



Intelligence artificielle générative et détection de la fraude dans les paiements électroniques en Algérie : marché, modélisation et arbitrages techniques

Generative artificial intelligence and fraud detection in electronic payments in Algeria: market, modelling and technical trade-offs

Brahim Fawzi Bourezg

Université Alger 3 (Algérie)

bourezgbrahim@gmail.com

Abstract

Cet article évalue la contribution de l'intelligence artificielle générative à la détection de la fraude sur les paiements électroniques en Algérie. L'ajustement d'un modèle de diffusion logistique à la série 2004-2024 établit que l'infrastructure de retrait est saturée à 95,9 % de son plafond, à un niveau 2,4 fois inférieur au Maroc. L'estimation d'un détecteur sur 284 807 transactions montre qu'un déplacement du point de fonctionnement de 99 % à 99,9 % de spécificité ramène la charge de traitement de cinquante-sept à six postes pour dix points de sensibilité perdus. L'apport de l'IA générative porte sur le coût unitaire de l'alerte et non sur la frontière de décision of social responsibility as a main criterion for excellence and excellence.

Article info

Received 19/09/2026
Accepted 16/10/2026

Keyword:

- ✓ Intelligence artificielle
- ✓ Detection de fraude
- ✓ paiement électronique

Abstract

This paper assesses the contribution of generative artificial intelligence to fraud detection in electronic payments in Algeria. A logistic diffusion model fitted to the 2004-2024 series shows that cash infrastructure has reached 95.9 % of its ceiling, at a level 2.4 times below Morocco. A detector estimated on 284,807 transactions shows that moving the operating point from 99 % to 99.9 % specificity cuts the workload from fifty-seven to six analysts for ten points of sensitivity. Generative AI acts on the unit cost of alerts, not on the decision boundary.

Article info

Recived 19/09/2026
Accepted 16/10/2026

Keyword:

- ✓ Artificial intelligence
- ✓ Fraud detection
- ✓ Electronic payment

1. Introduction

La détection de la fraude sur les moyens de paiement constitue le domaine bancaire où l'apprentissage automatique est le plus anciennement et le plus massivement déployé. Les moteurs de règles des années quatre-vingt-dix ont cédé la place à des modèles supervisés, puis à des méthodes de détection d'anomalies et à des approches par graphes. L'arrivée des modèles génératifs, à partir de 2022, modifie ce paysage de manière asymétrique : elle arme d'abord l'attaquant, en abaissant le coût de production de contenus trompeurs, avant d'armer le défenseur, dont les gains portent sur des tâches périphériques à la décision de détection.

L'ordre de grandeur du versant offensif est documenté. Le centre de recherche sur les services financiers de Deloitte estime que les pertes de fraude rendues possibles par l'intelligence artificielle générative aux États-Unis passeraient de 12,3 milliards de dollars en 2023 à 40 milliards de dollars en 2027 dans le scénario haut, soit un taux de croissance annuel moyen de 32 %, le scénario prudent retenant une valeur voisine de 22 milliards de dollars (Deloitte Center for Financial Services, 2024). Le versant défensif reste en revanche peu quantifié, et c'est cette asymétrie documentaire que le présent article se propose de réduire, en substituant des estimations à des affirmations partout où des données le permettent.

Le choix du terrain algérien répond à quatre raisons. La première est que le pays connaît une croissance rapide et mesurée de ses flux de paiement électronique, avec des séries publiées annuellement par le Groupement d'intérêt économique de la monétique. La deuxième est que la loi n° 23-09 du 21 juin 2023 relative à la monnaie et à la banque a ouvert le secteur aux prestataires de services de paiement et aux banques digitales, élargissant mécaniquement la surface d'exposition. La troisième est que le pays sort d'un cycle de mise à niveau de son dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme, ayant été inscrit sur la liste des juridictions sous surveillance renforcée du Groupe d'action financière en octobre 2024 puis retiré de cette liste le 19 juin 2026. La quatrième est que l'architecture monétique algérienne demeure centralisée autour d'un opérateur unique, configuration rare et analytiquement intéressante.

La problématique traitée est la suivante. Quelle est la contribution réelle de l'intelligence artificielle générative à la performance d'un dispositif de détection de la fraude sur paiement électronique, et comment cette contribution se situe-t-elle au regard de la structure du marché algérien et des arbitrages techniques et économiques auxquels un établissement est effectivement confronté ?

Quatre sous-questions structurent le propos. La première concerne la trajectoire de long terme de l'infrastructure : le système algérien est-il en phase d'expansion ou de saturation, et que vaut une projection de volumes fondée sur un simple prolongement de tendance ? La deuxième est métrologique : comment mesurer la performance d'un dispositif dans un contexte de très fort déséquilibre de classes, et quels indicateurs conduisent à des conclusions erronées ? La troisième est économique : quel est le point de fonctionnement optimal, et que valent les hypothèses de performance couramment avancées lorsqu'on les confronte à des données réelles ? La quatrième

est instrumentale : à quel endroit de la chaîne de traitement l'intelligence artificielle générative produit-elle un gain mesurable, et quels risques introduit-elle ?

L'hypothèse défendue est que la contribution de l'intelligence artificielle générative à la lutte contre la fraude ne passe pas par l'amélioration de la frontière de décision du classification, qui demeure du ressort des méthodes supervisées, mais par la réduction du coût unitaire de traitement de l'alerte, dont on montrera qu'il constitue la véritable contrainte de dimensionnement des dispositifs.

L'article comporte huit parties après cette introduction. La deuxième précise le cadre conceptuel et la méthodologie. Le troisième conduit l'analyse du marché algérien. La quatrième modélise la dynamique longue de l'infrastructure. La cinquième développe l'analyse technique du dispositif de détection. La sixième présente les résultats empiriques obtenus sur données de transactions. La septième localise et chiffre l'apport de l'intelligence artificielle générative. La huitième traite des risques et de l'encadrement. La neuvième formule les recommandations. Les annexes rassemblent les données et les sorties d'estimation permettant la réplication des résultats.

1. Cadre conceptuel et démarche méthodologique

1.1. La fraude sur paiement électronique : typologie et vecteurs

La fraude sur paiement électronique se distingue de la fraude bancaire au sens large par trois caractéristiques qui commandent le traitement technique. Elle porte sur des volumes très élevés de transactions unitaires de faible montant. Elle exige une décision en temps quasi réel, de l'ordre de quelques dizaines de millisecondes pour une autorisation. Elle présente enfin une prévalence extrêmement faible, ce qui place le problème dans la classe des événements rares.

Les données européennes fournissent la référence la mieux établie sur la structure de ce risque. Le rapport conjoint de l'Autorité bancaire européenne et de la Banque centrale européenne indique que le taux de fraude sur paiement rapporté à la valeur totale des transactions s'établit autour de 0,002 % pour l'ensemble des instruments, et que la fraude sur cartes émises dans l'Espace économique européen représentait, au premier semestre 2023, 0,031 % de la valeur et 0,015 % du nombre des paiements par carte. La fraude par carte est en outre massivement concentrée sur le canal distant, qui représente approximativement 80 % à 85 % de sa valeur, alors même que la majorité des transactions par carte sont réalisées en présence.

1.2. L'authentification forte comme variable de contrôle

L'authentification forte constitue la principale mesure de réduction de la fraude mise en œuvre à l'échelle d'un système de paiement. L'expérience européenne établit trois résultats. Les transactions authentifiées présentent un taux de fraude sensiblement inférieur aux transactions non authentifiées, en particulier pour les cartes. La couverture demeure toutefois partielle, l'authentification forte ne concernant qu'environ 40 % des paiements par carte en volume, du fait des exemptions, dont celle relative au sans contact représente à elle seule près de 79 % des transactions non authentifiées. Le

taux de fraude par carte est enfin dix-sept fois supérieur lorsque le bénéficiaire est situé hors de la zone.

La situation algérienne diffère sur ces trois points, et la différence joue dans le sens d'une protection supérieure. Le protocole d'authentification à trois domaines est appliqué à l'ensemble des paiements par carte sur internet, avec envoi d'un code à usage unique par message court, de sorte que la couverture est proche de la totalité et non de 40 %. La réglementation interdit les paiements en ligne en devises étrangères pour les achats locaux, ce qui ferme le canal transfrontalier sur lequel se concentre l'essentiel de la fraude européenne. Les transactions sont enfin plafonnées, à hauteur d'un ordre de grandeur de 100 000 dinars par opération et de 500 000 dinars par mois selon les établissements.

Ces trois éléments conduisent à une conclusion méthodologique : la référence européenne de 0,015 % doit être considérée comme une borne supérieure plutôt que comme une estimation centrale du risque algérien. Cette correction ne relâche pas la contrainte analysée ici, elle l'aggrave, puisque la précision d'un dispositif de détection décroît avec la prévalence. Un environnement mieux protégé produit mécaniquement une proportion plus élevée de fausses alertes.

1.3. L'intelligence artificielle générative comme arme offensive

L'intelligence artificielle générative modifie l'économie de l'attaque par quatre canaux. Le premier est le clonage vocal, qui rend possible la fraude au dirigeant et le contournement de l'authentification par empreinte vocale. Le deuxième est la génération de contenus vidéo synthétiques, qui fragilise la vérification d'identité à distance. Le troisième est la rédaction de messages d'hameçonnage exempts des maladroites linguistiques qui constituaient jusqu'ici un signal discriminant, ce qui importe particulièrement dans un dispositif où l'authentification repose sur un code transmis par message court et donc sur la vigilance du porteur. Le quatrième est la production de pièces justificatives falsifiées.

Le point commun de ces quatre canaux est qu'ils dégradent précisément les indices sur lesquels reposaient les dispositifs de détection. Il ne s'agit donc pas d'une simple intensification du risque mais d'une obsolescence partielle des variables explicatives, cas particulier de dérive conceptuelle. Les travaux sur les attaques visant les grands modèles de langage documentent par ailleurs une surface d'attaque propre à ces systèmes (Chowdhury et al., 2024).

1.4. Données, outils et protocole

L'étude mobilise trois corps de données, tous publics et référencés en annexe. Le premier regroupe les bilans du Groupement d'intérêt économique de la monétique, qui fournissent les volumes et la structure du parc algérien. Le deuxième est la série annuelle de l'enquête sur l'accès financier du Fonds monétaire international, pour l'Algérie, le Maroc et la Tunisie, sur la période 2004 à 2024, soit vingt et un points par pays. Le troisième est le jeu de transactions constitué par le groupe d'apprentissage automatique de l'Université libre de Bruxelles avec

Worldline, qui comprend 284 807 opérations par carte dont 492 frauduleuses, soit une prévalence de 0,173 %.

Les traitements ont été réalisés sous Python, au moyen des bibliothèques scikit-learn pour l'estimation des classificateurs et SciPy pour les ajustements non linéaires et les tests. L'ensemble des données d'entrée, des coefficients estimés, des valeurs ajustées et des résidus

figure en annexe sous une forme directement réutilisable, de manière à permettre la vérification des résultats sous tout logiciel statistique.

Le protocole appliqué au jeu de transactions mérite d'être précisé car il conditionne la validité des résultats. La partition entre apprentissage et test est temporelle et non aléatoire : les 70 % de transactions les plus anciennes constituent l'échantillon d'apprentissage, soit 199 364 opérations dont 384 fraudes, et les 30 % les plus récentes l'échantillon de test, soit 85 443 opérations dont 108 fraudes. Ce choix évite la fuite d'information future qui affecte une part importante de la littérature applicative sur ce jeu de données.

