزمية على البيانات لتقدير النموذج.

2.2.4. خوارزمية تحليل التمييز الخطي

تعتبر خوارزمية التحليل التمييزي الخطي (LDA) أحد خوارزميات تعلّم الآلة الخاضع للإشراف تُستخدم لمهام التصنيف، كما تعتبر تقنية لتقليل الأبعاد تقوم بإسقاط بيانات الإدخال على مساحة ذات أبعاد أقل مع الحفاظ على قابلية الفصل بين الفئات (Tatsat, 2020).

تفترض الخوارزمية أن البيانات يتم توزيعها بشكل طبيعي وأن الفئات لها نفس مصفوفة التباين المشترك. تعمل هذه الخوارزمية على إيجاد مجموعة خطية من الميزات التي تزيد من نسبة التباين بين الفئة إلى التباين داخل الفئة، وهو ما يدل على أن هذه الخوارزمية تعمل على إيجاد مجموعة خطية من الميزات التي تفصل بين الفئات قدر الإمكان مع تقليل التداخل بين الفئات. تبدأ هذه الخوارزمية بحساب المتجه المتوسط ومصفوفة التباين المشترك لكل فئة. ثم تقوم بحساب مصفوفة التشتت بين الفئة ومصفوفة التشتت داخل الفئة. يتم حساب المتجهات الذاتية للمصفوفة (معكوس مصفوفة التشتت داخل الصنف مضروبًا في مصفوفة تشتت بين الفئة) ، ويتم اختيار المتجهات الذاتية التي تتوافق مع أكبر قيم ذاتية (Eigenvalues) كمحاور جديدة للمساحة المسقطة. تساعد هذه الخوارزمية في الحفاظ على قابلية الفصل للفئة من خلال إسقاط البيانات في مساحة ذات أبعاد أقل. تعتبر هذه الخوارزمية جد مفيدة لاستخراج الميزات والتعرف على الوجوه وتصنيف النصوص. خوارزمية التحليل التمييزي الخطي مشابه لتحليل المكونات الرئيسية (PCA) ولكن على عكس تحليل المكونات الرئيسية، فإن تحليل التمييز الخطي يمثل تقنية خاضعة للإشراف، وتحاول تعظيم إمكانية فصل الفئة بينما يحاول تحليل المكونات الرئيسية تعظيم تباين البيانات.

من حيث المزايا، تعد خوارزمية تحليل التمييز الخطي نموذجاً بسيطاً نسبياً مع تنفيذ سريع وسهل التنفيذ، أما من حيث العيوب، فإنه يتطلب تحجيم الميزة (Standardization and Normalization) ويتضمن عمليات مصفوفاتية معقدة.

3.2.4. خوارزمية أقرب الجيران

تُعد خوارزمية أقرب الجيران (k-NN) أحد خوارزميات التعلم الخاضع للإشراف، تُستخدم لمهام التصنيف والانحدار. كما أنها طريقة غير بارامترية (Nonparametric) تقوم بالتنبؤات بناءً على فئة الأغلبية أو متوسط قيمة نقاط البيانات الأقرب في المساحة المختارة (Kulatilleke, 2022).

تبدأ الخوارزمية بحساب المسافة بين المدخلات الجديدة وجميع نقاط البيانات في مجموعة التدريب، باستخدام مقياس المسافة مثل المسافة الإقليدية، يتم اختيار نقاط البيانات الأقرب لمعلمة محددة (k) بناءً على المسافات، حيث k هي معلمة يحدّدها المستخدم. بالنسبة للتصنيف، يتم تعيين فئة الأغلبية بين أقرب نقاط بيانات k كفئة متوقعة للإدخال الجديد. بالنسبة للانحدار، يتم تعيين متوسط قيمة نقاط البيانات الأقرب لـ k كقيمة متوقعة للإدخال الجديد (Kulatilleke, 2022).

تمتاز خوارزمية أقرب الجيران بأنها سهلة التنفيذ والتفسير، ولا تتطلب الكثير من القدرة الحسابية لتشغيلها. كما إنها مفيدة لتطبيقات مثل تصنيف الصور وكشف الحالات الشاذّة وكذلك العمليات الاحتيالية. تتمثل إحدى

المزايا الرئيسية لها في قدرتها على التكيف مع البيانات الجديدة أثناء التدريب، نظراً لأن الخوارزمية تستخدم فقط بيانات التدريب للتنبؤ. ومع ذلك، يمكن أن يكون أداؤها حسّاساً لاختيار قياس المسافة وقيمة k. كما أنها لا تعمل بشكل جيد مع البيانات عالية الأبعاد (Tatsat, 2020)،لأن المسافة بين النقاط يمكن أن تصبح أقل أهمية.

من حيث المزايا، لا يوجد تدريب وبالتالي لا توجد مرحلة تعلم. نظراً لأن الخوارزمية لا تتطلب أي تدريب قبل إجراء التنبؤات، يمكن إضافة بيانات جديدة بسلاسة دون التأثير على دقة الخوارزمية. كما أنها بديهية وسهلة الفهم، وتتعامل بشكل طبيعي مع التصنيف متعدد الطبقات. كما أنها قوية للبيانات غير المنتظمة. أما من حيث العيوب، فإن اختيار مقياس المسافة ليس واضحاً ويصعب تبريره في كثير من الحالات. كما يعتبر أداء الخوارزمية ضعيفاً على مجموعات البيانات عالية الأبعاد. كما أن توقّع الحالات الجديدة أمر مكلف وبطيء لأنه ينبغي إعادة حساب المسافة إلى جميع الجيران. حيث الخوارزمية حساسة للقيم المفقودة في مجموعة البيانات، ونحتاج إلى إدخال القيم المفقودة يدويًا وإزالة القيم المتطرفة. أيضًا، مطلوب تحجيم البيانات (standardization and normalization) قبل تطبيق الخوارزمية على أي بيانات؛ خلاف ذلك، قد تولد الخوارزمية تنبؤات خاطئة.

4.2.4. خوارزمية شجرة القرار

تمثل خوارزمية شجرة القرار أحد خوارزميات تعلّم الآلة الخاضعة للإشراف، وتُستخدم لمهام التصنيف والانحدار. تتوافق كل عقدة داخلية في الشجرة مع ميزة أو سمة للبيانات، وكل عقدة طرفية تتوافق مع فئة أو قيمة (Kulatilleke, 2022).

تبدأ خوارزمية شجرة القرار بتحديد الميزة والعتبة التي تقسم البيانات بشكل أفضل إلى مجموعات فرعية ذات تسميات أو قيم فئة متشابهة. تتكرر العملية لكل مجموعة فرعية من البيانات، مما يؤدي إلى إنشاء بنية تشبه الشجرة. تعتبر الشجرة النهائية تمثيل هرمي لمساحة ميزة الإدخال، حيث يتوافق كل مسار من الجذر إلى عقدة طرفية مع مجموعة من القرارات التي تؤدي إلى تسمية فئة معينة أو قيمة.

يمكن تدريب خوارزمية شجرة القرار باستخدام تقنيات مختلفة مثل (ID3) و(C4.5)، و(C5.0). يتم استخدام (ID3) لإنشاء شجرة قرار من مجموعة ثابتة من المثيلات. يتم استخدام (C4.5)، و(C5.0) لإنشاء شجرة قرار من مجموعة ثابتة من الأمثلة، ولكنها تسمح أيضًا بتقليم الشجرة وإزالة الفروع التي لا توفر أي معلومات إضافية (Tatsat, 2020)..

تمتاز شجرة القرار بأنها سهلة الفهم والتفسير والتصوّر، ويمكنها التعامل مع كل من البيانات الفئوية والرقمية، وتعمل بشكل جيد مع مجموعات البيانات الكبيرة. لكنها معرضة للإفراط في التجهيز، خاصة عندما تكون الشجرة عميقة، ويمكن أن تصبح الشجرة معقدة للغاية بحيث لا يمكن تفسيرها بسهولة. يمكن معالجة هذه المشكلة باستخدام تقنيات مثل التقليم أو باستخدام طرق التجميع مثل الغابة العشوائية.

من حيث المزايا، يسهل تفسير شجرة القرار ويمكن أن تتكيّف لتعلم العلاقات المعقدة، كما يتطلب القليل من إعداد البيانات، وعادةً لا تحتاج البيانات إلى التحجيم. تم بناء أهمية الميزة نظرًا للطريقة التي يتم بها بناء عقد القرار. يعمل بشكل جيد على مجموعات البيانات الكبيرة. وهي تعمل مع كل من الانحدار والتصنيف. أما من حيث العيوب، تكون شجرة القرار عرضة للتركيب الزائد ما لم يتم استخدام تقنية التقليم، كما يمكن أن تكون غير قوية للغاية، مما يعني أن التغييرات الصغيرة في مجموعة بيانات التدريب يمكن أن تؤدي إلى اختلافات كبيرة جدًا في دالة الهدف التي يتم تدريبها. تتميز شجرة القرار عمومًا بأداء سيء مقارنة ببقية الخوارزميات.

5. نتائج الدراسة التطبيقة لكشف الاحتيال على البطاقات الإئتمانية

يعرض هذا القسم النتائج الخاصة بخوارزميات تعلّم الآلة. قبل مناقشة النتائج، نعمل على استكشاف البيانات قيد الدراسة مع عرض الإحصائيات الوصفية، إضافة إلى عرض الارتباط الخطي بين متغيرات الدراسة، وكذلك التوزيع الاحتمالي للمتغيرات قيد الدراسة.

1.5.التحليل الاستكشافي للبيانات

يعد تصور البيانات والتحليل الاستكشافي لها (data visualization) خطوة مهمة في إعداد البيانات لتعلّم الآلة، حيث يمكن أن تساعد هذه الخطوة في فهم البيانات وتحديد الأنماط والعلاقات التي يمكن أن تحسن دقة خوارزمية تعلّم الآلة. نعرض فيما يلي الخطوات الأساسية لتصور البيانات في سياق تعلّم الآلة الخاضع للإشراف (Tatsat, 2020).:

- **استيراد البيانات:** يتم استيراد مجموعة البيانات المراد استخدامها في خوارزمية تعلّم الآلة الخاضع للإشراف إلى أداة تحليل البيانات أو التصور المفضلة (يمكن استخدام مكتبات Python مثل Matplotlib أو Seaborn).
- **فهم البيانات:** قبل إنشاء أي تصورات، من المهم فهم البيانات التي نعمل عليها، بما يشمل ذلك فهم المتغيرات وأنواعها (مستمرة أو فئوية) وتوزيعاتها وأي علاقات بين المتغيرات.
- **استكشاف المتغير المُفسَّر:** من المهم استكشاف المتغير المستهدف (المتغير الذي نريد توقعه) لفهم توزيعه، وأي أنماط أو علاقات قد تكون له مع المتغيرات الأخرى.
- **استكشاف المتغير المفسِّر:** ينبغي استكشاف المتغير أو المتغيرات التي نستخدمها للتنبؤ بالمتغير المُفسَّر لفهم توزيعها الإحصائي وأي علاقات قد تكون لها مع بعضها البعض ومع المتغيرات المستقلة.
- **تصوّر التوزيعات:** يتم من خلال إنشاء تصورات مثل الرسوم البيانية، ومخططات الكثافة، ومخططات لتصور توزيعات كل متغير.
- **تصور العلاقات:** يتم من خلال إنشاء مخططات الانتشار وتصورات أخرى لاستكشاف العلاقة بين المتغيرات، لا سيما بين المتغير المُفسَّر والمتغيرات المفسِّرة.
- **تحديد القيم المتطرفة:** استخدم التصورات لتحديد أي قيم متطرفة أو قيم غير عادية في البيانات، حيث يمكن أن يكون لها تأثير كبير على نتائج نموذج تعلّم الآلة.
- **إنشاء مخططات أهمية المتغير:** بعد إنشاء نموذج تعلّم الآلة، يمكنك إنشاء تصورات لإظهار أهمية كل متغير مستقل في التنبؤ بالمتغير التابع.

نعرض فيما يلي خطوات تصور البيانات والتحليل الاستكشافي لها في سياق تعلّم الآلة الخاضع للإشراف باستخدام (Python):

2.5.استيراد المكتبات الضرورية لتحميل البيانات وتصور البيانات واستكشافها

يتطلب التصور والاستكشاف في البداية تحميل البيانات على برمجية (Python)، حيث نحتاج إلى استيراد بعض المكتبات الضرورية للتحميل والتصور والاستكشاف مثلاً: لتحميل البيانات نستخدم (Pandas DataFrame) وللتحليل والاستكشاف نستخدم (Matplotlib) و (Seaborn) و(Pandas).

أ. عرض البيانات الخام ومراجعة أبعاد مجموعة البيانات

نعرض الجدول التالي الذي يبرز طبيعة المتغيرات:

الجدول (3): نتائج استكشاف طبيعة متيغرات الدراسة

```
N                int64
Fraud            int64
MalFamel         int64
Emailtype        int64
Annual_slar    float64
State            int64
PhoneCha         int64
StudyLev         int64
Marr             int64
LonVol         float64
Home             int64
ChiN             int64
BankAppUse       int64
NInterTrans      int64
Jobtype          int64
Nbanks           int64
Maxcredit      float64
NCARD            int64
FinLiteracy      int64
NonlPy           int64
Age              int64
Cardtypes        int64
dtype: object
```

يظهر من خلال الجدول (3)، قائمة أسماء المتغيرات في العمود الأيسر وكذلك نوع البيانات في العمود الثاني، حيث أن جميع البيانات بأكملها صورية (تأخذ قيمة 0 أو1) أو فئوية داخل مجال محدد حيث يرمز لها بالرمز (int64)، باستثناء الدخل السنوي، حجم القرض، والحد الأقصى لبطاقة الائتمان التي تأخذ قيمهاعدداً صحيحاً، يرمز لها بالرمز (float64).

بعد الاطلاع على قائمة البيانات ونوعها، تبقى الحاجة إلى تجهيز البيانات، كالتصفية، واستبعاد القيم المفقودة أو استبدال النصوص بأرقام أو غيرها (Tatsat, 2020).