Quatre limites doivent être énoncées. Le jeu de transactions est européen et date de 2013 : il sert à estimer les paramètres de performance atteignables par un détecteur, non à mesurer la fraude algérienne, et la transposition est explicitement traitée en section 6.6. Les séries de place algériennes sont agrégées et ne permettent pas d'isoler les comportements individuels. Les coûts unitaires de traitement sont posés comme hypothèses, discutées et variées. Aucune statistique publique de fraude n'existe en Algérie, point analysé en section 3.8 comme une caractéristique du dispositif national et non comme une simple limite de l'étude.

2. Analyse du marché algérien des paiements

2.1. Volumétrie et structure

Le tableau n° 1 rassemble les principaux indicateurs du système de paiement par carte.

Tableau N° 1 : Indicateurs du paiement électronique en Algérie

Indicateur	Valeur 2025	Variation annuelle
Cartes de paiement en circulation	21 899 581	+9 %
dont cartes interbancaires CIB	4 244 542	+0,1 %
dont cartes Edahabia	17 655 039	+13 %
Distributeurs automatiques de billets	4 679	+737 unités
Retraits par carte, nombre d'opérations	235 millions	+19 %
Retraits par carte, valeur	4 397 milliards DA	+19 %
Paiements électroniques, valeur totale	939 milliards DA	+46 %
Paiements par internet, valeur	145 milliards DA	+179 %
Paiements par internet, nombre de transactions	27 123 648	+38 %
Marchands raccordés au paiement sur internet	644	en hausse
Terminaux de paiement en activité, mars 2026	plus de 100 000	+33 % depuis décembre 2025

Source : Groupement d'intérêt économique de la monétique, bilan de l'activité monétique interbancaire, exercice 2025, <https://www.giemonetique.dz>.

Le retraitement de ces séries produit cinq indicateurs que les bilans ne présentent pas directement. Premièrement, le rapport entre la valeur des paiements électroniques et celle des retraits en espèces

s'établit à 21,4 %, ce qui signifie que pour un dinar dépensé par voie électronique, près de cinq dinars sont retirés en billets. Deuxièmement, le montant moyen d'un paiement par internet ressort à 5 346 dinars, contre un retrait moyen de 18 711 dinars. Troisièmement, la valeur des paiements par internet a progressé de 179 % quand leur nombre augmentait de 38 %, ce qui implique un doublement du montant moyen unitaire, passé d'environ 2 650 dinars en 2024 à 5 346 dinars en 2025. Quatrièmement, avec un peu plus de 100 000 terminaux pour environ 1,2 million de commerçants déclarés, le taux d'équipement du commerce de détail demeure inférieur à 10 %. Cinquièmement, la valeur moyenne des paiements électroniques par carte en circulation ressort à 42 877 dinars par an.

2.2. Segmentation des émetteurs et localisation du gisement de données

Les cartes Edahabia, émises par Algérie Poste, représentent 17 655 039 unités, soit 80,6 % du parc, et progressent de 13 % sur l'exercice. Les cartes interbancaires émises par les banques représentent 4 244 542 unités, soit 19,4 % du parc, et stagnent avec une progression de 0,1 %. L'écart de dynamique est donc total : la croissance du parc est intégralement portée par un émetteur qui n'est pas une banque.

Trois conséquences en découlent. La première est que la majorité des données comportementales de paiement se constitue hors du bilan des banques, de sorte qu'un établissement bancaire algérien qui souhaiterait entraîner un modèle de détection dispose au mieux d'un cinquième du gisement national. La deuxième est que la connaissance du porteur diffère selon l'émetteur, la carte Edahabia étant accessible sans compte bancaire et servant largement une population non bancarisée, ce qui appauvrit les variables explicatives disponibles. La troisième est que l'asymétrie d'équipement technique entre les deux émetteurs crée un différentiel de maturité que les fraudeurs exploiteront en concentrant leurs tentatives sur le segment le moins protégé.

2.3. Structure de l'acceptation et concentration des marchands

Le paiement sur internet mobilise 644 marchands raccordés pour 27 123 648 transactions, soit une moyenne de 42 117 transactions par marchand et par an. Cette moyenne masque une concentration considérable, la population marchande étant dominée par les grands facturiers, à savoir les distributeurs d'eau et d'électricité, l'opérateur historique de télécommunications, les opérateurs de téléphonie mobile, les compagnies d'assurance et le transport aérien.

Cette composition a un effet direct sur le profil de risque. Une facture d'électricité constitue un paiement dont le bénéficiaire est identifié, non revendable et sans valeur de revente pour un fraudeur, de sorte que le rendement d'une fraude y est quasi nul. Un billet d'avion ou une recharge téléphonique constitue au contraire un actif liquide, immédiatement mobilisable, et concentre à ce titre le risque. La prévalence de la fraude est donc très

hétérogène entre segments, et un modèle calibré sur la moyenne sera simultanément trop sévère sur les facturiers et trop permissif sur les segments liquides. La recommandation technique qui en découle est de stratifier les seuils par catégorie de marchand.

2.4. Saisonnalité et dimensionnement de la capacité de pointe

Le mois de décembre 2025 a enregistré 3,6 millions de transactions sur internet pour une valeur de 65,27 milliards de dinars. Rapportées à la moyenne mensuelle de l'exercice, qui s'établit à 2,26 millions de transactions et 12,08 milliards de dinars, ces valeurs traduisent un coefficient saisonnier de 1,59 en volume mais de 5,40 en valeur.

L'écart entre ces deux coefficients est le fait le plus remarquable des séries disponibles. Il signifie que le montant moyen d'une transaction de décembre s'est établi à 18 131 dinars, soit 3,4 fois la moyenne annuelle. Le pic de fin d'exercice n'est donc pas un pic de fréquentation

mais un pic de valeur unitaire, vraisemblablement imputable à des règlements annuels de nature administrative ou assurantielle. Deux conséquences en résultent. Une règle de seuil de montant calibrée sur la distribution annuelle déclencherait en décembre sur une fraction considérable des transactions légitimes. Et le volume d'alertes passe d'une moyenne mensuelle de 22 905 à 36 481 en décembre, soit une majoration de 59 % de la charge sur un seul mois, ce qui rend insuffisant tout dimensionnement établi sur la moyenne annuelle.

2.5. Structure comparée du marché régional

Au Maroc, le Centre monétique interbancaire prévoyait de traiter près de 240 millions de transactions monétiques en 2025, en progression d'environ 15 %, dont 85 % réalisées par des cartes marocaines, pour un volume d'encaissements proche de 100 milliards de dirhams, les paiements par cartes étrangères représentant près de 32 milliards de dirhams. Le marché marocain de l'acquisition, longtemps quasi monopolistique, a été ouvert à de nouveaux opérateurs à compter du 1^{er} mai 2025.

Trois différences structurelles se dégagent. La première est d'intensité d'usage. Rapportées à la population, les transactions monétiques marocaines représentent environ 6,3 opérations par habitant et par an, contre un ordre de grandeur inférieur à une opération par habitant pour les paiements algériens par internet et par terminal réunis, soit un écart voisin d'un facteur huit. Ce constat sera confirmé et affiné en section 4.6 à partir des séries longues. La deuxième est l'ouverture internationale : les paiements par cartes étrangères représentent au Maroc un flux significatif, alors que le marché algérien est fermé aux devises, fermeture qui constitue du point de vue de la fraude une protection substantielle. La troisième est d'architecture de marché et constitue le point le plus important pour le sujet traité. Le Maroc s'oriente vers un modèle multi-acquéreurs depuis 2025, tandis que l'Algérie conserve une architecture centralisée autour d'un opérateur interbancaire unique.

Cette centralisation présente un inconvénient bien identifié, la constitution d'un point de défaillance unique, mais elle offre un avantage considérable et rarement relevé pour la détection : un acteur unique observe la totalité des flux interbancaires, configuration qui permet de construire un modèle national disposant d'une vision complète, là où les systèmes fragmentés doivent recourir à des mécanismes complexes de partage d'informations entre concurrents. Cet avantage est toutefois

transitoire, l'agrément des prestataires de services de paiement prévu par la loi n° 23-09 devant fragmenter progressivement l'observation des flux.

2.6. Le déplacement structurel du risque vers le canal distant

Les paiements par internet croissent de 179 % en valeur lorsque l'ensemble des paiements électroniques croît de 46 %, ce qui porte la part du canal distant dans la valeur totale des paiements électroniques de 8,1 % en 2024 à 15,4 % en 2025. Cette part aura donc pratiquement doublé en un exercice. Si l'on applique à ce canal la structure de risque observée en Europe, où le distant concentre 80 % à 85 % de la valeur de la fraude par carte, l'exposition du système algérien croît nettement plus vite que ses volumes. Le doublement du montant moyen unitaire aggrave ce constat : à taux de fraude inchangé, la perte attendue croît comme le produit du volume et du montant moyen, soit un facteur de 2,79 en une année.

Un canal supplémentaire mérite d'être signalé. Le service de paiement mobile interbancaire comptait à fin décembre 2025 quelque 95 014 comptes de particuliers et 14 283 comptes de commerçants, pour 12 682 transactions par code de réponse rapide et 44 369 transferts de particulier à particulier. Ces volumes demeurent marginaux mais le transfert entre particuliers ouvre le canal de la fraude par manipulation du payeur, qui représente désormais en Europe plus de la moitié de la valeur de la fraude sur virements et contre laquelle l'authentification forte est par construction inopérante, puisque le payeur authentifie lui-même une opération qu'il a été trompé d'initier.

2.7. L'absence de statistique publique de fraude

Aucune statistique publique de fraude sur moyens de paiement n'est publiée en Algérie, ni par le Groupement d'intérêt économique de la monétique, ni par la Banque d'Algérie. En premier lieu, cette absence interdit tout calibrage empirique des modèles au niveau du système. En deuxième lieu, elle empêche l'évaluation des politiques publiques : l'efficacité de la généralisation de l'authentification à trois domaines ne peut être mesurée faute de série avant et après, alors même que cette mesure constitue l'investissement de sécurité le plus important consenti par le système. En troisième lieu, elle prive le superviseur d'un indicateur d'alerte précoce, alors que l'expérience européenne montre que la publication semestrielle de données harmonisées a constitué le principal outil d'objectivation du débat.

2.8. Le cadre institutionnel

La loi n° 23-09 du 21 juin 2023 relative à la monnaie et à la banque a substitué un cadre nouveau à l'ordonnance de 2003. Elle institue un comité de stabilité financière, prévoit l'émission d'une monnaie digitale de banque centrale dénommée dinar algérien digital, crée un comité national des paiements et ouvre le secteur aux prestataires de services de paiement et aux banques digitales. Ce cadre a été précisé par la Banque d'Algérie au moyen d'instructions relatives à l'agrément des banques digitales et aux conditions d'autorisation et d'agrément des banques et des établissements financiers (Banque d'Algérie, 2025).

Le contexte de conformité renforce l'exigence de résultat. L'Algérie a été inscrite sur la liste des juridictions sous surveillance renforcée du Groupe d'action financière en octobre 2024, puis retirée de cette liste le 19 juin 2026 au terme d'un plan d'action portant notamment sur le renforcement du cadre juridique, l'amélioration des dispositifs de supervision et la consolidation des mécanismes de contrôle et de sanctions. Le maintien hors de cette liste suppose la pérennité des dispositifs, ce qui déplace l'enjeu de la conformité formelle vers l'efficacité opérationnelle mesurée de la détection et de la déclaration.