ب. الإحصائيات الوصفية

نعمل في البداية على تقديم الإحصائيات الوصفية لاستكشاف مجموعة البيانات والحصول على فهم أفضل للبيانات التي نعمل عليها باستخدم دوال مثل: (info.() و describe.() و head.()). سيساعد ذلك على فهم الخصائص الأساسية للبيانات، مثل عدد الملاحظات وعدد المتغيرات وأنواع المتغيرات والإحصائيات الموجزة. يلخص الجدولين (4) و(5) مختصر لبيانات الدراسة وللإحصائيات الوصفية للبيانات قيد الدراسة على التوالي. تعتبر هذه المرحلة جد مهمة خاصة على مستوى البيانات الضخمة، التي نحتاج فيها أخذ صورة مصغّرة عن البيانات بأكملها.

يبرز من الجدول (4) أن هناك أربعة متغيرات ذات أرقام حقيقية مستمرة، في حين بقية المتغيرات كلها صورية أو فئوية، وعدم وجود بيانات مفقودة في المختصر.

يبيّن الجدول (4) حجم العينة البالغ 200 ألف مشاهدة لجميع متغيرات قيد الدراسة، إضافة إلى أهم الإحصائيات الوصفية، ممثلة في المتوسط والإنحراف المعياري، أعلى وأدنى قيمة، إضافة إلى كل من الرُّبيع الأول والثاني والثالث. بلغ متوسط حالات الاحتيال على البطاقات 5.7 في المائة، وبانحراف معياري في حدود 23 في المائة.

الجدول(4): عرض مختصر لبيانات الدراسة

N	Fraud	MalFamel	Emailtype	Annual_slar	State	PhoneCha	StudyLev	Marr	LonVol	...	BankAppUse	NInterTrans	Jobtype	Nbanks	Maxcredit	NCARD	FinLiteracy	NonlPy	Age	Cardtypes
1	0	0	2	3094.584052	24	3	3	0	273.764643	...	0	2	3	0	203.142524	1	0	1	32	0
2	0	0	1	1951.660712	27	3	0	0	2115.651645	...	1	4	3	1	347.299234	0	0	0	22	1
3	0	0	2	3466.631755	38	1	3	1	1083.236240	...	0	4	3	0	332.907365	0	0	1	63	1
4	0	0	3	5867.670606	20	0	0	0	1805.424684	...	0	7	4	0	84.869680	0	0	1	47	1
5	0	0	1	2609.876522	25	1	1	0	1466.246246	...	1	8	4	0	115.442895	0	0	0	21	1
6	0	0	2	1235.340850	15	0	1	0	619.380048	...	0	6	3	1	409.951668	1	0	0	24	0
7	0	0	2	313.590222	40	3	0	0	1590.011791	...	0	10	1	1	107.078778	0	0	0	30	0
8	0	0	2	8148.779001	15	0	0	0	2128.071910	...	0	7	2	0	280.742049	0	0	0	56	1
9	0	0	3	7851.135392	37	2	2	0	293.411554	...	1	7	3	1	198.850689	0	0	1	36	1
10	0	0	0	7956.461586	51	2	2	0	2457.385592	...	0	8	4	1	187.310307	1	0	1	59	1

الجدول(5): الإحصاءات الوصفية لبيانات الدراسة

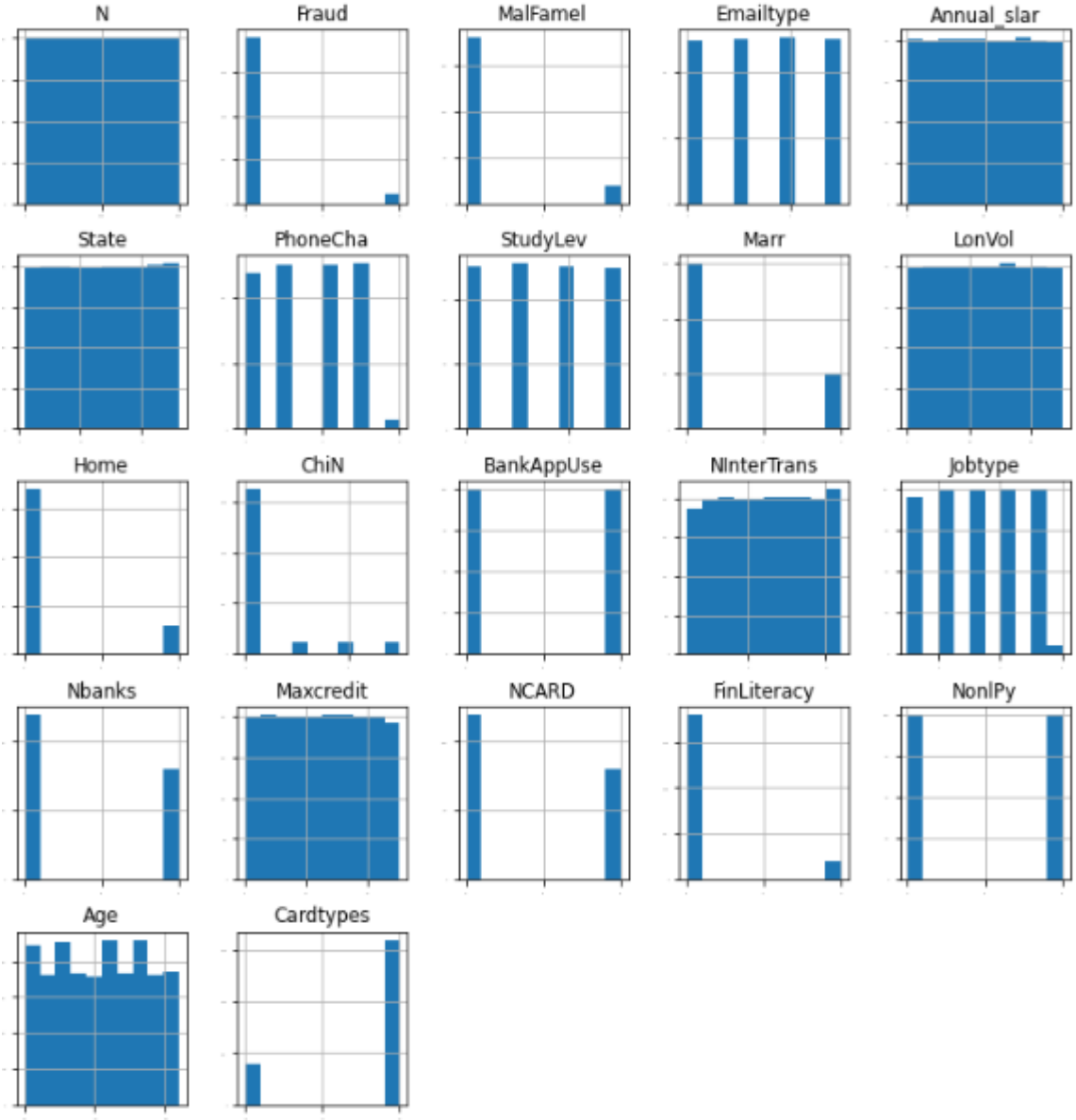
	N	Fraud	MalFamel	Emailtype	Annual_slar	State	PhoneCha	StudyLev	Marr	LonVol	...	BankAppUse	NInterTrans	Jobtype	Nbanks	Maxcredit	NCARD	FinLiteracy	NonlPy	Age	Cardtypes
count	200000.000	200000.000	200000.0	200000.000	200000.000	200000.000	200000.000	200000.000	200000.000	200000.000	...	200000.0	200000.000	200000.000	200000.000	200000.000	200000.000	200000.000	200000.000	200000.000	200000.0
mean	100000.500	0.057	0.1	1.503	4998.539	26.583	1.559	1.495	0.250	1251.461	...	0.5	5.567	3.055	0.401	253.432	0.401	0.100	0.501	41.627	0.8
std	57735.171	0.232	0.3	1.117	2884.682	14.458	1.143	1.115	0.433	720.867	...	0.5	2.877	1.434	0.490	144.359	0.490	0.299	0.500	12.693	0.4
min	1.000	0.000	0.0	0.000	0.038	2.000	0.000	0.000	0.000	0.040	...	0.0	1.000	1.000	0.000	3.000	0.000	0.000	0.000	20.000	0.0
25%	50000.750	0.000	0.0	1.000	2496.484	14.000	1.000	1.000	0.000	626.722	...	0.0	3.000	2.000	0.000	128.337	0.000	0.000	0.000	31.000	1.0
50%	100000.500	0.000	0.0	2.000	4998.243	27.000	2.000	1.000	0.000	1253.459	...	1.0	6.000	3.000	0.000	253.862	0.000	0.000	1.000	42.000	1.0
75%	150000.250	0.000	0.0	2.000	7497.297	39.000	3.000	2.000	1.000	1875.843	...	1.0	8.000	4.000	1.000	378.382	1.000	0.000	1.000	53.000	1.0
max	200000.000	1.000	1.0	3.000	10003.356	52.000	4.000	3.000	1.000	2501.825	...	1.0	11.000	6.000	1.000	505.970	1.000	1.000	1.000	64.000	1.0