3. La dynamique longue de l'infrastructure : modélisation

3.1. Données et spécifications concurrentes

La projection des volumes futurs conditionne le dimensionnement des dispositifs de détection. Elle est le plus souvent conduite par prolongement d'un taux de croissance récent, méthode dont il convient d'éprouver la validité. La série retenue est le nombre de distributeurs automatiques pour 100 000 adultes, issue de l'enquête sur l'accès financier du Fonds monétaire international, disponible pour l'Algérie, le Maroc et la Tunisie de 2004 à 2024, soit vingt et

un points par pays. Cet indicateur mesure l'infrastructure d'accès aux espèces et non l'infrastructure de paiement, ce qui sera exploité comme un résultat et non subi comme une limite. Les données figurent intégralement en annexe A1.

Deux spécifications sont mises en concurrence. La première est le modèle log-linéaire, qui suppose un taux de croissance constant et une expansion illimitée :

$$\ln(y_t) = a + b \times t + \varepsilon_t, \text{ avec un taux annuel égal à } \exp(b) - 1$$

La seconde est le modèle de diffusion logistique, qui suppose l'existence d'un niveau de saturation : $y_t = K / [1 + \exp(-r \times (t - t_0))]$

Où K désigne le niveau de saturation, r la vitesse de diffusion et t_0 la date du point d'inflexion. Le choix entre les deux spécifications n'est pas indifférent : le premier modèle autorise une extrapolation exponentielle, le second impose un plafond.

Deux familles d'analyses ont été écartées, et il convient d'en donner la raison. Les tests de racine unitaire et les modèles autorégressifs intégrés à moyenne mobile n'ont pas été conduits, la puissance de ces procédures étant trop faible sur vingt et un points annuels pour que le résultat soit interprétable. La détection endogène de ruptures multiples a été écartée pour la même raison, au profit d'un test de rupture à date connue appliqué successivement à chaque année candidate.

3.2. Estimation du modèle log-linéaire et sa réfutation

Le tableau n° 2 présente les estimations par moindres carrés ordinaires pour les trois pays.

Tableau N° 2 : Estimation du modèle log-linéaire, 2004 à 2024

Pays	b	Écart type	t de Student	Probabilité critique	R ²	Durbin-Watson	Taux annuel
Algérie	0,09451	0,00997	9,48	$1,2 \times 10^{-8}$	0,8254	0,240	9,91 %
Maroc	0,04887	0,00571	8,56	$6,1 \times 10^{-8}$	0,7940	0,732	5,01 %
Tunisie	0,06722	0,00525	12,81	$8,5 \times 10^{-11}$	0,8962	0,176	6,95 %

Source : Estimations de l'auteur sous Python. Données : Fonds monétaire international, Financial Access Survey, séries DZAFCAANUM, MARFCAANUM et TUNFCAANUM, diffusées par la Federal Reserve Bank of St. Louis, <https://fred.stlouisfed.org/series/DZAFCAANUM>, <https://fred.stlouisfed.org/series/MARFCAANUM> et <https://fred.stlouisfed.org/series/TUNFCAANUM>, Détail en annexe A2.

Les coefficients sont tous significatifs à moins de un pour mille et les coefficients de détermination paraissent satisfaisants. La lecture de ces seuls indicateurs conduirait à retenir le modèle et à extrapoler une croissance de 9,91 % par an pour l'Algérie. La statistique de Durbin-Watson interdit toutefois cette conclusion : elle s'établit à 0,240 pour l'Algérie, 0,176 pour la Tunisie et 0,732 pour le Maroc, soit des valeurs très éloignées de 2 qui signalent une autocorrélation positive massive des résidus. L'examen des résidus algériens reportés en annexe A3 en donne la raison : ils sont négatifs jusqu'en 2006, positifs de 2007 à 2018, puis négatifs de 2019 à 2024. Cette configuration en vagues est la signature d'une erreur de spécification fonctionnelle et non d'un simple bruit autocorrélé.

Le modèle log-linéaire est donc rejeté, non pour insignifiance statistique, mais pour inadéquation de forme. Ce point mérite d'être souligné car il illustre un écueil courant : un coefficient de détermination de 0,825 associé à un coefficient hautement significatif peut masquer une spécification fausse, et seul l'examen des résidus le révèle.

3.3. Test de rupture structurelle

L'hypothèse alternative d'une rupture de régime a été testée par un test de Chow appliqué successivement à chaque année candidate entre 2009 et 2020, les résultats complets figurant en annexe A4. La statistique de Fisher est significative à 5 % pour toutes les dates testées, ce qui confirme l'instabilité, et atteint son maximum en 2009 avec une valeur de 158,83 pour une probabilité critique inférieure à 10^{-4} .

Le modèle segmenté correspondant estime une pente de 0,33042 avant 2009, soit un taux annuel de 39,15 %, et de 0,05497 après, soit 5,65 %. La rupture est donc très ancienne et l'idée d'un régime récent nouveau, qu'on aurait pu inférer de la reprise observée en 2022, n'est pas soutenue par les données. La croissance algérienne s'est effondrée d'un facteur sept dès 2009, ce qui correspond à l'achèvement de la phase d'équipement initial du réseau.

3.4. Le modèle de diffusion logistique

La forme des résidus et la nature du phénomène, qui relève de la diffusion d'une technologie dans une population finie, conduisent à privilégier la spécification logistique. Le tableau n° 3 présente les estimations obtenues par moindres carrés non linéaires.

Tableau N° 3 : Estimation du modèle de diffusion logistique, 2004 à 2024

Pays	K, saturation	Écart type de K	r, vitesse	Année d'inflexion	R ²	Niveau 2024 en part de K
Algérie	12,601	0,787	0,1988	2012	0,9683	95,9 %
Maroc	29,916	0,608	0,2365	2007	0,9779	95,1 %
Tunisie	37,529	0,860	0,1885	2010	0,9932	94,4 %

Source : Estimations de l'auteur. Données : Fonds monétaire international, Financial Access Survey, séries DZAFCAANUM, MARFCAANUM et TUNFCAANUM, diffusées par la Federal Reserve Bank of St. Louis, <https://fred.stlouisfed.org/series/DZAFCAANUM>, <https://fred.stlouisfed.org/series/MARFCAANUM>

et <https://fred.stlouisfed.org/series/TUNFCAANUM>, Détail en annexe A5.

L'ajustement est nettement supérieur pour les trois pays, le coefficient de détermination passant de 0,8254 à 0,9683 pour l'Algérie, de 0,7940 à 0,9779 pour le Maroc et de 0,8962 à 0,9932 pour la Tunisie. Trois résultats en découlent.

Premièrement, les trois pays du Maghreb central ont atteint leur niveau de saturation en infrastructure de retrait, avec des taux de remplissage de 95,9 %, 95,1 % et 94,4 % en 2024. La phase d'équipement est donc achevée partout, et la croissance résiduelle observée n'est qu'un approfondissement marginal.

Deuxièmement, les niveaux de saturation diffèrent considérablement : 12,6 distributeurs pour 100 000 adultes en Algérie contre 29,9 au Maroc et 37,5 en Tunisie, soit un plafond algérien 2,4 fois inférieur au marocain et 3,0 fois inférieur au tunisien. L'écart n'est donc pas un retard de calendrier que la croissance comblerait, mais une différence de palier structurel.

Troisièmement, les dates d'inflexion s'échelonnent de 2007 au Maroc à 2010 en Tunisie et 2012 en Algérie, ce qui situe le décalage temporel entre les trois systèmes à cinq ans environ, très en deçà du facteur de retard que suggérerait la seule comparaison des niveaux.

3.5. Validation hors échantillon et conséquence pour les projections

Les deux spécifications ont été réestimées sur la seule période 2004 à 2021, puis utilisées pour prévoir les trois années suivantes, dont les valeurs observées étaient réservées. Le tableau n° 4 rapporte les erreurs.

Tableau N° 4 : Validation hors échantillon, Algérie, modèles ajustés sur 2004 à 2021

Année	Valeur observée	Prévision log-linéaire	Erreur	Prévision logistique	Erreur
2022	11,57	15,32	+32,4 %	9,90	-14,4 %
2023	12,02	17,05	+41,9 %	9,98	-16,9 %
2024	12,09	18,99	+57,1 %	10,05	-16,9 %

Source : Calculs de l'auteur. Données : Fonds monétaire international, Financial Access Survey, séries DZAFCAANUM, MARFCAANUM et TUNFCAANUM, diffusées par la Federal Reserve Bank of St. Louis, <https://fred.stlouisfed.org/series/DZAFCAANUM>, <https://fred.stlouisfed.org/series/MARFCAANUM>

et <https://fred.stlouisfed.org/series/TUNFCAANUM>. Détail en annexe A6.

Le modèle log-linéaire surestime de 57 % à trois ans, le modèle logistique sous-estime de 17 %. Le second est donc très supérieur, mais il n'est pas exact, et son biais est de sens inverse, ce qui doit être signalé honnêtement : la saturation estimée sur données antérieures à 2022 était légèrement trop basse.

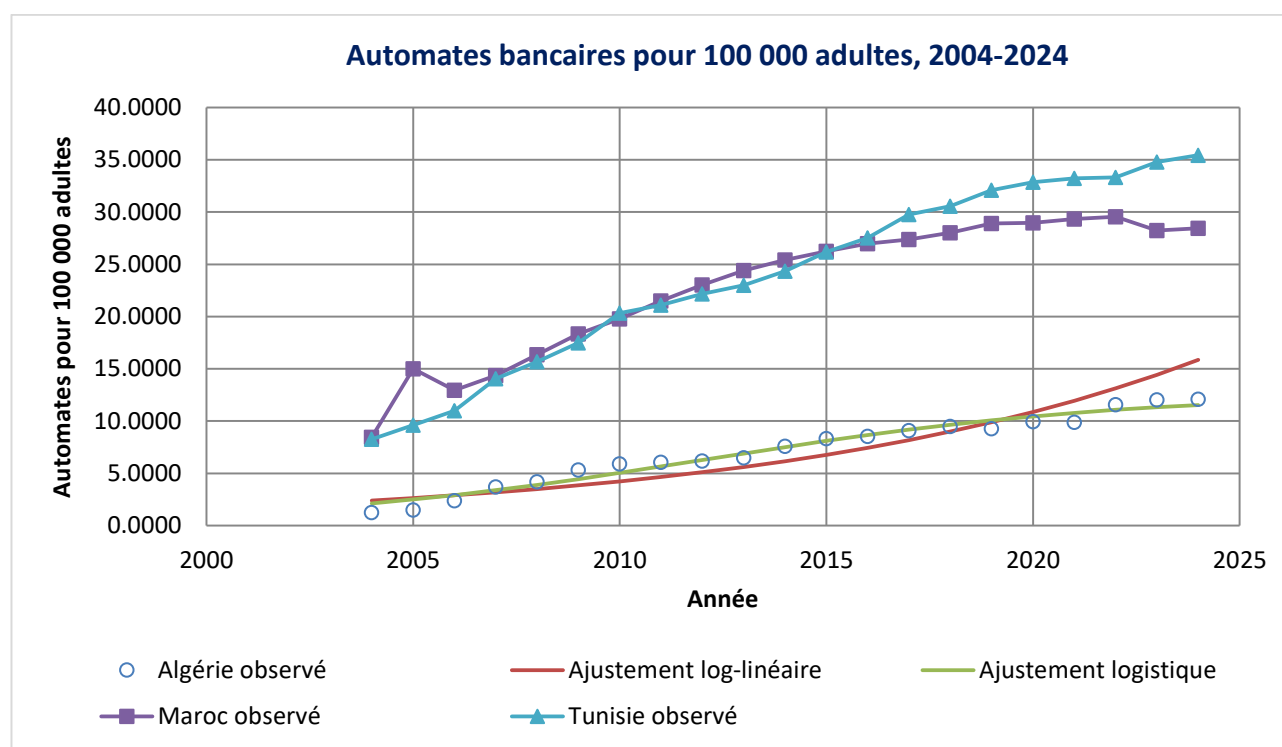
La conséquence pour l'article est directe. La projection des volumes de paiement à l'horizon 2028 conduite en section 4.7 repose sur un prolongement de taux de croissance récents. La démonstration ci-dessus établit qu'un tel prolongement appliqué à une infrastructure de paiement peut se tromper de 57 % en trois ans, systématiquement à la hausse. Les scénarios de projection sont donc maintenus mais présentés comme des bornes hautes, et l'incertitude qui les entoure est désormais quantifiée plutôt que supposée.