8 rows × 22 columns

ت. تصور التوزيعات

نقوم بإنشاء تصورات مثل الرسوم البيانية ومخططات الكثافة ومخططات لتصور توزيعات كل متغير. يمكن استخدام (Matplotlib) أو (Seaborn) لإنشاء هذه الأنواع من التصورات.

الشكل (5): التوزيع الاحتمالي لمتغيرات الدراسة



المصدر: الباحث بالاعتماد على بيانات الدراسة.

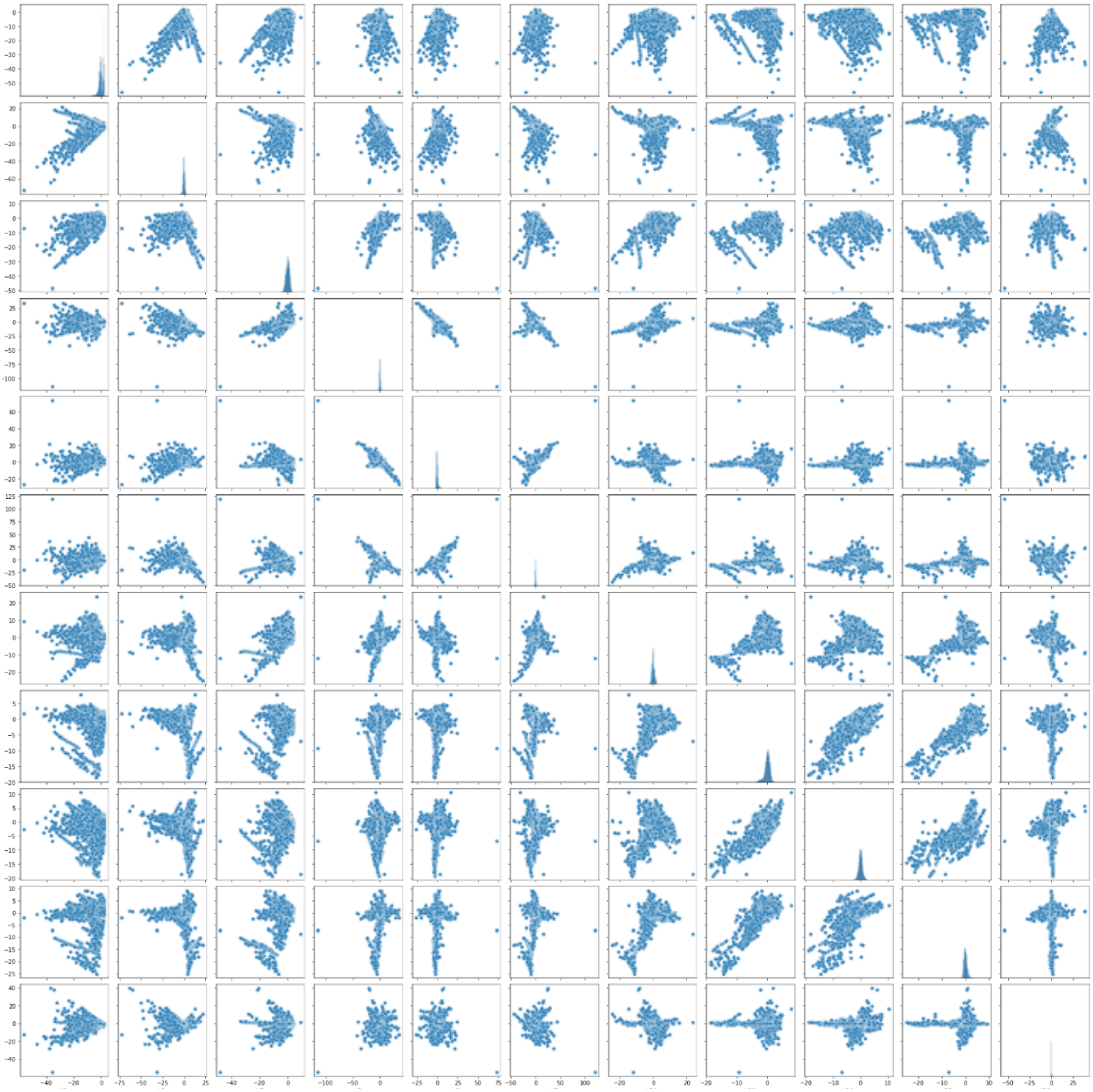
تبرز أهمية الشكل (5) للتأكد من طبيعة بيانات الدراسة، ففي ظل البيانات الضخمة فالأمر مختلف وأكثر تعقيدا عن البيانات الإحصائية العادية. يظهر من الشكل (5) أن طبيعة البيانات الفئوية والبيانات المستمرة، والنتائج تؤكد صحة ما ورد في الجدول (3).

ث. تصور العلاقات

نقوم بإنشاء مخططات الانتشار وتصورات أخرى لاستكشاف العلاقات بين المتغيرات، لا سيما بين المتغيرات المستقلة والمتغير التابع. يمكنك استخدام وظائف مثل: (Seaborn's pairplot) أو (Jointplot) المخصصة لهذا الغرض.