3.6. Lecture économique de l'écart régional

Le rapport entre les niveaux marocain et algérien s'établit à 2,35 en 2024, et le rapport tunisien à 2,93, après avoir atteint respectivement 10,00 et 6,40 en 2005. La convergence a donc été réelle et forte, mais elle s'est interrompue : les trois séries ayant atteint leur plafond, l'écart résiduel est désormais structurel et ne se refermera pas par simple continuation de tendance. Les valeurs annuelles figurent en annexe A8.

Ce résultat éclaire directement le sujet de l'article. L'Algérie plafonne à un niveau d'infrastructure de retrait deux fois et demi inférieur à celui de ses voisins, alors même que sa préférence pour les espèces demeure forte, comme l'établit le ratio de 21,4 % calculé en section 3.1. La croissance des usages ne peut donc plus venir de l'extension du réseau physique et devra passer par les canaux électroniques, ce qui confirme le déplacement du risque vers le canal distant analysé en section 3.6. Le saut technologique n'est pas une option stratégique parmi d'autres, il est la seule voie disponible.

La figure n° 1 rassemble ces résultats. Elle superpose aux valeurs observées pour l'Algérie les deux ajustements, ce qui rend visible le décrochage du modèle log-linéaire à partir de 2018, et situe le Maroc et la Tunisie sur les mêmes axes.

Figure N° 1 : Ajustements comparés pour l'Algérie et comparaison régionale

Source : Élaboré par l'auteur, à partir des données Fonds monétaire international, Financial Access Survey, séries DZAFCAANUM, MARFCAANUM et TUNFCAANUM, diffusées par la Federal Reserve Bank of St. Louis, <https://fred.stlouisfed.org/series/DZAFCAANUM>, <https://fred.stlouisfed.org/series/MARFCAANUM>

et <https://fred.stlouisfed.org/series/TUNFCAANUM>.

3.7. Projection des volumes de paiement et charge induite

La trajectoire des volumes détermine la charge future des dispositifs de détection. Le tableau n° 5 projette le nombre de paiements par internet à l'horizon 2028 selon trois hypothèses de croissance annuelle, et en déduit le volume d'alertes et la charge de traitement au point de fonctionnement de référence défini en section 5.2.

Tableau N° 5 : Projection des volumes et de la charge de traitement à l'horizon 2028

Hypothèse de croissance annuelle	Transactions en 2028	Alertes annuelles	Heures de traitement	Effectif requis
Prudente, 20 %	46,9 millions	474 954	158 318	98,9 postes
Centrale, 30 %	59,6 millions	603 862	201 287	125,8 postes
Haute, maintien de 38 %	71,3 millions	722 345	240 782	150,5 postes

Source : Calculs de l'auteur, point de fonctionnement à 90 % de sensibilité et 99 % de spécificité, vingt minutes par alerte, 1 600 heures par poste.

Ces projections doivent être lues à la lumière du résultat établi en section 4.5. Un prolongement de taux de croissance récents appliqué à une infrastructure de paiement a surestimé la valeur observée de 57 % à trois ans dans le cas du réseau d'automates. Les trois scénarios ci-dessus constituent donc des bornes hautes et non des prévisions centrales. Leur enseignement demeure néanmoins robuste dans son ordre de grandeur : à technologie de détection inchangée, la charge de traitement des alertes serait multipliée par un facteur compris entre 1,7 et 2,6 en trois ans, ce qui fait de la question du coût unitaire de traitement une contrainte croissante et non un problème de conjoncture. La projection concurrente issue

du modèle logistique, reportée en annexe A7, conduit au contraire à une quasi-stabilité de l'infrastructure de retrait, ce qui souligne l'écart entre les deux spécifications.

4. Analyse technique du dispositif de détection

4.1. Le déséquilibre de classes et l'inadéquation de l'exactitude

La fraude étant un événement rare, un classifieur qui déclarerait toutes les transactions légitimes afficherait une exactitude globale supérieure à 99,9 % tout en étant sans valeur opérationnelle. L'indicateur pertinent n'est pas l'exactitude mais la précision, définie comme la part des alertes émises qui correspondent effectivement à une fraude, puisqu'elle détermine directement la charge de travail des équipes et donc le coût du dispositif. En notant p la prévalence, Se la sensibilité et Sp la spécificité :

$$\text{Précision} = (p \times Se) / [p \times Se + (1 - p) \times (1 - Sp)]$$

Cette formule met en évidence une propriété essentielle : lorsque p est très petit, le second terme du dénominateur domine, de sorte que la précision dépend beaucoup plus de la spécificité que de la sensibilité. Un gain de dix points de sensibilité est sans effet notable sur la charge de travail, alors qu'un gain de quelques dixièmes de point de spécificité la divise.

4.2. Calage de la prévalence et matrice de confusion

En l'absence de statistique algérienne, la prévalence est calée sur la référence européenne de 0,015 %, traitée comme une borne supérieure pour les raisons exposées en section 2.2. Le tableau n° 6 applique un détecteur de sensibilité 90 % et de spécificité 99 % aux 27 123 648 paiements par internet recensés en 2025. Ces valeurs de performance sont ici posées comme hypothèses, et seront confrontées à l'estimation empirique en section 6.

Tableau N° 6 : Matrice de confusion appliquée au volume d'Algérie, prévalence de 0,015 %

Grandeur	Mode de calcul	Valeur
Transactions traitées	Bilan du GIE Monétique pour 2025	27 123 648
Transactions frauduleuses	Prévalence de 0,015 %	4 069
Vrais positifs	Sensibilité de 90 %	3 662
Faux négatifs	Fraudes non détectées	407
Faux positifs	Spécificité de 99 %	271 196
Total des alertes émises	Vrais positifs et faux positifs	274 858
Précision	Vrais positifs rapportés aux alertes	1,3 %
Exactitude globale	Décisions correctes rapportées au total	99,0 %
Charge de traitement	Alertes rapportées à 260 jours ouvrés	1 057 par jour
Effectif requis	À vingt minutes par alerte et 1 600 heures par poste	57,3 postes

Source : Calculs de l'auteur.

Le résultat central est l'écart entre une exactitude globale de 99,0 % et une précision de 1,3 %, qui signifie que soixante-quinze alertes doivent être examinées pour identifier une fraude avérée. La traduction en effectif, cinquante-sept postes à temps plein, appelle une

lecture critique. Aucun établissement algérien ne consacre cinquante-sept analystes à la seule fraude sur paiement par internet. Soit les dispositifs en place fonctionnent à une spécificité très supérieure à 99 %, au prix d'une sensibilité réduite, soit une part importante des alertes n'est pas examinée. Dans les deux cas, la contrainte effective est la capacité de traitement et non la qualité du modèle.

4.3. Sensibilité de la précision à la prévalence

Le tableau n° 7 fait varier la prévalence en maintenant la sensibilité à 90 % et la spécificité à 99 %, afin d'isoler l'effet propre du taux de fraude sur les indicateurs du dispositif.

Tableau N° 7 : Précision et volume d'alertes selon la prévalence, à performance constante

Prévalence	Fraudes détectées	Alertes émises	Précision
0,005 %	1 221	272 443	0,45 %
0,010 %	2 441	273 650	0,89 %
0,015 %	3 662	274 858	1,33 %
0,050 %	12 206	283 307	4,31 %
0,100 %	24 411	295 376	8,26 %
0,200 %	48 823	319 517	15,28 %

Source : Calculs de l'auteur.

Deux enseignements se dégagent. Le premier est que le volume d'alertes est presque insensible à la prévalence, variant seulement de 272 443 à 319 517 lorsque celle-ci est multipliée par quarante.

Ce volume est déterminé par les faux positifs, donc par la spécificité appliquée à la population légitime, qui est quasiment constante. Le dimensionnement des équipes est ainsi indépendant du niveau réel de fraude, résultat contre-intuitif d'une portée pratique directe.

Le second est que la précision est proportionnelle à la prévalence dans ce domaine de valeurs. Si les protections algériennes ramènent la prévalence à 0,005 %, la précision tombe à 0,45 %, soit deux cent vingt-trois alertes par fraude. Le paradoxe mérite d'être énoncé : mieux un système est protégé en amont, plus la détection en aval devient coûteuse par fraude évitée.

4.4. Spécificité requise pour une précision cible

$$Sp = 1 - [p \times Se \times (1 - P)] / [(1 - p) \times P]$$

Le tableau n° 8 applique cette relation à l'hypothèse centrale de prévalence, la sensibilité étant maintenue à 90 %.

Tableau N° 8 : Spécificité requise et volume d'alertes pour différentes cibles de précision

Précision cible	Spécificité requise	Faux positifs	Alertes émises
1,3 %, situation de référence	99,000 %	271 196	274 858
10 %	99,879 %	32 955	36 617
25 %	99,960 %	10 985	14 647
50 %	99,987 %	3 662	7 323
75 %	99,996 %	1 221	4 882

Source : Calculs de l'auteur.

Porter la précision de 1,3 % à 50 % exige de faire passer la spécificité de 99,000 % à 99,987 %, c'est à dire de diviser le taux de faux positifs par soixante-quatorze. La section 6 montrera qu'un tel niveau de spécificité est effectivement atteignable, mais au prix d'une perte de sensibilité que le calcul analytique, qui traite Se et Sp comme indépendants, ne fait pas apparaître.

4.5. Un modèle de coût pondéré par le montant

$$C = N \times p \times (1 - Se) \times cFN + N \times (1 - p) \times (1 - Sp) \times cFP$$

La valorisation du coût d'une fraude non détectée appelle une discussion, car l'assimiler au montant moyen d'une transaction constitue une erreur de spécification : le fraudeur maximise le rendement de chaque tentative réussie, dans la limite du plafond réglementaire. Trois valorisations sont retenues, soit 5 346 dinars correspondant au montant moyen, 16 038 dinars correspondant à trois fois cette moyenne, et 160 380 dinars intégrant les conséquences réputationnelles et réglementaires. Le coût de traitement d'une fausse alerte est fixé à 400 dinars, correspondant à vingt minutes d'analyse valorisées à 1 200 dinars l'heure. Le tableau n° 9 compare cinq points de fonctionnement sous ces trois valorisations.

Tableau N° 9 : Coût annuel attendu selon le point de fonctionnement, en millions de dinars

Point de fonctionnement	Faux négatifs	Faux positifs	cFN = 5 346 DA	cFN = 16 038 DA	cFN = 160 380 DA
Se 99 % et Sp 95 %	41	1 355 979	542,6	543,0	548,9
Se 90 % et Sp 99 %	407	271 196	110,7	115,0	173,7
Se 90 % et Sp 99,9 %	407	27 120	13,0	17,4	76,1
Se 70 % et Sp 99,9 %	1 221	27 120	17,4	30,4	206,6
Se 50 % et Sp 99,99 %	2 034	2 712	12,0	33,7	327,3

Source : Calculs de l'auteur.