بعد ذلك، يمكن تصور العلاقة بين جميع المتغيرات في الانحدار باستخدام مصفوفة مخطط التشتت (scatterplot matrix) الموضحة أدناه:

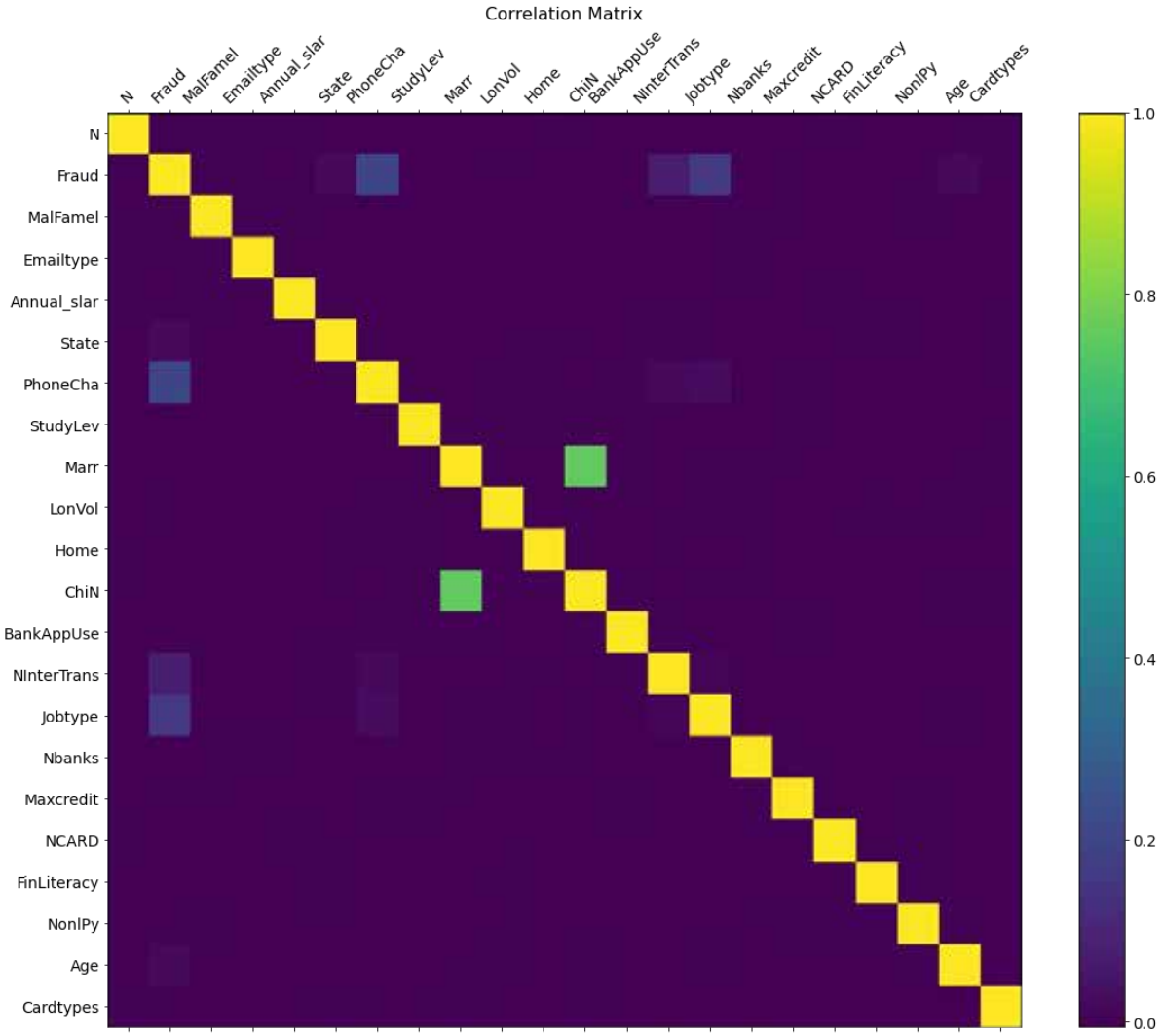
الشكل (6): مخطط الانتشار لبعض متغيرات الدراسة وطبيعة العلاقة مع بعضها



المصدر: الباحث بالاعتماد على بيانات الدراسة.

يبدو من مخطط الانتشار وجود علاقة خطية للمتغير التابع مع بعض المتغيرات، في حين يبدو البعض منها غير خطي، أو عدم وجود علاقة خطية بين المتغيرات. تعتبر هذه الخطوة جد مهمة في اختيار الخوارزمية المناسبة. كما أن دراسة الارتباط بين المتغيرات لا يقل أهمية عن الخطوة السابقة.

الشكل (7): مخطط مصفوفة الارتباط الخطي بين متيغيرات الدراسة



المصدر: الباحث بالاعتماد على بيانات الدراسة.

يبدو من الشكل (7) أن بعض المتغيرات ترتبط مع بعضها، مثل عدد الأولاد مع الوضع العائلي، أما بقية المتغيرات المستقلة فتبدو غير مرتبطة خطيا بالمتغير التابع، باستثناء ثلاث متغيرات مثل تبديل الهاتف الجوال، وعدد الصفقات الدولية، ونوع الشغل.

بشكل عام، تساعد هذه الخطوات في إعداد وتصور البيانات لتعلّم الآلة الخاضع للإشراف باستخدام (Python). من خلال تصور البيانات، يمكن اكتساب فهم أفضل للعلاقات بين المتغيرات وتحديد الأنماط التي يمكنها تحسين دقة نموذج تعلّم الآلة الذي سيتم اختياره.

3.5.نتائج خوارزميات تعلّم الآلة الخاضع للإشراف والمفاضلة بينها

نعمل في البداية على اختيار أربع خوارزميات باستخدام برمجية بايثون:

```
# Used ML algorithms
#Given Data is huge, some used ML algorithms are commented
models = []
models.append(('CART', DecisionTreeClassifier()))
models.append(('KNN', KNeighborsClassifier()))
models.append(('LDA', LinearDiscriminantAnalysis()))
models.append(('LR', LogisticRegression()))
```

تتمثل الخوارزميات المختارة في كل من:

- شجرة القرار،
- أقرب الجيران،
- التحليل التمييزي الخطي،
- الانحدار اللوجستي،

تختلف معلمات الإعداد الافتراضية لخوارزميات تعلم الآلة الخاضعة للإشراف بناءً على الخوارزمية والمكتبة أو إطار العمل المستخدم. تشمل الافتراضيات الشائعة معايير شجرة القرار (مثل "جيني" أو "إنتروبيا")، وخيارات التقسيم، والعمق الأقصى، والحد الأدنى من العينات للتقسيم والعقد. قد تحتوي الغابات العشوائية على قيم افتراضية لعدد المقدر والمعايير والحد الأدنى من العينات. تشمل الإعدادات الافتراضية للانحدار اللوجستي نوع العقوبة وقوة التنظيم (C) واختيار الحل. من المهم ملاحظة أن اختيار قيم المعلمات المناسبة أمر حيوي لأداء الخوارزمية الأمثل، وغالبًا ما يتطلب ضبطًا خاصًا بمجموعة البيانات والمشكلة المطروحة. تستخدم جميع الخوارزميات المطبقة معلمات الضبط الافتراضية، تبعا لمكتبة باثيون (Python library).