Trois résultats se dégagent. Premièrement, le coût total est dominé par le traitement des fausses alertes dès que la spécificité descend à 99 % ou en deçà, et un dispositif réglé pour maximiser la détection est économiquement absurde, son coût étant quarante-cinq fois supérieur à celui du point le plus économique. Deuxièmement, la valorisation retenue détermine la localisation de l'optimum : sous la borne basse, l'optimum se situe dans une configuration où une fraude sur deux n'est pas détectée, résultat prudemment inacceptable ; dès que la pondération par le montant frauduleux est introduite, l'optimum se déplace vers le point combinant sensibilité de 90 % et spécificité de 99,9 %. La simple correction de spécification du coût suffit donc à réconcilier l'optimum économique et l'exigence prudentielle. Troisièmement, le paramétrage d'un dispositif antifraude revient à fixer implicitement la valeur que l'établissement attribue à une fraude subie par son client, décision qui devrait être documentée et validée par les organes compétents au même titre qu'un appétit pour le risque de crédit.

Le coût de traitement d'une fausse alerte, fixé à 400 dinars, mérite lui aussi une analyse de sensibilité, car il constitue le paramètre le plus incertain du modèle. Une variation de ce

coût dans un rapport de un à quatre, soit de 200 à 800 dinars, fait varier le coût total au point de référence de 55,6 à 218,0 millions de dinars dans l'hypothèse centrale de valorisation de la fraude. Elle ne déplace toutefois pas la localisation de l'optimum, puisque le coût de traitement affecte proportionnellement tous les points de fonctionnement à travers le même terme. Le paramètre commande donc le niveau du coût mais non l'arbitrage, ce qui autorise à raisonner sur une valeur approchée.

4.6. La construction de l'étiquette et l'endogénéité de la classe positive

En détection de fraude, la vérité terrain n'est pas observée au moment de la transaction : elle se construit a posteriori, à partir des contestations des porteurs et des procédures de rétro-facturation, avec un délai de plusieurs semaines à plusieurs mois. Trois conséquences en découlent.

La première est un biais d'évaluation. Une fraude non encore déclarée au moment de la mesure est comptabilisée comme légitime. Si le modèle l'avait signalée, elle est comptée en faux positif, ce

qui minore la précision mesurée ; s'il l'avait manquée, elle est comptée en vrai négatif, ce qui majore la sensibilité mesurée. Toute évaluation conduite sur une période récente sous-estime donc la précision et surestime la sensibilité. La parade consiste à n'évaluer que sur des périodes dont l'étiquetage est mûr.

La deuxième conséquence est un problème d'endogénéité. Une transaction bloquée par le dispositif ne donne jamais lieu à contestation, puisqu'elle n'a pas abouti, et n'entre donc jamais dans la classe positive observée. Le dispositif détruit ainsi sa propre vérité terrain : plus il est efficace, moins il produit d'étiquettes positives, et plus il devient difficile de ré-entraîner le modèle qui l'alimente. Cette rétroaction est spécifique à la détection de fraude et n'a pas d'équivalent en risque de crédit, où le refus laisse une trace exploitable par les techniques d'inférence des refusés.

La troisième conséquence est organisationnelle. La qualité de l'étiquette dépend du traitement effectif des alertes par les analystes, puisque c'est leur conclusion qui qualifie l'événement. Un dispositif dont les alertes ne sont pas toutes examinées produit des étiquettes incomplètes et biaisées, qui dégraderont le prochain modèle. La capacité de traitement se révèle ainsi également une contrainte statistique.

4.7. Dérive conceptuelle et cadence de réentraînement

La fraude est un phénomène adverse : la distribution des variables explicatives se déforme en réaction au dispositif de détection lui-même, contrairement au risque de crédit dont la distribution évolue avec le cycle mais sans intention. Cette dérive impose un réentraînement fréquent et un suivi des indicateurs de stabilité de population. Dans le contexte algérien, trois sources supplémentaires de dérive doivent être prises en compte : le raccordement régulier de nouveaux marchands, le doublement du montant moyen unitaire constaté en 2025, et la saisonnalité de valeur analysée en section 3.4.

5. Résultats empiriques sur données de transactions

5.1. Le jeu de données et le protocole

Les hypothèses de performance utilisées en section 5 sont maintenant confrontées à des données réelles. Le jeu mobilisé rassemble 284 807 transactions par carte de porteurs européens sur deux journées de septembre 2013, dont 492 frauduleuses, soit une prévalence de 0,173 %, ce qui en fait l'un des rares corpus publics étiquetés de cette nature. Les variables explicatives sont vingt-huit composantes principales anonymisées, auxquelles s'ajoutent l'horodatage et le montant. Les statistiques descriptives complètes figurent en annexe B1.

Deux caractéristiques du jeu méritent d'être relevées avant toute estimation. Le montant moyen des transactions frauduleuses s'établit à 122,21 unités contre 88,29 pour les transactions légitimes, ce qui confirme la logique d'optimisation du fraudeur retenue en section 5.5. Mais leur montant médian est de 9,25 contre 22,00 pour les légitimes, ce qui révèle une distribution bimodale : une majorité de tentatives de très faible montant, vraisemblablement des transactions de test destinées

à valider la validité d'une carte, et une minorité de montant élevé. Cette structure justifie a posteriori le recours à une pondération par le montant dans la fonction de coût, un comptage en nombre traitant à égalité une transaction de test et une fraude aboutie.

La partition entre apprentissage et test est temporelle : les 199 364 transactions les plus anciennes, dont 384 fraudes, servent à l'estimation, et les 85 443 plus récentes, dont 108 fraudes, au test. La prévalence de l'échantillon de test ressort à 0,126 %, valeur proche de la borne supérieure retenue pour le cas algérien, ce qui facilite la transposition.

5.2. Performance globale et choix de la métrique

Le tableau n° 10 rapporte les aires sous les deux courbes usuelles pour les deux modèles estimés, ainsi que la référence fournie par un classement aléatoire.

Tableau N° 10 : Performance sur l'échantillon de test

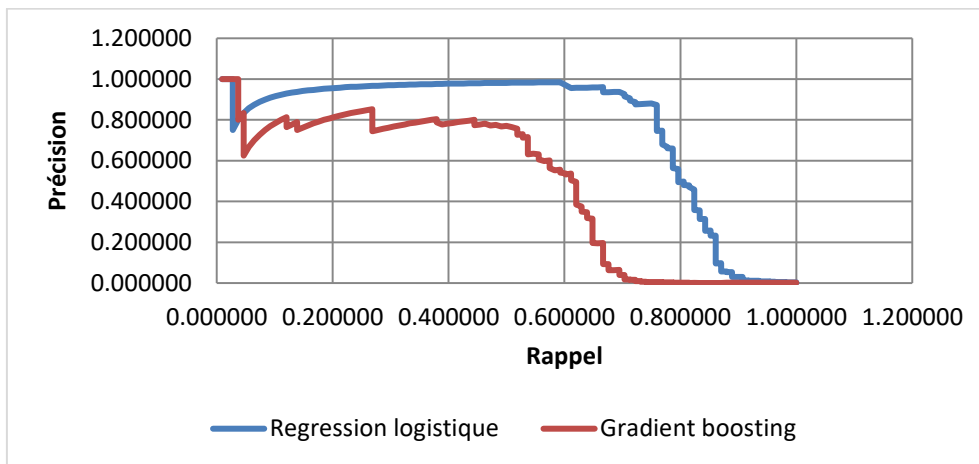
Modèle	Aire sous la courbe caractéristique	Aire sous la courbe précision-rappel
Régression logistique pondérée	0,9796	0,7677
Gradient boosting	0,7843	0,4758
Classifieur aléatoire	0,5000	0,0013

Source : Estimations de l'auteur. Données : Machine Learning Group, Université libre de Bruxelles, et Worldline, Credit Card Fraud Detection, <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>. Détail en annexe B2.

Deux enseignements se dégagent. Le premier concerne le choix du modèle : la régression logistique pondérée domine nettement le gradient boosting sur les deux métriques, résultat contraire à l'intuition dominante mais explicable par la nature des variables explicatives, qui sont des composantes principales, donc des combinaisons linéaires pour lesquelles un séparateur linéaire est adapté. Ce constat invite à la prudence quant à la supériorité présumée des méthodes d'ensemble.

Le second enseignement valide la recommandation métrologique formulée en section 5.1. Le classificateur aléatoire obtient 0,5000 sur la courbe caractéristique mais 0,0013 sur la courbe précision-rappel, soit la prévalence elle-même. La première métrique écrase donc les différences dans le haut de l'échelle, tandis que la seconde les révèle. Un modèle affichant une aire de 0,78 sous la courbe caractéristique paraît honorable et se révèle très inférieur au concurrent une fois évalué sur la métrique appropriée. Le tableau de contingence par vingtile de score reporté en annexe B3 permet de reconstituer les deux courbes et de vérifier ces aires.

La figure n° 2 représente la courbe précision-rappel des deux modèles. La courbe caractéristique de fonctionnement n'est pas reproduite, cette métrique écrasant les différences entre modèles en régime de fort déséquilibre. Le tableau de contingence de l'annexe B3 permet de l'établir si besoin.

Figure N° 2 : Courbe précision-rappel sur l'échantillon de test

Source : Élaboré par l'auteur.

5.3. La frontière de performance effective

Le tableau n° 11 présente les points de fonctionnement obtenus en faisant varier le seuil de décision de la régression logistique. Il constitue le résultat central de cette partie, car il substitue une frontière estimée aux hypothèses de performance couramment avancées.

Tableau N° 11 : Points de fonctionnement estimés, régression logistique, échantillon de test

Spécificité	Sensibilité	Vrais positifs	Faux positifs	Alertes	Précision
90,00 %	91,67 %	99	8 534	8 633	1,15 %
95,00 %	90,74 %	98	4 267	4 365	2,25 %
99,00 %	86,11 %	93	854	947	9,82 %
99,50 %	86,11 %	93	427	520	17,88 %
99,90 %	79,63 %	86	86	172	50,00 %
99,95 %	77,78 %	84	43	127	66,14 %
99,99 %	71,30 %	77	9	86	89,53 %

Source : Estimations de l'auteur. Données : Machine Learning Group, Université libre de Bruxelles, et Worldline, Credit Card Fraud Detection, <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>. Détail en annexe B4.

Trois résultats en découlent. Premièrement, l'hypothèse de travail retenue en section 5.2, à savoir une sensibilité de 90 % associée à une spécificité de 99 %, n'est pas atteignable : à 99 % de spécificité, la sensibilité effective plafonne à 86,11 %, et une sensibilité de 90 % exige de descendre à 95 % de spécificité. L'hypothèse était donc légèrement optimiste, d'environ quatre points de sensibilité, ce qui reste un ordre de grandeur acceptable mais doit être signalé.

Deuxièmement, le gain de spécificité coûte beaucoup moins cher en sensibilité que ne le suggère l'intuition. Passer de 99,00 % à 99,90 % de spécificité divise les faux positifs par dix et multiplie la précision par cinq, pour une perte de sensibilité de seulement 6,5 points. Passer de 99,90 % à 99,99 % divise encore les faux positifs par dix pour une perte supplémentaire de 8,3 points.

Troisièmement, la précision de 50 % que la section 5.4 décrivait comme exigeant une division des faux positifs par soixante-quatorze est effectivement obtenue, à 99,90 % de spécificité. L'objectif n'est donc pas hors d'atteinte, contrairement à ce que le raisonnement analytique pouvait laisser croire lorsqu'il traitait la sensibilité comme une contrainte fixe.