سنعرض متوسط الدقة والانحراف المعياري لكل خوارزمية بينما نحسب النتائج ونجمعها بصفة آلية لاستخدامها لاحقاً.

```
LR: 0.942506 (0.001287)
LDA: 0.944788 (0.001265)
KNN: 0.940831 (0.001467)
CART: 0.935638(0.001939)
```

يبدو أن متوسط الدقة فاق 90 في المائة للخوارزميات الأربعة المطبقة، حيث حققت كل من خوارزمية الانحدار اللوجستي، التحليل التمييزي الخطي، أقرب الجيران، شجرة القرار متوسط دقة بقيمة 94.25، 94.47، 94.08، 93.56 في المائة على التوالي، مقابل انحراف معياري0.1287، 0.1265، 0.1467، 0.19.39 في المائة على التوالي، حيث يبدو أن خوارزمية التحليل التمييزي الخطي أحسن أداء من بقية الخوارزميات قيد الدراسة وفق معيار متوسط الدقة والإنحراف المعياري.

1.3.5. معايير المقارنة بين خوارزميات تعلّم الآلة

يمكن البحث عن أفضل خوارزمية تعلم الآلة لموضوع معين بالاعتماد على معايير محددة تسمح لنا باختيار الخوارزمية الأفضل (Khatri et al., 2020)، لكن اختيار الخوارزمية يعتمد في النهاية على الخصائص المحددة للبيانات والمهمة المطروحة، وقد يكون من الضروري تجربة خوارزميات متعددة لتحديد أي منها يعمل بشكل أفضل. تتمثل معايير الاختيار في كل من ما يلي (Tatsat, 2020):

a) **الدقة:** يمثّل هذا المعيار أهم معايير مقارنة الخوارزميات في القدرة على بناء تنبؤات بشأن بيانات جديدة غير مرئية. تشير الدقة الأعلى إلى أن خوارزمية أفضل، على الرغم من أنه ينبغي الأخذ في الحسبان الدقة، لكن هذا المعيار لوحده قد لا يكون كافياً في بعض الحالات.

b) **التعقيد:** قد تكون بعض الخوارزميات أكثر تكلفة من الناحية الحسابية أو تتطلب ذاكرة أكبر من غيرها مما يجعلها أقل عملية لتطبيقات معينة، لذلك لابد من الأخذ في الحسبان هذا المعيار.

c) **التفسير:** تعد قابلية تفسير الخوارزمية أيضاً معياراً مهماً. في المفاضلة بين الخوارزميات، حيث أن البعض منها قد يكون من السهل تفسيره، مثل شجرة القرار أو الانحدار الخطي، وتوفير نظرة ثاقبة للعلاقات الأساسية بين ميزات الإدخال والمتغير المستهدف. يمكن أن تكون الخوارزميات الأخرى، مثل الشبكات العصبية، أكثر غموضًا ويصعب تفسيرها.

d) **المتانة:** تكمن قوة الخوارزمية في قدرتها على الأداء الجيد في ظل وجود بيانات مبعثرة أو غير كاملة، حيث يفضّل الخوارزميات الأكثر متانة لمثل هذه الاختلافات في البيانات بشكل عام.

e) **قابلية التوسع:** قد لا تتناسب بعض الخوارزميات بشكل جيد مع مجموعات البيانات الكبيرة أو مساحات الميزات عالية الأبعاد، وبالتالي من المهم مراعاة قابلية توسيع الخوارزمية عند اختيار نموذج مناسب لمهمة معينة.

f) **التنظيم:** يمكن أن تساعد تقنيات التنظيم في منع الإفراط في التخصيص وتحسين أداء التعميم للخوارزمية، فقد تكون الخوارزميات التي تتضمن التنظيم، مثل انحدار (Lasso or Ridge)، مفضلة لتطبيقات معينة.

g) **وقت التدريب:** يمكن أن يكون مقدار الوقت المطلوب لتدريب خوارزمية أحد المعايير الهامّة، لا سيما لمجموعات البيانات الكبيرة. تتمتع بعض الخوارزميات، مثل أقرب الجيران أو شجرة القرار، بأوقات تدريب سريعة، في حين أن البعض الآخر مثل الشبكات العصبية، يمكن أن يكون أكثر كثافة من الناحية الحسابية، وهو عامل مهم خاصة في كشف عمليات الاحتيال حيث يكون الوقت مكلف جداً.

يلخّص الجدول (7) المقارنة بين الخوارزميات المطبقّة في الدراسة حسب المعايير السبعة سالفة الذكر على النحو التالي :

الجدول (6): المقارنة بين الخوارزميات المطبّقة في الدراسة حسب معايير الأداء

الخوارزمية	الدقة Accuracy	التعقيد Complexity	التفسير Interpretation	الصلابة Rigidity	التوسع Expansion	التنظيم Regulation	وقت التدريب Training time
الانحدار اللوجستي	عالية	منخفض	عالية	متوسط	عالية	L1 / L2 penalty	سريع
التحليل التمييزي الخطي	عالية	منخفض	عالية	عالية	عالية	لا شيء	سريع
أقرب الجيران	متوسط	متوسط	منخفض	منخفض	منخفض	لا شيء	سريع
شجرة القرار	عالية	متوسط	عالية	منخفض	عالية	التقليم	متوسط

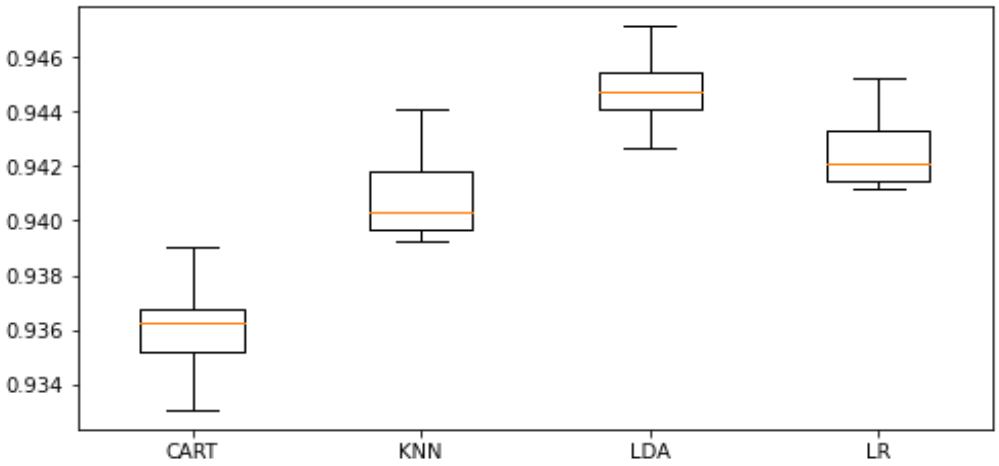
المصدر: الباحث.

للمقارنة بين الخوارزميات المطبّقة في هذه الدراسة، نرجع للنتائج التطبيقة التي تُظهِر مخرجاتها أن الخوارزميات الأربع المختارة حققت نتائج، جيدة، ويمكن المقارنة بينها من خلال استخدام الكود التالي:

```
# Comarison between used ML algorithms
fig = pyplot.figure()
fig.suptitle(Comarison between used ML algorithms ')
ax = fig.add_subplot(111)
pyplot.boxplot(results)
ax.set_xticklabels(names)
fig.set_size_inches(9,5)
pyplot.show()
```

تتلخص مخرجات المقارنة بين الخوارزميات الأربع المطبقة في الشكل التالي :

الشكل(8): نتائج المقارنة بين خوارزميات تعلّم الآلة المستخدمة



المصدر: الباحث بالاعتماد على بيانات الدراسة.