5.4. Optimisation du seuil sous coût pondéré par le montant

Le modèle de coût de la section 5.5 est ici appliqué au montant réel de chaque transaction, et non à un montant moyen. Le coût d'une fraude non détectée est le montant effectivement détourné. Celui d'une fausse alerte est fixé à quatre euros, hypothèse de travail retenue par analogie avec les 400 dinars de la section 5.5, rapportés au montant moyen des transactions du jeu de données. Les transactions de ce jeu concernent des porteurs européens et leurs montants sont présumés libellés en euros, cette devise n'étant toutefois pas explicitée par ses auteurs. Cette réserve est sans effet sur les résultats, puisque seuls les rapports entre coûts sont interprétés et non leur niveau absolu. Le tableau n° 12 rapporte les résultats.

Tableau N° 12 : Coût total selon le point de fonctionnement, montants réels, échantillon de test

Spécificité	Alertes	Montant non détecté	Coût de traitement	Coût total
90,00 %	8 633	2 096	34 532	36 628
95,00 %	4 365	2 097	17 460	19 557
99,00 %	947	2 481	3 788	6 269
99,50 %	520	2 481	2 080	4 561
99,90 %	172	2 772	688	3 460
99,95 %	127	2 775	508	3 283
Optimum estimé, 99,987 %	92	2 778	368	3 146
99,99 %	86	3 439	344	3 783

Source : Estimations de l'auteur. Données : Machine Learning Group, Université libre de Bruxelles, et Worldline, Credit Card Fraud Detection, <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>, consulté le 15 septembre 2026. Détail en annexe B5.

La recherche exhaustive du minimum sur l'ensemble des rangs situe l'optimum à 92 alertes émises, soit une spécificité de 99,987 %, une sensibilité de 75,00 % et une précision de 88,04 %. L'intervalle de confiance à 95 % de cette précision, obtenu par ré-échantillonnage, s'établit entre 80,90 % et 94,67 %. Le coût au point optimal est 11,6 fois inférieur à celui obtenu à 90 % de spécificité. Deux observations complètent ce résultat. La première est que le coût varie peu autour de l'optimum, de moins de 10 % entre 99,90 % et 99,987 % de spécificité, ce qui signifie que le réglage fin importe moins que l'ordre de grandeur et qu'une erreur de calibrage modérée demeure sans conséquence sérieuse. La seconde est que le montant non détecté augmente à peine lorsque la spécificité passe de 99,00 % à 99,95 %, de 2 481 à 2 775, alors que le coût de traitement est divisé par sept. Les fraudes perdues en resserrant le seuil sont donc principalement les transactions de très faible

montant identifiées en section 6.1, ce qui confirme la pertinence du critère en valeur. La figure n° 3 ci-dessous représente la fonction de coût selon le seuil de décision.

Figure N° 3. Coût total en fonction du seuil de décision



Source : Élaboré par l'auteur.

5.5. Transposition aux volumes algériens

La frontière de performance estimée est maintenant appliquée aux 27 123 648 paiements par internet recensés en Algérie en 2025, sous la prévalence de référence de 0,015 %. Le tableau n° 13 en donne les conséquences opérationnelles.

Tableau N° 13. Transposition des points de fonctionnement estimés au volume algérien

Point de fonctionnement	Alertes annuelles	Précision	Effectif requis	Coût annuel 10 ⁶ DA
Spécificité 99,00 % et sensibilité 86,1 %	274 698	1,28 %	57,2 postes	118,9
Spécificité 99,90 % et sensibilité 79,6 %	30 358	10,67 %	6,3 postes	25,5
Spécificité 99,987 % et sensibilité 75,0 %	6 549	46,59 %	1,4 poste	18,9
Spécificité 99,99 % et sensibilité 71,3 %	5 612	51,68 %	1,2 poste	21,0

Source : Calculs de l'auteur, coût de la fraude non détectée valorisé à 16 038 dinars.

Ce tableau constitue le principal résultat opérationnel de l'article. Le déplacement du point de fonctionnement de 99,00 % à 99,90 % de spécificité ramène la charge de traitement de cinquante-sept à six postes et le coût annuel de 118,9 à 25,5 millions de dinars, au prix d'une perte de sensibilité de 6,5 points seulement. Le passage à l'optimum estimé ramène l'effectif à moins d'un poste et demi et le coût à 18,9 millions de dinars.

Autrement dit, la difficulté identifiée en section 5.2, à savoir un effectif requis hors de portée des établissements algériens, ne provient pas de la nature du problème mais d'un point de fonctionnement mal choisi. Un dispositif réglé à 99 % de spécificité, valeur qui paraît élevée et que

l'intuition considérée comme exigeante, est en réalité très en deçà de ce qu'exige un traitement économiquement soutenable des alertes. C'est un résultat directement actionnable et il ne suppose aucun investissement technologique nouveau, seulement un changement de calibrage documenté.

5.6. Limites de la transposition

Quatre réserves doivent accompagner ces résultats. Le jeu de données est européen et date de 2013, de sorte que les typologies de fraude qu'il contient sont antérieures à la généralisation de l'authentification forte et à l'apparition des attaques assistées par intelligence artificielle générative. Il est anonymisé par analyse en composantes principales, ce qui interdit toute interprétation économique des variables explicatives et tout enrichissement par des signaux comportementaux ou de marchand. Sa prévalence de 0,126 % sur l'échantillon de test est huit fois supérieure à la référence européenne de place, ce qui indique un portefeuille sélectionné et non un système complet. Il ne comporte enfin que deux journées d'observation, ce qui ne permet ni de mesurer la dérive conceptuelle ni de tester la saisonnalité.

Ces limites n'invalident pas la démarche, à condition d'en préciser la portée. Les résultats estiment ce qu'un détecteur peut atteindre comme frontière entre sensibilité et spécificité, et cette frontière est une propriété du problème statistique plus que du jeu de données particulier. Ils n'estiment ni la fraude algérienne, ni la performance qu'obtiendrait un établissement algérien sur ses propres données.

6. La contribution de l'intelligence artificielle générative

6.1. Ce qu'elle n'améliore pas

Les modèles génératifs n'améliorent pas la frontière de décision d'un détecteur de fraude en temps réel. Les contraintes de latence, de l'ordre de quelques dizaines de millisecondes, l'exigence de reproductibilité et la nécessité d'expliquer un blocage de transaction excluent le recours à un modèle de langage dans la chaîne d'autorisation. Cette chaîne demeure le domaine des modèles supervisés à variables structurées, comme l'illustre la performance de la régression logistique établie en section 6.2.

6.2. La génération de données pour les classes rares

Le premier apport concerne l'apprentissage. Le déséquilibre de classes dégrade l'estimation, et la génération de transactions frauduleuses synthétiques vise à enrichir la classe minoritaire. Les modèles génératifs adverses (Goodfellow et al., 2014) et leurs dérivés tabulaires permettent de produire des observations respectant les dépendances entre variables. Cet apport prend une importance particulière dans le contexte décrit en section 5.6, où la classe positive observée est à la fois rare et endogène au dispositif.

Trois précautions méthodologiques conditionnent la validité de cette approche. Les observations synthétiques ne doivent jamais figurer dans l'échantillon de test, sous peine de mesurer la capacité

du modèle à reconnaître les productions du générateur. La partition entre apprentissage et test doit être temporelle et non aléatoire, protocole appliqué en section 6.1. Le générateur, entraîné sur les fraudes passées, reproduit enfin les typologies connues et demeure par construction aveugle aux typologies nouvelles, précisément celles que l'intelligence artificielle générative fait apparaître du côté de l'attaque.

6.3. Le triage des alertes et l'évaluation du gain

C'est ici que se situe l'apport principal. Les modèles de langage agissent sur le coût unitaire de traitement par quatre moyens : la constitution automatique du dossier d'alerte, la reconstitution narrative du contexte transactionnel du porteur, la comparaison avec les cas similaires traités antérieurement et la rédaction du projet de conclusion de l'analyste. Le tableau n° 14 chiffre ce gain sur la situation de référence.

Tableau N° 14 : Effet d'une réduction du temps de traitement unitaire des alertes

Scénario	Temps alerte par	Heures annuelles	Effectif	Coût annuel 10 ⁶ DA
Référence à Sp 99,00 %	20 minutes	91 619	57,3 postes	109,9
Réduction de 20 %	16 minutes	73 295	45,8 postes	88,0
Réduction de 30 %	14 minutes	64 134	40,1 postes	77,0
Réduction de 50 %	10 minutes	45 810	28,6 postes	55,0

Source : Calculs de l'auteur, sur la base de 274 858 alertes annuelles.

Une réduction de trente pour cent du temps unitaire libère l'équivalent de dix-sept postes et près de trente-trois millions de dinars par an. Ce gain doit toutefois être replacé au regard du résultat de la section 6.5, et cette confrontation constitue la conclusion la plus importante de l'article sur le plan pratique. Le déplacement du point de fonctionnement de 99,00 % à 99,90 % de spécificité économise cinquante et un postes, soit trois fois le gain permis par l'assistance générative la plus optimiste, et il ne coûte rien.

La hiérarchie des priorités s'en déduit sans ambiguïté. Le calibrage du seuil vient en premier, car il est gratuit et produit le gain le plus important. L'assistance générative vient ensuite, car elle est rapide à déployer et son gain reste substantiel une fois le seuil corrigé, l'équivalent de deux postes environ sur une base de six. L'enrichissement des variables explicatives vient en troisième position, car il produirait le gain le plus durable mais suppose un investissement en données que l'état du système algérien ne permet pas à court terme.

6.4. La production documentaire de conformité

Un second apport concerne l'interface avec le dispositif de lutte contre le blanchiment. La déclaration de soupçon est un acte formalisé dont la rédaction mobilise un temps significatif et dont la qualité rédactionnelle conditionne l'exploitabilité par la cellule de traitement du renseignement financier. L'assistance générative produit un gain de temps et surtout un gain d'homogénéité, la

variabilité rédactionnelle entre analystes constituant une source connue d'hétérogénéité des déclarations. Cet enjeu prend un relief particulier au regard des engagements pris dans le cadre du plan d'action mentionné en section 3.8.

Cet usage appelle une réserve ferme. La décision de déclarer relève de l'appréciation humaine et engage la responsabilité de l'établissement. L'assistance doit porter sur la forme et sur la collecte des éléments, jamais sur la qualification du soupçon.

6.5. La simulation adverse

Un troisième apport consiste à retourner la capacité générative contre le dispositif lui-même. La production de scénarios d'attaque synthétiques permet d'éprouver les règles en place et d'identifier les zones non couvertes avant qu'un fraudeur ne les découvre. Cette pratique produit des cas de test documentés et rejouables, donc utilisables comme éléments de preuve devant le superviseur, et apporte une réponse partielle au problème d'endogénéité décrit en section 5.6.

7. Les risques introduits et leur encadrement

7.1. Risque de modèle et dépendance à un tiers

La gestion du risque de modèle appliquée aux systèmes génératifs suppose trois adaptations que Bhattacharyya et al. (2025) détaillent : la traçabilité des instructions et des versions de modèle, la constitution de jeux d'évaluation propres à chaque cas d'usage, et la définition de seuils d'intervention humaine explicites. S'y ajoute une difficulté spécifique : le fournisseur du modèle est un tiers extérieur au secteur financier, dont les cycles de mise à jour ne suivent pas ceux de la validation interne, de sorte qu'une modification du modèle sous-jacent peut altérer le comportement d'une application validée sans que l'établissement en soit informé. Le Financial Stability Board (2024) range la dépendance à un petit nombre de fournisseurs tiers parmi les vulnérabilités susceptibles d'amplifier le risque systémique.