2.3.5. نتائج التدريب والتنبؤ للخوارزمية المختارة

يبدو من الشكل (8) أن جميع الخورزميات المختارة ذات أداء جيّد، لكن خوارزمية التحليل التمييزي الخطي (LDA) هي الأفضل. يبدو أن دقة النتيجة الإجمالية عالية جدًا لجميع الخوارزميات حيث فاقت القدرة التنبؤية 90 في المائة. لكن نحاول أن نتحقق من مدى نجاح أفضل الخوارزميات في التنبؤ بحالات الاحتيال. اختيار نموذج (LDA) من النتائج أعلاه والنظر إلى النتيجة في مجموعة الاختبارات :

الجدول (8): نتائج التدريب والتنبؤ وفق خوارزمية (LDA)

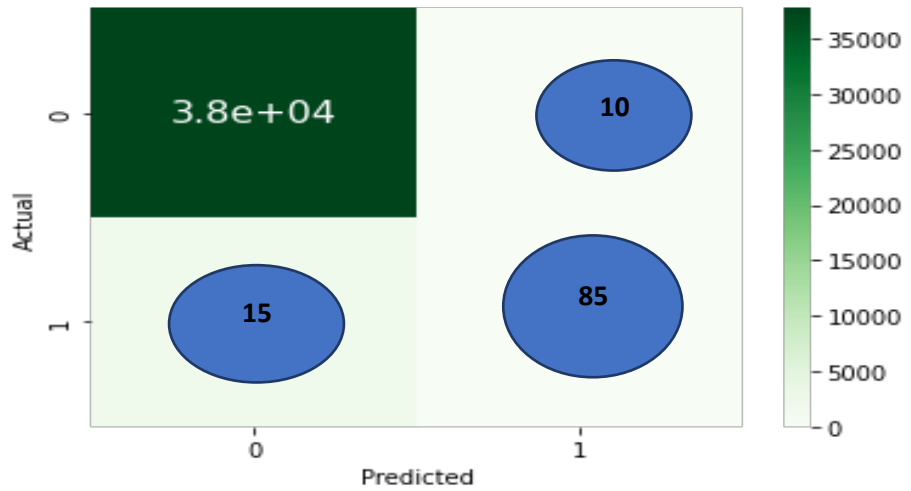
```
0.9462
[[37744     0]
 [ 2152   104]]
              precision    recall  f1-score   support

           0       0.95      1.00      0.97     37744
           1       1.00      0.05      0.09      2256
    accuracy                           0.95     40000
   macro avg       0.97      0.52      0.53     40000
weighted avg       0.95      0.95      0.92     40000
```

المصدر: الباحث بالاعتماد على بيانات الدراسة.

تم اختيار نسبة 80 في المائة للتدريب، و20 في المائة للتنبؤ، بما أن حجم العينة 200 ألف مشاهدة، فسيتم التنبؤ بنسبة 20 في المائة والبالغة 40000 مشاهدة. يبدو من النتائج الواردة في الجدول (8) أن نسبة دقة التنبؤ بالاحتيال على البطاقات الإئتمانية في ظل خوارزمية التحليل التمييزي الخطي كانت في حدود 95 في المائة، وهي نسبة جد عالية، كما يتضح أن خوارزمية التحليل التمييزي الخطي أصاب في بعض الحالات وأخطأ في البعض الآخر. والسؤال المطروح هنا بشكل أساسي حول مدى كفاءة هذا النموذج، وهو ما تبرزه مصفوفة الارتباك (confusion matrix"CM") في الشكل الموالي:

الشكل(9): مصفوفة الارتباك (CM) لنتائج خوارزمية التحليل التمييزي الخطي.



المصدر: الباحث بالاعتماد على بيانات الدراسة.

تمثل مصفوفة الارتباك جدولاً يُستخدم لبيان كفاءة خوارزمية التحليل التمييزي الخطي، إذ يعرض عدد حالات الصواب والخطأ المُمكنة المختلفة (Le Borgne, et al., 2021). يُبين الشكل (9) أن خوارزمية تحليل التمييزي الخطي (LDA) تعمل بشكل أفضل، حيث أخطأت في كشف 15 حالة فقط، واستطاعت التنبؤ بكشف 85 حالة من أصل 100 حالة احتيال.

6. الاستنتاجات والتوصيات

في الختام، تسلّط هذه الورقة الضوء على التحدّيات المتزايدة للاحتيال على بطاقات الائتمان في سياق التجارة الإلكترونية وأنظمة الدفع الإلكترونية. لمكافحة هذه الظاهرة، تبحث المؤسسات المالية وصنّاع القرار عن طرق مبتكرة لكشف وتحليل الاحتيال باستخدام تقنيات جديدة قائمة على الذكاء الاصطناعي وتعلّم الآلة وتطبيقاتها على تحليل البيانات الضخمة. توضّح هذه الدراسة أن خوارزمية تحليل التمييز الخطي كانت الأفضل أداءً، مما يشير إلى الفوائد المحتملة من خوارزميات تعلّم الآلة لتحسين كشف الاحتيال. توصي الدراسة باستخدام تعلّم الآلة لتحليل الاحتيال على بطاقات الائتمان في الدول العربية، مع التأكيد على أهمية مواكبة التطورات العالمية في هذا المجال. بصفة عامّة، تبرز هذه الدراسة الإمكانات الكبيرة لتعلّم الآلة في تعزيز كشف الاحتيال والوقاية منه، مما يساعد المؤسسات المالية والهيئات التنظيمية على إدارة المخاطر وتقليل التكاليف المرتبطة بالأنشطة الاحتيالية.
نعرض فيما يلي بعض التوصيات في ضوء نتائج هذه الدراسة:

إعادة تطبيق هذه الدراسة على بيانات حقيقية موسّعة: يمكن للجهات المعنية في الدول العربية إعادة تطبيق هذه الدراسة على بيانات حقيقية للاستفادة من دور خورزميات تعلّم الآلة في كشف الاحتيال على البطاقات الإئتمانية، كما يمكن توسيع المتغيرات لتشمل خصائص كل بنك، ومتغيرات أخرى ذات أهمية.

تشجيع التقييم والتحسين المستمر: ينبغي تشجيع المؤسسات المالية على التقييم المستمر وتحسين أنظمة الكشف عن الاحتيال، وتعزيز البحث في تقنيات الذكاء الاصطناعي وتعلّم الآلة الحديثة التي يمكنها تحسين دقّة الكشف عن الاحتيال على البطاقات الإئتمانية وسرعته.

مراقبة خوارزميات الكشف عن الاحتيال وتنظيمها: تعمل مراقبة وتنظيم خوارزميات الكشف عن الاحتيال من قبل صانعي السياسات على المساهمة في الحد من عمليات الاحتيال على البطاقات الإئتمانية، كما أن التأكد من أن هذه الخوارزميات ليست متحيزة أو تمييزية أمراً مهماً، وذلك من خلال مطالبة المؤسسات المالية بالكشف عن كيفية عمل الخوارزميات الخاصة بها وتوفير الشفافية في عمليات صنع القرار الخاصة بها.