7.2. Injection d'instructions et intégrité des données d'entrée

Les dossiers d'alerte contiennent des champs alimentés par des tiers, notamment les libellés de marchands et les références de transaction. Un attaquant qui contrôle un commerce accepteur peut y insérer un texte destiné à être interprété comme une instruction par le modèle chargé de rédiger la synthèse d'alerte, technique connue sous le nom d'injection indirecte d'instructions. La conséquence possible est une synthèse orientée conduisant l'analyste à clore une alerte fondée. La parade relève de l'architecture : neutralisation des champs libres avant transmission au modèle, séparation stricte entre instructions et données, et interdiction faite au modèle de proposer une conclusion.

7.3. L'encadrement juridique

Le règlement (UE) 2024/1689 comporte sur ce sujet une disposition rarement relevée : les systèmes destinés à la détection de la fraude financière sont explicitement exclus de la catégorie des systèmes

à haut risque relative à l'évaluation de la solvabilité des personnes physiques. Un dispositif de notation en temps réel dédié à la lutte contre la fraude ne bascule donc pas dans ce régime du seul fait qu'il analyse des comportements de paiement. La qualification dépend de la finalité déclarée du système, ce qui fait de la documentation de cette finalité un acte juridique déterminant.

Cette exclusion ne vaut pas exemption de toute obligation. La date d'application générale du règlement demeure fixée au 2 août 2026, tandis que l'entrée en application des obligations propres aux systèmes à haut risque de l'annexe III a été reportée au 2 décembre 2027 sans modification de leur contenu. Surtout, un dispositif antifraude produit des décisions individuelles défavorables, blocage de carte ou refus d'opération, dont le régime relève du droit commun de la protection des données et du droit de la consommation.

8. Recommandations opérationnelles

Le tableau n° 15 récapitule la feuille de route qui découle de l'analyse, en distinguant ce qui relève de l'établissement et ce qui relève de l'autorité.

Tableau N° 15. Feuille de route issue de l'analyse

Horizon	Établissement	Autorité
Immédiat	Mesurer la précision réelle du dispositif et la part des alertes effectivement traitées ; relever le seuil de décision vers une spécificité de 99,9 % au moins ; documenter le point de fonctionnement et la valorisation implicite de la fraude, et les faire valider par les organes compétents	Engager une collecte semestrielle harmonisée des données de fraude par instrument, par canal et par catégorie de marchand
Court terme	Déployer l'assistance générative sur la constitution et la synthèse des dossiers d'alerte, sans délégation de la qualification ; neutraliser les champs libres transmis au modèle ; dimensionner la capacité sur la pointe de décembre ; instaurer un délai de latence avant toute mesure de performance	Publier les séries agrégées et fixer un format de reporting opposable aux prestataires de services de paiement et aux banques digitales dès leur agrément
Moyen terme	Stratifier les seuils par catégorie de marchand ; enrichir les variables par les signaux comportementaux et les représentations par graphes ; évaluer sur la courbe précision-rappel et en valeur plutôt qu'en nombre	Construire un dispositif mutualisé de détection tant que l'architecture demeure centralisée ; intégrer l'efficacité opérationnelle mesurée au périmètre du contrôle sur place

Source : Élaboré par l'auteur.

9. Conclusion

L'analyse aboutit à huit résultats. Premièrement, l'infrastructure algérienne de retrait est saturée : l'ajustement d'un modèle de diffusion logistique à la série 2004 à 2024 situe le niveau de saturation à 12,60 distributeurs pour 100 000 adultes, atteint à 95,9 % en 2024, avec un coefficient de détermination de 0,9683 contre 0,8254 pour le modèle log-linéaire, lui-même rejeté par une

statistique de Durbin-Watson de 0,240. Deuxièmement, ce plafond est 2,4 fois inférieur au marocain et 3,0 fois inférieur au tunisien, tous deux également saturés, de sorte que l'écart régional est structurel et que la croissance des usages algériens ne peut plus venir que des canaux électroniques.

Troisièmement, la validation hors échantillon établit qu'un prolongement de tendance exponentielle appliqué à une infrastructure de paiement surestime de 57 % à trois ans, ce qui impose de traiter les projections de volumes comme des bornes hautes. Quatrièmement, 80,6 % du parc de cartes est émis hors du système bancaire et l'acceptation en ligne se concentre sur 644 marchands dominés par les grands facturiers, ce qui localise le gisement de données hors des banques et rend hétérogène la prévalence entre segments.

Cinquièmement, l'estimation d'un détecteur sur 284 807 transactions établit que la régression logistique pondérée domine le gradient boosting, avec une aire sous la courbe précision-rappel de 0,7677 contre 0,4758, et que l'hypothèse courante d'une sensibilité de 90 % associée à une spécificité de 99 % n'est pas atteignable, la sensibilité effective

plafonnant à 86,11 % à ce niveau de spécificité. Sixièmement, l'optimisation du seuil sous coût pondéré par le montant réel situe l'optimum à 99,987 % de spécificité, 75,00 % de sensibilité et 88,04 % de précision, pour un coût onze fois et demi inférieur à celui obtenu à 90 % de spécificité.

Septièmement, la transposition aux volumes algériens montre que le déplacement du point de fonctionnement de 99,00 % à 99,90 % de spécificité ramène la charge de traitement de cinquante-sept à six postes à temps plein et le coût annuel de 118,9 à 25,5 millions de dinars, pour une perte de sensibilité de 6,5 points seulement. Huitièmement, la contribution de l'intelligence artificielle générative porte sur le coût unitaire de traitement de l'alerte, avec un gain de dix-sept postes pour une réduction de trente pour cent du temps unitaire, gain trois fois inférieur à celui que procure le seul recalibrage du seuil.

La recommandation principale en découle. Avant tout investissement technologique, un établissement doit vérifier et documenter son point de fonctionnement, car l'essentiel du coût d'un dispositif antifraude provient d'un réglage et non d'une insuffisance de modèle. La recommandation adressée à l'autorité demeure la publication d'une statistique de place de la fraude, sans laquelle aucun calibrage empirique n'est possible, y compris dans le présent article, ainsi que la construction d'un dispositif mutualisé de détection tant que l'architecture monétique demeure centralisée.

Quatre perspectives de recherche se dégagent. La première consisterait à estimer la prévalence réelle de la fraude sur le canal distant algérien à partir de données d'un établissement, ce qui transformerait les transpositions présentées ici en mesures. La deuxième porterait sur l'évaluation expérimentale du gain de temps de traitement permis par l'assistance générative, au moyen d'un protocole comparant deux groupes d'analystes sur un même corpus d'alertes. La troisième porterait sur la mesure du biais d'endogénéité de la classe positive et sur l'évaluation des méthodes de correction applicables. La quatrième relèverait de l'économie de la régulation et porterait sur la

détermination du coût social de la fraude non détectée, paramètre dont on a montré qu'il commande le point de fonctionnement des dispositifs.

Liste bibliographique

- Aldasoro, I., Gambacorta, L., Korinek, A., Shreeti, V., & Stein, M. (2024), Intelligent financial system: how AI is transforming finance, BIS Working Papers n° 1194, Bank for International Settlements, Bâle.
- Banque d'Algérie (2025), Instruction n° 01-25 et Instruction n° 02-25 relatives à l'agrément des banques digitales et aux conditions d'autorisation et d'agrément des banques et des établissements financiers, Alger.
- Basel Committee on Banking Supervision (2024), Digitalisation of finance, Bank for International Settlements, Bâle.
- Bhattacharyya, A., Yu, Y., Yang, H., Singh, R., Joshi, T., Chen, J., & Yalavarthy, K. (2025), Model risk management for generative AI in financial institutions, arXiv, n° 2503.15668.
- Bommasani, R., et al. (2021), On the opportunities and risks of foundation models, Center for Research on Foundation Models, Stanford University, États-Unis.
- Centre monétique interbancaire (2025), Transition monétique : le centre des paiements garantit la continuité, la sécurité et la fluidité des paiements, Casablanca, décembre.
- Chowdhury, A. G., Islam, M. M., Kumar, V., Shezan, F. H., Jain, V., & Chadha, A. (2024), Breaking down the defenses: a comparative survey of attacks on large language models, arXiv, n° 2403.04786.
- Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015), Calibrating probability with undersampling for unbalanced classification, IEEE Symposium on Computational Intelligence and Data Mining, Le Cap, pp. 159-166.
- Machine Learning Group, Université libre de Bruxelles, & Worldline (2018), Credit Card Fraud Detection, jeu de données de 284 807 transactions par carte, septembre 2013, site web : <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>, copie archivée : <https://zenodo.org/records/7395559> (consultés le 15/09/2026).
- Danielsson, J., & Uthemann, A. (2025), Artificial intelligence and financial crises, Journal of Financial Stability, Elsevier, Amsterdam, vol. 80.
- Deloitte Center for Financial Services (2024), Generative AI is expected to magnify the risk of deepfakes and other fraud in banking, Deloitte Insights, New York.

- European Banking Authority & European Central Bank (2024), 2024 report on payment fraud, Francfort et Paris, août, site web : <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf> (consulté le 15/09/2026).
- European Banking Authority & European Central Bank (2025), 2025 report on payment fraud, Francfort et Paris, 15 décembre, site web : <https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf> (consulté le 15/09/2026).
- Financial Action Task Force (2026), Jurisdictions under increased monitoring, plénière du 19 juin 2026, Paris.
- Financial Stability Board (2024), The financial stability implications of artificial intelligence, Bâle, 14 novembre.
- Fonds monétaire international (2026), Financial Access Survey, séries DZAFCAANUM, MARFCAANUM et TUNFCAANUM, Washington, diffusion Federal Reserve Bank of St. Louis, site web : <https://fred.stlouisfed.org/series/DZAFCAANUM>, <https://fred.stlouisfed.org/series/MARFCAANUM> et <https://fred.stlouisfed.org/series/TUNFCAANUM> (consultés le 15/09/2026).
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014), Generative adversarial nets, Advances in Neural Information Processing Systems, Montréal, vol. 27.
- Groupement d'intérêt économique de la monétique (2026), Bilan de l'activité monétique interbancaire, exercice 2025, Alger, site web : <https://www.giemonetique.dz> (consulté le 15/09/2026).
- Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Xu, Y., Ishii, E., Bang, Y., Madotto, A., & Fung, P. (2023), Survey of hallucination in natural language generation, ACM Computing Surveys, New York, vol. 55, n° 12, pp. 1-38.
- Lundberg, S. M., & Lee, S.-I. (2017), A unified approach to interpreting model predictions, Advances in Neural Information Processing Systems, Long Beach, vol. 30.
- Parlement européen et Conseil de l'Union européenne (2024), Règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, Journal officiel de l'Union européenne, Bruxelles.
- Pedregosa, F., et al. (2011), Scikit-learn: machine learning in Python, Journal of Machine Learning Research, vol. 12, pp. 2825-2830.

- République algérienne démocratique et populaire (2023), Loi n° 23-09 du 21 juin 2023 relative à la monnaie et à la banque, Journal officiel de la République algérienne n° 43, Alger.
- Ribeiro, M. T., Singh, S., & Guestrin, C. (2016), Why should I trust you? Explaining the predictions of any classifier, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, pp. 1135-1144.
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017), Attention is all you need, Advances in Neural Information Processing Systems, Long Beach, vol. 30.
- Virtanen, P., et al. (2020), SciPy 1.0: fundamental algorithms for scientific computing in Python, Nature Methods, vol. 17, pp. 261-272.

Annexes

Les tableaux qui suivent rassemblent l'ensemble des données d'entrée et des sorties d'estimation utilisées dans l'article. Ils sont présentés sous une forme directement réutilisable afin de permettre la vérification des résultats sous tout logiciel statistique. Les séries de l'annexe A proviennent de l'enquête sur l'accès financier du Fonds monétaire international. Les tableaux de l'annexe B sont issus du jeu de transactions constitué par le groupe d'apprentissage automatique de l'Université libre de Bruxelles avec Worldline, accessible à l'adresse <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud>.

A1. SERIES BRUTES, AUTOMATES POUR 100 000 ADULTES, FMI, 2004-2024

Année	Algérie	Maroc	Tunisie
2004	1.2644617361	8.4568761994	8.2563179963
2005	1.5014670141	15.0095394175	9.6093135207
2006	2.3849268634	12.9431869127	10.9805786363
2007	3.7161643238	14.3514944304	14.0413044117
2008	4.1938225946	16.3589790194	15.6751544399
2009	5.3133021454	18.3447948460	17.4848974044
2010	5.9044051662	19.7736932351	20.3397323438
2011	6.0642723135	21.4922684302	21.0858804536
2012	6.1700035521	23.0413078980	22.1810689430
2013	6.4788326403	24.3975344952	23.0094838471
2014	7.5829833284	25.4137541814	24.3348017290
2015	8.3282031836	26.2269652409	26.1957900605
2016	8.5521712306	26.9901164971	27.5321624141
2017	9.1011239648	27.3764774352	29.7769861662
2018	9.5040070163	28.0261773494	30.5632625500
2019	9.2875537190	28.8917375399	32.0923901004
2020	9.9479861500	28.9589298421	32.8518956948
2021	9.8731157484	29.3232323538	33.2369186180
2022	11.5733307219	29.5494570478	33.3180392679
2023	12.0175626309	28.2318980655	34.7858457728
2024	12.0860949386	28.4570615815	35.4392466764

A2. MODELE LOG-LINEAIRE $\ln(y) = a + b.t$

Pays	a	b	écart-type(b)	t	p	R2	Durbin-Watson	taux annuel %
Algérie	0.8734	0.09451	0.00997	9.48	1.238e-08	0.8254	0.240	9.91
Maroc	2.5960	0.04887	0.00571	8.56	6.084e-08	0.7940	0.732	5.01
Tunisie	2.4228	0.06722	0.00525	12.81	8.539e-11	0.8962	0.176	6.95

A3. VALEURS AJUSTEES ET RESIDUS, ALGERIE

Année	y observe	ln(y)	ajuste log-linéaire	résidu	ajuste logistique	résidu
2004	1.2645	0.2346	2.3950	-0.6388	2.1180	-0.8535
2005	1.5015	0.4064	2.6324	-0.5615	2.4916	-0.9901
2006	2.3849	0.8692	2.8934	-0.1932	2.9128	-0.5279
2007	3.7162	1.3127	3.1801	+0.1558	3.3814	+0.3348
2008	4.1938	1.4336	3.4953	+0.1822	3.8951	+0.2988
2009	5.3133	1.6702	3.8418	+0.3243	4.4491	+0.8642
2010	5.9044	1.7757	4.2226	+0.3353	5.0364	+0.8680
2011	6.0643	1.8024	4.6411	+0.2675	5.6475	+0.4168
2012	6.1700	1.8197	5.1011	+0.1902	6.2712	-0.1012
2013	6.4788	1.8685	5.6067	+0.1446	6.8956	-0.4168
2014	7.5830	2.0259	6.1625	+0.2074	7.5084	+0.0746
2015	8.3282	2.1196	6.7733	+0.2067	8.0983	+0.2299
2016	8.5522	2.1462	7.4446	+0.1387	8.6558	-0.1036
2017	9.1011	2.2084	8.1825	+0.1064	9.1735	-0.0723
2018	9.5040	2.2517	8.9935	+0.0552	9.6464	-0.1424
2019	9.2876	2.2287	9.8849	-0.0623	10.0721	-0.7845
2020	9.9480	2.2974	10.8647	-0.0881	10.4501	-0.5021
2021	9.8731	2.2898	11.9416	-0.1902	10.7818	-0.9087
2022	11.5733	2.4487	13.1252	-0.1258	11.0699	+0.5035
2023	12.0176	2.4864	14.4261	-0.1827	11.3177	+0.6998
2024	12.0861	2.4921	15.8560	-0.2715	11.5294	+0.5567

A4. TEST DE CHOW, ALGERIE, RUPTURE TESTEE ANNEE PAR ANNEE

Année de rupture	F(2,17)	p
2009	158.830	0.0000
2010	135.023	0.0000
2011	87.444	0.0000
2012	47.329	0.0000
2013	27.267	0.0000
2014	18.142	0.0001
2015	14.633	0.0002
2016	12.206	0.0005
2017	9.588	0.0016
2018	7.622	0.0043
2019	5.961	0.0109
2020	3.990	0.0379

- Maximum de F en 2009 : $F = 158.830$, $p = 0.0000$
- Pente avant = 0.33042 soit 39.15% par an
- Pente après = 0.05497 soit 5.65% par an

A5. MODELE DE DIFFUSION LOGISTIQUE $y = K / (1 + \exp(-r(t - t_0)))$

Pays	K	écart-type(K)	r	écart-type(r)	t ₀	année inflexion	R ²	niveau 2024 en % de K
Algérie	12.601	0.787	0.1988	0.0246	8.05	2012	0.9683	95.9
Maroc	29.916	0.608	0.2365	0.0206	2.91	2007	0.9779	95.1
Tunisie	37.529	0.860	0.1885	0.0104	6.09	2010	0.9932	94.4

A6. VALIDATION HORS ECHANTILLON, ALGERIE, AJUSTEMENT 2004-2021

Année	observe	prévu linéaire	log-erreur %	prévu logistique	erreur %
2022	11.57	15.32	+32.4	9.90	-14.4
2023	12.02	17.05	+41.9	9.98	-16.9
2024	12.09	18.99	+57.1	10.05	-16.9

A7. PROJECTION 2025-2030, ALGERIE, MODELE LOGISTIQUE

Année	projection	borne basse	borne haute
2025	11.71	10.50	12.92
2026	11.86	10.65	13.07
2027	11.99	10.78	13.20
2028	12.09	10.88	13.30
2029	12.18	10.97	13.39
2030	12.26	11.04	13.47

A8. ECART REGIONAL, RAPPORT A ALGERIE

Année	Algérie	Maroc	Tunisie	Maroc/Algérie	Tunisie/Algérie
2004	1.26	8.46	8.26	6.69	6.53
2005	1.50	15.01	9.61	10.00	6.40
2006	2.38	12.94	10.98	5.43	4.60
2007	3.72	14.35	14.04	3.86	3.78
2008	4.19	16.36	15.68	3.90	3.74
2009	5.31	18.34	17.48	3.45	3.29
2010	5.90	19.77	20.34	3.35	3.44
2011	6.06	21.49	21.09	3.54	3.48
2012	6.17	23.04	22.18	3.73	3.59
2013	6.48	24.40	23.01	3.77	3.55
2014	7.58	25.41	24.33	3.35	3.21
2015	8.33	26.23	26.20	3.15	3.15
2016	8.55	26.99	27.53	3.16	3.22
2017	9.10	27.38	29.78	3.01	3.27
2018	9.50	28.03	30.56	2.95	3.22
2019	9.29	28.89	32.09	3.11	3.46
2020	9.95	28.96	32.85	2.91	3.30
2021	9.87	29.32	33.24	2.97	3.37
2022	11.57	29.55	33.32	2.55	2.88
2023	12.02	28.23	34.79	2.35	2.89
2024	12.09	28.46	35.44	2.35	2.93

B1. STATISTIQUES DESCRIPTIVES, JEU ULB WORLDLINE

Grandeur	Valeur
Transactions	284807
Fraudes	492
Prévalence	0.1727 %
Période couverte	deux journées, septembre 2013
Variables	28 composantes principales, temps, montant
Montant moyen, ensemble	88.35
Montant médian, ensemble	22.00
Ecart type du montant	250.12
Montant moyen, fraudes	122.21
Montant médian, fraudes	9.25
Montant maximal, fraudes	2125.87
Montant moyen, légitimes	88.29
Apprentissage, transactions	199364
Apprentissage, fraudes	384
Test, transactions	85443
Test, fraudes	108
Prévalence dans le test	0.1264 %

B2. PERFORMANCE GLOBALE SUR L'ECHANTILLON DE TEST

Modèle	AUC	AUPRC
Régression logistique	0.9796	0.7677
Gradient boosting	0.7843	0.4758
Classificateur aléatoire	0.5000	0.0013

Ce tableau permet de reconstituer les courbes ROC et précision-rappel.

B3. TABLEAU DE CONTINGENCE PAR VINGTILE DE SCORE, REGRESSION LOGISTIQUE

Vingtile	score minimal	score maximal	transactions	légitimes	fraudes	montant total des fraudes
1	0.000000	0.000435	4273	4273	0	0.00
2	0.000435	0.001562	4272	4272	0	0.00
3	0.001562	0.002866	4272	4272	0	0.00
4	0.002867	0.004173	4272	4272	0	0.00
5	0.004173	0.005598	4272	4272	0	0.00
6	0.005598	0.007108	4272	4272	0	0.00
7	0.007108	0.008637	4272	4272	0	0.00
8	0.008637	0.010381	4272	4272	0	0.00
9	0.010382	0.012349	4272	4272	0	0.00
10	0.012350	0.014768	4273	4273	0	0.00
11	0.014769	0.017790	4272	4272	0	0.00
12	0.017790	0.021820	4272	4271	1	4.49
13	0.021820	0.027220	4272	4272	0	0.00
14	0.027220	0.034899	4272	4271	1	19.95
15	0.034900	0.046284	4272	4270	2	295.62
16	0.046287	0.064160	4272	4272	0	0.00
17	0.064169	0.094381	4272	4269	3	1141.99

18	0.094402	0.148969	4272	4270	2	634.30
19	0.148978	0.265682	4272	4271	1	0.69
20	0.265790	1.000000	4273	4175	98	12469.54

B4. MATRICES DE CONFUSION A DIFFERENTS SEUILS, REGRESSION LOGISTIQUE

Spécificité cible	seuil	VP	FP	FN	VN	sensibilité	précision	alertes	montant détecté	non
0.9000	0.147073	99	8534	9	76801	0.9167	0.0115	8633	2096.35	
0.9500	0.261500	98	4267	10	81068	0.9074	0.0225	4365	2097.04	
0.9900	0.656565	93	854	15	84481	0.8611	0.0982	947	2480.97	
0.9950	0.799594	93	427	15	84908	0.8611	0.1788	520	2480.97	
0.9990	0.986670	86	86	22	85249	0.7963	0.5000	172	2771.97	
0.9995	0.997354	84	43	24	85292	0.7778	0.6614	127	2775.19	
0.9999	0.999965	77	9	31	85326	0.7130	0.8953	86	3439.37	

Cout = somme des montants non détectés + 4 euros par alerte émise

B5. COUT ATTENDU SELON LE SEUIL, PONDERE PAR LE MONTANT REEL

Spécificité	seuil	alertes	montant non détecté	cout de traitement	cout total
0.9000	0.147073	8633	2096.35	34532.00	36628.35
0.9500	0.261500	4365	2097.04	17460.00	19557.04
0.9900	0.656565	947	2480.97	3788.00	6268.97
0.9950	0.799594	520	2480.97	2080.00	4560.97
0.9990	0.986670	172	2771.97	688.00	3459.97
0.9995	0.997354	127	2775.19	508.00	3283.19
0.9999	0.999965	86	3439.37	344.00	3783.37
Optimum	0.999946	92	2777.72	368.00	3145.72