ضمان خصوصية البيانات وأمنها وحوكمتها: يتحقق ذلك من خلال قيام السلطات الرقابية والإشرافية والتنظيمية بالتأكد من أن المؤسسات المالية تستخدم بيانات العملاء بما يتوافق مع القوانين ولوائح الخصوصية، مع تشجيع المؤسسات المالية على تنفيذ تدابير أمنية قوية لحماية بيانات العملاء من الانتهاكات والهجمات الإلكترونية، مع التركيز على البيانات الضخمة وحوكمتها.

تعزيز الابتكار والتعاون مع صناعة التقنيات المالية الحديثة (FinTech): يتطلب تعزيز الابتكار التعاون مع رواد صناعة التقنيات المالية لتطوير أنظمة جديدة لكشف الاحتيال قائمة على تعلّم الآلة. يمكن أن يساعد

هذا التعاون المؤسسات المالية في الاستفادة من التقنيات والأدوات الجديدة لمكافحة الاحتيال بشكل أكثر فعالية.

وضع وتحديث الأطر التنظيمية للكشف عن الاحتيال: ينبغي تطوير وتحديث أطر تنظيمية لأنظمة الكشف عن الاحتيال للتأكد من أن المؤسسات المالية تستخدم هذه الأنظمة بشكل أخلاقي ومسؤول، على أن تتضمن هذه الأطر إرشادات لاستخدام البيانات والشفافية والمساءلة.

تعزيز التعاون بين المؤسسات المالية: يكون ذلك من خلال تأطير السلطات الرقابية والإشرافية والتنظيمية للتعاون وتشجيع المؤسسات المالية على مشاركة البيانات والتعاون في جهود الكشف عن الاحتيال. يمكن أن يساعد هذا التعاون في تحديد أنماط الاحتيال عبر مؤسسات متعددة، ومنع المحتالين من التنقل بين المؤسسات المالية.

تعزيز التعاون الإقليمي والدولي: يُعد الاحتيال على بطاقات الائتمان أحد التحدّيات الدولية، وبالتالي تعزيز التعاون الدولي لمكافحة الاحتيال. يمكن أن يشمل هذا التعاون تبادل الخبرات وجمع البيانات وأفضل الممارسات والتقنيات الجديدة في حدود القوانين واللوائح المحلية، فضلاً عن تطوير المعايير واللوائح الدولية.

تشجيع التعليم والتوعية: من خلال تأطير تشجيع المؤسسات المالية على توفير برامج التثقيف والتوعية لعملائها حول الاحتيال على بطاقات الائتمان وكيفية حماية أنشطتهم وبياناتهم الشخصية والمالية، حيث تساعد هذه البرامج العملاء على فهم مخاطر الاحتيال، وكيفية كشف النشاط الاحتيالي والإبلاغ عنه.

قائمة المراجع

Alamri, M., & Ykhlef, M. (2022). Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques. *Electronics*, *11*(23), 4003.

Alfaiz, N. S., & Fati, S. M. (2022). Enhanced Credit Card Fraud Detection Model Using Machine Learning. *Electronics*, *11*(4), 662.

Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. (2022). A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach. *Electronics*, *11*(5), 756.

Bai, F., & Chen, X. (2013). Analysis on the new types and countermeasures of credit card fraud in mainland China. *Journal of Financial Crime*.

Berkmans, T. J., & Karthick, S. (2023). A widespread survey on machine learning techniques and user substantiation methods for credit card fraud detection. *International Journal of Business Intelligence and Data Mining*, *22*(1-2), 223-247.

Credit card fraud. (2022, March 16). In Wikipedia. Retrieved March 16, 2022, from https://en.wikipedia.org/wiki/Credit_card_fraud#Countermeasures_to_combat_card_payment_fraud

Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: a review. *Banks and Bank systems*, *4*(2), 57-68. Retrieved from https://usir.salford.ac.uk/id/eprint/2595/1/BBS.pdf (08/04/2022)

Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for Improved Credit Card Fraud Detection. *IEEE Access*, *10*, 16400-16407.

Euronews, (2023), Audio deepfake scams: Criminals are using AI to sound like family and people are falling for it, avaolible at : https://www.euronews.com/next/2023/03/25/audio-deepfake-scams-criminals-are-using-ai-to-sound-like-family-and-people-are-falling-fo

European Central Bank (2021, October), Seventh report on card fraud, available at:https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf (15/03/2023)

Gangwar, A. K., & Ravi, V. (2019). Wip: Generative adversarial network for oversampling data in credit card fraud detection. In *Information Systems Security: 15th International Conference, ICISS 2019, Hyderabad, India, December 16–20, 2019, Proceedings 15* (pp. 123-134). Springer International Publishing.

Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. *Mathematics*, *10*(13), 2272.

Kaur, P., & Gosain, A. (2018). Comparing the behavior of oversampling and undersampling approach of class imbalance learning by combining class imbalance problem with noise. In *ICT Based Innovations: Proceedings of CSI 2015* (pp. 23-30). Springer Singapore.

Khatri, S., Arora, A., & Agrawal, A. P. (2020, January). Supervised machine learning algorithms for credit card fraud detection: a comparison. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 680-683). IEEE.

Kulatilleke, G. K. (2022). Challenges and complexities in machine learning based credit card fraud detection. *arXiv preprint arXiv:2208.10943*.

Le Borgne, Yann-Aël; Bontempi, Gianluca (2021). "Machine Learning for Credit Card Fraud Detection - Practical Handbook", Available at: https://fraud-detection-handbook.github.io/fraud-detection-handbook/Foreword.html

Richards, D. A., Melancon, B. C., & Ratley, J. D. (n.d.). Managing the Business Risk of fraud: A Practical Guide [PDF]. Retrieved from https://us.aicpa.org/content/dam/aicpa/forthepublic/auditcommitteeeffectiveness/guidanceandresources/downloadabledocuments/managing-the-business-risk-of-fraud.pdf (08/04/2022)

Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach. *Computers and Electrical Engineering*, *102*, 108132.

Salekshahrezaee, Z., Leevy, J. L., & Khoshgoftaar, T. M. (2023). The effect of feature extraction and data sampling on credit card fraud detection. Journal of Big Data, 10(1), 1-17.

Sandhya, G., Abishek, M., Gunal Kumar, S., & Jisenthira Kumar, R. S. (2023). Credit Card Fraud Detection using Machine Learning Algorithms. In *ICT Systems and Sustainability* (pp. 313-320). Springer, Singapore.

SEON, (2023). Fraud Detection & Prevention - How to Find the Right Tools And Solutions, Available at: https://seon.io/resources/guides/guide-to-fraud-detection-rules/

Sybersource, (2022). Global Fraud and Payments Survey Report, https://www.cybersource.com/en-us.html

Tatsat, H., Puri, S., & Lookabaugh, B. (2020). *Machine Learning and Data Science Blueprints for Finance*. O'Reilly Media.

Van Belle, R., Baesens, B., & De Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. *Decision Support Systems*, *164*, 113866.

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND