Article

Les risques IT liés à l'utilisation de l'intelligence artificielle générative (IAG) dans les processus métiers au sein d'établissements bancaires

Valdrin Salihi
Institut des risques industriels, assurantiels et financiers (IRIAF)
Université de Poitiers 11 rue Archimède, 79000 Niort

RÉSUMÉ

L'article approfondit l'exploration de l'utilisation de l'intelligence artificielle générative dans le secteur bancaire, en mettant l'accent sur une évaluation détaillée des risques informatiques et des avantages opérationnels. Après avoir établi un cadre théorique basé sur une revue exhaustive de la littérature, l'étude emploie une méthodologie mixte pour collecter et analyser des données provenant de plusieurs banques. Cette approche cherche à mettre en lumière des différences significatives en termes de performance opérationnelle et de gestion des risques entre les banques adoptant l'IA générative et celles qui ne l'adoptent pas. Comme il s'agit d'un protocole théorique et inexpérimenté, il n'y a rien qui puisse démontrer que les premières bénéficient d'une réduction notable des incidents de sécurité et d'une amélioration de l'efficacité, grâce à l'automatisation et à la personnalisation des services que l'IAG propose actuellement. L'article discute également des défis liés à l'adoption de l'IA, notamment en termes de gouvernance des données et de conformité réglementaire. En conclusion, il souligne le potentiel innovateur de l'IA générative pour le secteur bancaire, tout en appelant à une approche équilibrée pour maximiser les bénéfices tout en atténuant les risques.

ABSTRACT

This article explores the use of generative artificial intelligence in the banking sector, focusing on a detailed assessment of IT risks and operational benefits. After establishing a theoretical framework based on an exhaustive literature review, the study employs a mixed methodology to collect and analyze data from several banks. This approach seeks to highlight significant differences in operational performance and risk management between banks adopting generative AI and those not. As this is a theoretical and inexperienced protocol, there is nothing to show that the former benefit from a significant reduction in security incidents and improved efficiency, thanks to the automation and personalization of services that IAG currently offers. The article also discusses the challenges associated with AI adoption, particularly in terms of data governance and regulatory compliance. In conclusion, it highlights the innovative potential of generative AI for the banking sector, while calling for a balanced approach to maximize benefits while mitigating risks.

MOTS CLÉS

#Intelligence artificielle générative ; #Risques informatiques ; #Secteur bancaire ; #Efficacité opérationnelle ; #Gestion des risques ; #Automatisation des services ; #Sécurité des données ; #Conformité réglementaire ; #Transformation numérique ; #Analyse quantitative et qualitative ; #Performance financière ; #Innovation technologique ; #Gouvernance données ; #Stratégies d'adoption de l'IA ; #EBIOS RM ; #Business Intelligence ;

KEYWORDS

#Generative artificial intelligence ; #IT risks ; #Banking sector ; #Operational efficiency ; #Risk management ; #Automation of services ; #Data security ; #Regulatory conformity ; #Digital transformation ; #Quantitative and qualitative analysis ; #Financial performance ; #Technological innovation ; #Data governance ; #AI adoption strategies ; #EBIOS RM ; #BusinessIntelligence ;

1. INTRODUCTION

A. Contexte de l'intelligence artificielle générative dans le secteur bancaire

L'Intelligence artificielle générative (IAG) se réfère aux systèmes d'intelligences artificielles capables de générer de nouvelles données, imitant souvent des formes humaines de création. Ces systèmes utilisent des techniques telles que les réseaux de neurones, le deep learning et l'apprentissage non supervisé pour produire des résultats qui n'ont pas été explicitement programmés [1]. Dans le domaine de la cybersécurité, l'IAG peut jouer un rôle important en améliorant la détection et la réduction des risques. Les systèmes d'IA sont capables d'analyser de grandes quantités de données pour identifier des modèles complexes et des anomalies, ce qui est essentiel pour contrer les cyberattaques de plus en plus sophistiquées. Cette capacité, à détecter des menaces avancées et à répondre de manière proactive aux incidents est particulièrement pertinente dans le secteur bancaire, où la sécurité des données est primordiale [2].

L'IAG est en passe de transformer de manière significative le secteur bancaire. Cette transformation est impulsée par le besoin croissant d'efficacité, de personnalisation des services et de renforcement de la sécurité informatique. Elle influence la façon dont les nouveaux services bancaires sont conçus et fournis. L'IA permet d'automatiser et d'optimiser divers processus, allant de la gestion des risques à la personnalisation de l'expérience client. Cette intégration de l'IA dans les opérations bancaires quotidiennes contribue non seulement à une plus grande efficacité opérationnelle, mais aussi à une meilleure satisfaction cliente [3].

Comme mentionné, l'IAG offre de nombreux avantages substantiels dans différents processus métiers du secteur bancaire. Toutefois, cette évolution s'accompagne de défis significatifs, notamment en termes de gestion des risques et de considérations éthiques. Un nombre important de recherches met en lumière des risques de différents types : IT, conformité, opérationnel, financier.. Ces risques peuvent avoir des conséquences significatives dans le secteur bancaire, affectant la crédibilité des décisions prises sur la base de ces technologies et potentiellement mener à des discriminations injustes. Il est donc essentiel que le secteur bancaire aborde ces défis de manière proactive pour maximiser les avantages de l'IA tout en minimisant ses risques potentiels.

En plus de cela, le secteur bancaire est également encadré par un environnement réglementaire national et international complexe. Les établissements bancaires sont confrontés à la nécessité de naviguer dans un paysage réglementaire en constante évolution, tout en exploitant les technologies d'intelligence artificielle générative pour rester compétitifs avec la concurrence.

Dans cette étude, nous nous concentrons sur l'impact que peut avoir l'intégration de l'intelligence artificielle générative dans des activités du secteur bancaire. Notre analyse couvre une période significative s'étendant de 2015 à 2023, une ère marquée par des avancées rapides et substantielles dans les technologies d'IA, ainsi que par des évolutions notables dans les pratiques de gestion des risques dans le secteur bancaire. Cette période a été choisie pour sa pertinence dans la maturation de l'IA générative et son adoption croissante dans les processus bancaires, tout en tenant compte des changements réglementaires et des nouvelles menaces en matière de cybersécurité.

B. Objectifs de l'étude

Avancée précédemment, l'IAG promet de transformer radicalement les opérations, les services clients et la gestion des risques dans le secteur bancaire. Notre hypothèse de départ postule que son intégration présente une balance bénéfice-risque profitable, malgré les préoccupations croissantes concernant la sécurité des données bancaires, la confidentialité et les risques opérationnels. Pour évaluer cette hypothèse, nous définissons des objectifs spécifiques : (**i**) évaluer quantitativement et qualitativement l'impact de l'IAG sur les risques IT/techniques, et (**ii**) identifier et mesurer les bénéfices potentiels de son intégration, tels que l'amélioration de l'efficacité opérationnelle, la personnalisation des services clients et l'innovation des produits bancaires.

Pour quantifier ces risques, nous proposerons d'utiliser des indicateurs tels que le nombre d'incidents de sécurité liés à l'IAG, la gravité des violations de données et le temps de résolution des problèmes IT. Les bénéfices seront quant à eux, évalués à travers de métriques telles que la réduction des coûts opérationnels, l'augmentation de la satisfaction client (mesurable par des enquêtes et des scores NPS), et le taux d'adoption des nouveaux services basés sur l'IAG au sein des différents établissements bancaires.

Cette approche scientifique tentera d'établir une compréhension claire de la manière dont l'IAG peut être intégrée de manière sécurisée et efficace dans les activités bancaires, tout en maximisant les avantages et en minimisant les risques.

Les verrous rencontrés lors de la réalisation de la bibliographie ont été multiples, à commencer par le caractère récent du bond d'intérêt porté par la communauté scientifique internationale aux technologies d'intelligence artificielle générative (moins de 10 ans). À cela, s'ajoute la complexité de l'environnement d'étude, car le secteur bancaire est un domaine sensible où l'information ainsi que la recherche en sont la clé. Une partie importante de la recherche scientifique dans le milieu est menée en interne et n'est partagée qu'à des consortiums financiers internationaux et n'est donc pas accessible au grand public.

La méthodologie de l'article utilise une approche quantitative et qualitative pour évaluer les risques IT et les bénéfices de l'utilisation de l'IAG dans les banques. Elle utilise des indicateurs spécifiques pour quantifier les risques, comme le nombre d'incidents de sécurité, et évalue les bénéfices à travers des métriques telles que l'amélioration de l'efficacité opérationnelle. L'étude propose une comparaison entre établissements bancaires intégrant l'IAG et ceux ne l'utilisant pas, pour isoler l'effet de l'IA sur les performances et la sécurité.

Le plan de l'article se décompose en différentes sections avec l'introduction, présentation du cadre théorique, méthodologie de recherche, analyse des résultats, et conclusion. Il débute par un contexte de l'étude, suivi d'une revue de la littérature sur l'IA dans le secteur bancaire. La méthodologie explique la collecte, l'analyse des données et l'évaluation des risques/bénéfices. L'article se clôture par une synthèse des découvertes, leurs implications pratiques, et des suggestions pour des recherches futures.

2. REVUE DE LITTÉRATURE

Offrant des perspectives d'optimisation des processus et d'amélioration de la qualité des services et processus métiers, l'intégration de l'intelligence artificielle générative dans le secteur bancaire représente une réelle avancée majeure. Cependant, cette intégration soulève également de nombreuses questions relatives aux différents types de risques qu'elle amène avec elle. La revue de littérature s'appuie sur des articles scientifiques récents (moins de 10 ans pour la plupart) afin de dresser un état des lieux des connaissances actuelles sur le sujet.

L'IA, en particulier les modèles génératifs, ont le potentiel de révolutionner le secteur bancaire en proposant des solutions novatrices pour la personnalisation des services, la gestion des risques, et l'optimisation des opérations internes. Un article clé a souligné l'importance de l'IA dans le champ de la cybersécurité, montrant comment elle peut améliorer la détection des menaces et la réponse aux incidents, ce qui est crucial dans un secteur aussi sensible que la banque. Cette étude propose une classification exhaustive des cas d'utilisation de l'IA au sein du cadre de cybersécurité du NIST, illustrant la diversité des applications possibles [4].

Pour prendre un exemple d'application actuelle dans une activité bancaire, la gestion des risques de crédit bénéficie de l'apport de l'IAG. L'utilisation de modèles prédictifs permet une évaluation plus précise du risque de crédit, en intégrant une variété plus large de données et en réduisant le temps nécessaire pour l'analyse. Ces technologies offrent une approche plus nuancée et flexible de la gestion des risques, en permettant une meilleure compréhension des profils de risque [5].

Néanmoins, comme évoqué dans l'introduction, l'intégration n'est pas sans défis. La question des biais algorithmiques et de leurs implications éthiques est particulièrement persistante. Un article s'est intéressé aux défis, implications et aux moyens de remédiations liés aux biais de l'IA, soulignant la nécessité d'approches multidisciplinaires/transversaux pour les atténuer. La sensibilisation et l'implémentation de pratiques éthiques dans le développement des systèmes d'IA sont cruciales pour garantir l'équité et la transparence [6].

Des travaux menés sur l'impact de l'utilisation de l'IAG sur les performances dans le secteur bancaire indiquent une amélioration significative de l'efficacité opérationnelle et de la satisfaction clientèle, tout en mettant en évidence les défis liés à la sécurité des données. Ces études tendent à montrer que malgré les défis inhérents à l'activité utilisatrice d'IAG, les bénéfices de son intégration peuvent être notables, à condition de mettre en place des stratégies adéquates pour gérer les risques associés [7].

Cette revue de littérature cherche à mettre en lumière les contrastes concernant l'intégration de l'IA générative dans le secteur bancaire : d'un côté, un potentiel considérable pour l'innovation et l'amélioration des services, et de l'autre, des défis significatifs liés à la cybersécurité, l'éthique et la gestion des risques. Au vu de sa complexité, l'évaluation de cette balance bénéfice-risque nécessitera une approche méthodique, qui sera développée dans les sections suivantes de cet article.

3. CONCEPTION DU CADRE EXPÉRIMENTAL

A. Sélection des variables

La conception de notre protocole expérimental repose sur l'identification et la classification des variables qui influencent directement l'intégration de l'intelligence artificielle générative dans les activités et/ou processus métiers. Ces variables sont catégorisées en deux types principaux : les variables indépendantes, qui influencent les changements dans le système, et les variables dépendantes, qui sont affectées par ces changements. Nous allons à présent proposer un référentiel non-exhaustif de variables dépendantes et indépendantes pouvant intégrer le cadre expérimental.

1. Variables dépendantes

- Incidents de sécurité :
  Description : nombre et gravité des incidents de sécurité liés aux activités/processus intégrant l'IAG.
  Pertinence : permet d'apporter un lien de causalité de l'impact de l'IAG sur la sécurité des applications et des systèmes d'information.

- Temps de réponse aux incidents :
  Description : durée moyenne entre la détection d'un incident de sécurité et sa résolution.
  Pertinence : mesure l'efficacité de la réponse aux incidents, qui peut être influencée par l'intégration de l'IAG.

- Taux de faux positifs/négatifs dans la détection des incidents de sécurité :
  Description : proportion d'alertes de sécurité incorrectement classées (faux positifs) et d'incidents réels non détectés (faux négatifs).
  Pertinence : évalue la précision des systèmes de détection des incidents liés directement/indirectement à l'IAG.

- Conformité réglementaire :
  Description : nombre de non-conformités aux normes réglementaires (RGPD, Bâle, etc...) liées à l'utilisation de l'IAG au sein d'une activité/processus.
  Pertinence : mesure les risques de non-conformité induits par l'IAG, essentiels pour le secteur bancaire hautement réglementé.

- Charge horaire de maintenance par le personnel IT :
  Description : heures de travail nécessaires pour la maintenance, les mises à jour et la gestion des systèmes d'IAG.
  Pertinence : révèle l'impact de l'IAG sur les ressources humaines en IT, indiquant si l'IAG conduit à une efficacité accrue ou à une surcharge de travail.

- Coûts liés à la sécurité de l'activité intégrant de l'IAG :
  Description : dépenses totales consacrées à la sécurité IT, incluant logiciels, matériel, et formation du personnel.
  Pertinence : fournit une mesure financière de l'impact de l'IAG sur la sécurité IT.

- Disponibilité des systèmes :
  Description : pourcentage de temps pendant lequel les systèmes d'IAG sont opérationnels et disponibles sans interruption.
  Pertinence : essentiel pour évaluer la fiabilité des systèmes d'IAG dans des environnements critiques tels que le secteur bancaire.

2. Variables indépendantes

- Type d'application IAG :
  Description : catégorise les applications IAG utilisées, telles que les chatbots pour le service client, les systèmes de recommandation, l'analyse prédictive pour la détection des fraudes, etc
  Pertinence : permet d'évaluer l'impact spécifique de différentes applications IAG sur les risques IT, offrant une vue détaillée de quels outils présentent plus de bénéfices ou de risques.

- Niveau d'intégration de l'IAG
  Description : mesure le degré d'intégration de l'IAG dans les processus opérationnels, de faible à élevé.
  Pertinence : une intégration plus profonde de l'IAG pourrait augmenter les risques techniques, mais aussi potentiellement les bénéfices. Cette variable permet d'explorer cette dynamique.

- Maturité technologique de l'IAG
  Description : évalue le niveau de développement des solutions IAG utilisées, allant des systèmes basiques aux systèmes avancés dotés de capacités d'apprentissage profond (non)supervisés.
  Pertinence : les systèmes plus matures pourraient présenter des risques différents par rapport aux systèmes moins avancés, influençant la gestion des risques.

- Formation et compétence du personnel
  Description : niveau de formation et d'expertise du personnel IT et des utilisateurs finaux dans la gestion et l'utilisation de l'IAG.
  Pertinence : un personnel mieux formé peut réduire certains risques techniques liés à l'utilisation incorrecte ou à la mauvaise interprétation des outils d'IAG.

- Fréquence des mises à jour et de la maintenance de l'IAG
  Description : fréquence à laquelle les systèmes IAG sont mis à jour et maintenus, allant de non-fréquemment à fréquemment.
  Pertinence : des mises à jour régulières peuvent corriger des vulnérabilités et améliorer la sécurité, tandis que des mises à jour irrégulières peuvent à l'inverse augmenter les risques.

Il faut bien comprendre ici la différence fondamentale entre ces deux types de variables qui réside dans leur rôle dans la relation de cause à effet. La variable indépendante est la cause présumée qui est manipulée pour tester son effet, tandis que la variable dépendante est l'effet qui est mesuré ou observé. De plus, les chercheurs ne peuvent contrôler ou modifier que la variable indépendante, mais ils ne contrôlent pas la variable dépendante ; ils l'observent seulement pour voir comment elle réagit aux changements dans la variable indépendante.

B. Groupe de contrôle vs. groupe expérimental

Dans le cadre de notre protocole expérimental sur l'intégration de l'intelligence artificielle générative dans les métiers/activités du secteur bancaire, la distinction entre groupe de contrôle et groupe expérimental constitue un pilier méthodologique fondamental. Cette approche à deux entrées permet une analyse comparative rigoureuse des impacts de l'IAG sur divers aspects opérationnels et de sécurité IT au sein des établissements bancaires.

1. Groupe de contrôle : Établissements bancaires n'utilisant pas ou peu d'IAG

Le groupe de contrôle sera soigneusement composé d'établissements bancaires qui n'implémentent pas ou peu l'IAG dans leurs processus métier. Ce groupe servira de référentiel essentiel pour mesurer les performances et les risques dans un environnement exempt de l'influence de l'IAG. L'objectif est de saisir un aperçu fidèle du fonctionnement dit “en temps normal”, fournissant ainsi un point de comparaison crucial pour évaluer les effets spécifiques attribuables à l'IAG. La sélection rigoureuse des banques pour ce groupe pourra être réalisée via un processus d’échantillonnage pour s’assurer que le groupe de contrôle représente un large éventail d’établissements bancaires et nécessitera une attention particulière aux critères de comparabilité (en termes de taille, de type de services offerts, de clientèle desservie et de localisation géographique), assurant que toute différence observée dans les résultats puisse être raisonnablement attribuée à l'utilisation de l'IAG.

2. Groupe expérimental : Établissements bancaires intégrant activement l'IAG dans leurs opérations

Par contraste, le groupe expérimental va regrouper des institutions qui intègrent activement l'IAG dans leurs activités, allant des systèmes de chatbots aux outils avancés d'analyse de données. L'objectif est d'évaluer l'impact direct de l'IAG sur les variables dépendantes définies au préalable par les équipes. Cela implique d'observer les avantages et les défis de l'adoption de l'IAG, offrant des insights précieux sur les meilleures pratiques et les stratégies d'atténuation des risques. La sélection des banques pour ce groupe vise à couvrir un éventail de modalités d'intégration de l'IAG (diversité d’applications d’IAG et de niveaux d’intégration), tout en assurant une comparabilité démographique et opérationnelle avec le groupe de contrôle.

3. Considérations supplémentaires

Dans la section des groupes, il va y avoir une attention particulière à porter sur l'assignation aléatoire qui jouera un rôle important dans l'attribution équitable des établissements aux groupes de contrôle et expérimental, garantissant que les différences observées soient bien attribuables à l'effet de l'IAG. Cette méthode contribue à minimiser les biais potentiels et renforce la validité des conclusions de l'étude. De plus, maintenir l'homogénéité entre les groupes et envisager une évaluation en double aveugle, lorsque possible, aidera à prévenir les biais de collecte et d'analyse des données, assurant une interprétation objective et fiable des résultats.

Cette composition expérimentale binaire, couplée à la suite du protocole expérimental permettra d’isoler l’effet de l’IAG des autres variables influentes est pertinente pour comprendre l’impact de l’IAG dans le secteur bancaire et offrant in fine une analyse claire et mesurable des bénéfices et des risques associés à son intégration.

4. MÉTHODOLOGIE DE COLLECTE DES DONNÉES

A. Définition de la Business Intelligence

Pour ce qui est de la partie collecte des données de notre protocole, nous allons nous servir du concept de Business Intelligence (BI). La Business Intelligence désigne l'ensemble des technologies, des applications, des stratégies et des pratiques utilisées pour collecter, intégrer, analyser et présenter les informations commerciales. L'objectif de la BI est de soutenir la prise de décision basée sur des données. La BI utilise des données historiques et actuelles pour générer des insights pertinents, permettant aux organisations de prendre des décisions stratégiques et opérationnelles éclairées [8]. En intégrant la BI dans notre méthodologie de collecte de données, nous prévoyons d'exploiter sa capacité à fournir une vue complète et multidimensionnelle des performances et des risques associés à l'IAG dans le secteur bancaire. Cela implique l'utilisation d'outils de BI pour analyser les données extraites, transformées et chargées via le processus ETL, permettant ainsi d'identifier

des tendances, des modèles et des anomalies dans les comportements et les performances des banques au sein des groupes de contrôle et expérimental.

B. Processus et application de l'ETL

L'ETL (Extraction-Transformation-Load), qui signifie Extraction, Transformation et Chargement, est un processus clé en Business Intelligence (BI) qui permet de manipuler des données issues de sources diverses, de les transformer selon des besoins spécifiques, puis de les charger dans une destination cible pour l'analyse. L'ETL est essentiel pour les organisations cherchant à extraire des connaissances pertinentes à partir de grandes quantités de données hétérogènes, facilitant ainsi une prise de décision éclairée [9].

Le processus ETL commence par l'extraction des données de leurs sources originales, qui peuvent varier de bases de données internes à des fichiers externes ou des flux de données en ligne. La phase de transformation adapte ensuite ces données à des formats et structures prédéfinis, corrigeant les anomalies et enrichissant les données si nécessaire. Enfin, le chargement implique l'insertion des données transformées dans une base de données, un entrepôt de données, ou un Data Lake (lac de données), où elles peuvent être ensuite analysées et exploitées par des requêtes, dashboards (voir figure 1 [9]).

Pour notre étude, l'utilisation d'un processus ETL nous permettra de collecter systématiquement des données sur les variables dépendantes et indépendantes identifiées, provenant de sources multiples telles que les applications hébergeuses d'IAG, les logs (journalisation), les rapports de sécurité IT, les systèmes d'information…

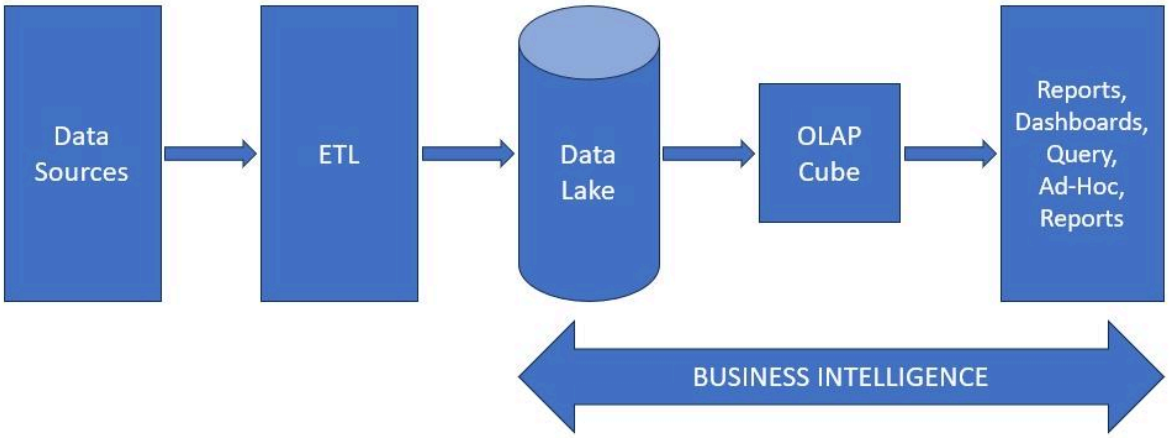

Fig.1 Processus de l'ETL et de la BI

1. Étape 1 : Extraction

L'étape d'extraction dans le processus ETL définit la qualité et la pertinence des données qui seront utilisées pour l'analyse. Cette phase implique l'identification précise des sources de données qui seront pertinentes pour notre étude. Chaque source de données servira à offrir un aperçu de l'impact de l'IAG, nécessitant une approche méthodique pour leur extraction. L'extraction des données doit être effectuée en respectant strictement les protocoles de sécurité et de confidentialité pour protéger les informations sensibles des clients, du personnel et des institutions. Les données extraites doivent être anonymisées ou semi-anonymisées et sécurisées pour éviter toute fuite d'informations personnelles ou financières. De plus, il est essentiel de s'assurer que l'extraction des données ne perturbe pas les opérations quotidiennes des systèmes sources (applications, sites, ..).

Pour chaque type de données, des méthodes d'extraction spécifiques doivent être mises en place. Par exemple, l'accès aux données d'une application CRM (gestion de la relation client) peut nécessiter l'utilisation d'APIs qui permettent une extraction automatisée et régulière des données sans compromettre la sécurité du système. Pour les bases de données de transactions, des requêtes SQL personnalisées peuvent être nécessaires pour extraire des ensembles de données pertinents en fonction des besoins de l'étude.

Il sera important pour chaque étape de l'ETL de documenter, le processus lui correspondant. Pour l'étape de l'extraction, il devra y avoir une documentation pour chaque source de données, en incluant les détails sur les méthodes d'extraction utilisées, les défis rencontrés, et les solutions mises en œuvre. Cette documentation facilitera l'étape de transformation en fournissant un contexte clair sur la provenance des données et les manipulations nécessaires pour les préparer à l'analyse.

2. Étape 2 : Transformation

L'étape de transformation dans le processus ETL est essentielle pour préparer les données extraites à une analyse précise et significative. Cette phase va venir modifier les données pour garantir leur qualité, leur cohérence et leur compatibilité avec les objectifs d'analyse. Inspiré des pratiques décrites dans la recherche, voici une approche détaillée pour la transformation des données qui devra être appliqué dans notre protocole :

a. Standardisation : Les données provenant de diverses sources n'ont pas souvent le même format. La standardisation implique l'harmonisation des formats de données, comme les dates et les montants monétaires, pour assurer leur uniformité. Cela facilite les comparaisons et les analyses transversales entre les données des groupes de contrôle et expérimental.
b. Nettoyage : Cette étape visera à identifier et à corriger les anomalies dans les données, telles que les valeurs aberrantes, les erreurs de saisie, et les incohérences. Des algorithmes de nettoyage peuvent être appliqués pour automatiser la détection et la correction des erreurs, améliorant ainsi la fiabilité des données.
c. Enrichissement : Cette étape est optionnelle dans la transformation et va dépendre de la nécessité d'ajouter des informations aux données extraites pour enrichir les analyses. L'enrichissement augmente la valeur analytique des données en fournissant des contextes supplémentaires.
d. Intégration : Les données issues des différentes sources devront être fusionnées pour créer un ensemble cohérent. L'intégration implique l'alignement des schémas de données et la résolution des conflits pour assurer une vue unifiée. Cette fusion servira pour la partie analyse de l'impact global de l'IAG sur les établissements bancaires.
e. Anonymisation : Obligatoire dans notre contexte et conformément aux réglementations sur la protection des données, les informations personnellement identifiables devront être anonymisées. Cette étape garantit que les analyses respectent la vie privée des clients et des employés, sans compromettre l'intégrité des insights générés.
f. Agrégation : Pour faciliter l'analyse, les données peuvent être agrégées selon différents critères, tels que le temps, les coûts.. Cette consolidation permet d'identifier des tendances et des modèles significatifs au sein des données.

Comme montrée dans l'approche précédente, la transformation est un processus itératif qui nécessitera une validation continue par les manipulateurs de l'ETL pour s'assurer que les données modifiées répondent aux exigences de qualité et d'analyse. Des tests de qualité des données devront être effectués tout au long de cette étape pour détecter et rectifier les problèmes éventuels, garantissant ainsi que les données transformées sont prêtes pour l'analyse.

3. Étape 3 : Chargement

Dans le processus de l'ETL, le chargement est la phase finale où les données transformées seront transférées vers leur destination cible, souvent un entrepôt de données (de type Data lake, Data warehouse,..) ou une base de données analytique. Cette phase rend les données disponibles pour l'analyse et la prise de décision. Le chargement doit être géré avec soin pour assurer l'intégrité des données et la performance du système dans son ensemble.

Dans notre contexte, l'entrepôt de données aura une place centrale dans la méthode de collecte, car elle consolidera toutes les données pertinentes pour l'étude de l'impact de l'IA générative dans le secteur bancaire. Les données chargées devront être organisées de manière à faciliter les requêtes complexes et l'analyse multidimensionnelle.

Le processus de chargement peut varier en complexité, selon la taille des données et la structure de la destination. Il existe deux approches principales :

- le chargement complet, où l'ensemble de données transformées est chargé en une seule opération.
- le chargement incrémental, qui ne transfère que les données modifiées ou ajoutées depuis le dernier chargement, optimisant ainsi les performances et minimisant l'interruption des opérations.

La réussite de cette étape dépendra de la précision dans la planification des séquences de chargement, la gestion des erreurs et la vérification post-chargement pour confirmer l'exactitude et la complétude des données dans l'entrepôt. Cela inclut également des considérations sur la sécurité des données pendant le transfert et leur stockage, assurant que les informations restent protégées conformément aux normes de conformité.

C. Outils de Business Intelligence

L'utilisation d'outils de Business Intelligence sera essentielle pour pouvoir analyser les données collectées via le processus d'ETL. Plusieurs outils de BI existent actuellement sur le marché et pour l'envergure de cette expérience, il serait plus pertinent de mettre en place une méthode d'analyse multicritères (M.A.M) afin de trouver l'outil correspondant le plus à notre besoin. Toutefois, un outil de BI qui revient souvent dans la recherche sur les ETL et que j'ai pu déjà utiliser semble convenir à notre besoin étant ses fonctionnalités avancées.

Cet outil développé par la société Microsoft© se nomme "Power BI" et se distingue comme un outil extrêmement pertinent pour cette mission, offrant une plateforme robuste et flexible pour l'analyse de données. Power BI est réputé pour sa capacité à traiter de grands volumes de données et à fournir des visualisations interactives et des tableaux de bord personnalisés. Cette capacité est essentielle pour analyser les complexes interactions entre les variables dépendantes et indépendantes de notre étude, telles que les incidents de sécurité IT, l'efficacité opérationnelle.. Les fonctionnalités avancées de Power BI en matière de visualisation de données permettent de transformer des données brutes en insights pertinents, rendant l'interprétation des résultats à la fois intuitive et accessibles pour les différents groupes de lecteurs de ces données.

L'un des principaux intérêts pour notre étude est que Power BI est compatible avec une large gamme de sources de données, ce qui est fondamental pour notre étude qui implique la collecte de données à partir de divers systèmes informatiques bancaires. Power BI propose aussi des options avancées de partage et de collaboration, facilitant le travail d'équipe entre les chercheurs et permettant une diffusion efficace des résultats de l'étude.

5. MÉTHODOLOGIE D'ANALYSE DES DONNÉES

Une fois après avoir collecté ces vastes ensembles de données, il faut pouvoir les analyser afin d'en faire ressortir des tendances permettant d'apporter des éléments de réponses à l'étude. Nous proposons dans cette étude une revue de différentes méthodes d'analyses statistiques permettant d'évaluer les impacts de l'IAG sur les risques IT ainsi que de distinguer des tendances significatives :

- Analyse descriptive : L'analyse descriptive constitue une méthode fournissant un aperçu global des tendances et variations au sein de notre ensemble de données. Cette phase implique un examen des mesures de tendance centrale - moyenne, médiane, et mode - qui nous renseignent sur la position centrale autour de laquelle les données se regroupent. Par exemple, la moyenne des incidents de sécurité IT au sein des banques utilisant l'IAG pourrait indiquer une tendance générale.

- Tests d’hypothèse :
  Les tests d’hypothèse permettent de déterminer s'il existe des différences statistiquement significatives entre les groupes de contrôle et expérimental, offrant une base solide pour l'évaluation de l'impact de l'IAG.
    - Test t pour échantillon indépendant : En comparant les moyennes de deux groupes sur des variables continues, cette méthode est pertinente pour analyser par exemple l'efficacité opérationnelle et les incidents de sécurité IT, permettant de déceler des différences significatives dans les performances ou les risques attribuables à l'usage de l'IA générative.
    - Test de Chi-carré : Ce test d’hypothèse s’applique sur des variables catégorielles (nombre fini de valeurs possibles). Un exemple d’utilisation de ce test dans notre étude pour porter sur l’adoption de nouveaux produits financiers en analysant si l'introduction de l'IAG dans un processus métier financier influence le taux d'adoption de nouveaux produits ou services financiers parmi les clients.

- Régression linéaire : Il s’agit d’une méthode statistique éprouvée et utilisée fréquemment dans la recherche pour étudier et modéliser la relation entre une variable dépendante et une ou plusieurs variables indépendantes. Dans le contexte de notre étude sur l'intégration de l'IA générative dans le secteur bancaire, cette technique nous permet d'analyser comment différents facteurs (variables indépendantes) tels que le niveau d'intégration de l'IA, la complexité des tâches automatisées, et le niveau de sécurité IT existant influencent des aspects clés des performances bancaires (variables dépendantes) comme l'efficacité opérationnelle, les incidents de sécurité, et la satisfaction client.

- Analyse de corrélation : L'analyse de corrélation est une méthode pouvant être employée pour examiner la force et la direction des relations entre les variables. Cela nous aidera à identifier les associations significatives entre l'intégration de l'IAG et les différentes mesures de performance et de risque.

Pour appuyer ces analyses, les données recueillies et transformées via le processus ETL seront exploitées à l'aide de Power BI, comme discuté précédemment. Cet outil de BI fournira les visualisations nécessaires pour interpréter les résultats statistiques et faciliter la communication des insights générés.

Ces méthodes statistiques, combinées à au logiciel Power BI, pourront offrir une compréhension approfondie de l'impact de l'IAG dans le secteur bancaire, permettant de tirer par la suite du protocole des conclusions basées sur des données probantes. L'application rigoureuse de ces techniques statistiques garantira la validité et la fiabilité et la reproductibilité des résultats, fournissant ainsi une base solide pour les décisions stratégiques.

6. ÉVALUATION DES RISQUES ET BÉNÉFICES

A. Méthode d’analyse des risques EBIOS Risk Manager

Il est primordial ici une fois après avoir récolté et analysé l’ensemble des données de l’étude de mettre en place une évaluation des risques IT/techniques dans les groupes expérimental et de contrôle afin de pouvoir apporter un élément de réponse à la première partie de notre hypothèse (**i**). L’évaluation des risques survient à ce moment stratégique dans le protocole pour la raison qu’après l’analyse de données cela lui permet d’appliquer des insights pertinents et des tendances identifiées sur les risques potentiels associés à l'IA générative. En disposant de données actualisées et spécifiques aux établissements bancaires, l'évaluation des risques devient plus précise et ancrée dans la réalité opérationnelle des banques.

Pour cela, nous proposons donc l’utilisation d’une méthode d’évaluation des risques créée par l’ANSSI du nom d’EBIOS Risk Manager. La méthode EBIOS offre un cadre systématique pour décomposer et évaluer les risques, assurant que tous les aspects, des menaces aux vulnérabilités, en passant par les impacts potentiels, sont considérés.

Cette rigueur méthodologique est particulièrement bénéfique après une phase d'analyse de données, car elle permet de lier directement les risques identifiés à des données spécifiques et mesurables. Par exemple, si l'analyse révèle une augmentation des tentatives de phishing avec l'introduction de l'IA, l'évaluation des risques peut se concentrer sur l'élaboration de contre-mesures spécifiques à ce type de menace. L'application de la méthode EBIOS Risk Management pour l'évaluation des risques associés à l'intégration de l'IA générative se décompose en plusieurs étapes clés, facilitant l'identification, l'analyse et le traitement des risques :

1. Contextualisation :

La première étape consiste à définir le contexte d'utilisation de l'IA générative dans le secteur bancaire, incluant la cartographie des actifs informationnels critiques à protéger. Dans notre hypothèse, les données client, les infrastructures IT, et les algorithmes d'IA constituent des actifs clés. Il sera essentiel d'identifier les menaces potentielles, telles que les menaces cyber ciblant les systèmes d'IA ou les violations de données.

2. Identification des risques :

Cette phase implique l'identification des événements redoutés pouvant affecter les actifs identifiés. Hypothétiquement, une analyse des données pourrait révéler une augmentation des tentatives de phishing ou de malware spécifiquement conçues pour exploiter les vulnérabilités des systèmes d'IA, ainsi qu'une potentielle exposition accrue aux violations de données personnelles.

3. Analyse des risques :

L'analyse des risques se concentrera sur l'évaluation de la fréquence d'occurrence des événements redoutés et de leur impact sur l'organisation. Par exemple, si l'analyse indique que l'intégration de l'IA générative augmente significativement le risque de violations de données, cela souligne un besoin critique de renforcer les mesures de sécurité des données ou d'abandonner le dispositif si cela ne s'avère pas rentable.

4. Traitement des risques :

Cette étape vise à définir des stratégies pour réduire, éliminer ou accepter les risques identifiés. En supposant que l'analyse de données révèle un risque accru de menaces cyber par exemple, les groupes bancaires pourraient envisager d'investir dans des solutions de sécurité avancées, comme des systèmes de détection et de réponse améliorée (IDS/IPS), ou de renforcer les protocoles de formation des employés sur la sécurité informatique.

5. Acceptation des risques :

La décision finale sur l'acceptation des risques devra être prise par la direction, en tenant compte des avantages opérationnels de l'IA générative par rapport aux risques identifiés. Si les bénéfices, tels que l'amélioration de l'efficacité opérationnelle et la personnalisation des services clients, surpassent significativement les risques, une stratégie d'acceptation mesurée peut être adoptée.

Si la méthode EBIOS RM est menée à bien dans les deux groupes, cela permet d'offrir un cadre rigoureux et isolant pour les risques IT associés à l'usage de l'IAG dans les établissements financiers. Cette approche méthodique aidera les groupes bancaires à naviguer de manière informée dans le paysage complexe des risques IT/techniques, assurant ainsi une intégration réfléchie de l'IAG dans leurs services qui maximisera les avantages tout en minimisant les risques potentiels.

B. Méthode d'évaluation des bénéfices

Pour évaluer aussi les bénéfices de l'intégration de l'IAG dans le secteur bancaire, il sera essentiel d'adopter une méthode rigoureuse qui permette d'appréhender de manière structurée et mesurable les avantages afin de vérifier la seconde partie de notre hypothèse initiale (**ii**). Cette approche comprend plusieurs étapes clés, inspirées de la même rigueur que la méthode EBIOS Risk Manager pour l'évaluation des risques, mais orientée vers l'identification et la quantification des bénéfices.

1. Définition des objectifs de bénéfices attendus :

La première étape consistera à définir clairement les objectifs de l'intégration de l'IAG dans les activités bancaires, tels que l'amélioration de l'efficacité opérationnelle, l'enrichissement de l'expérience client, ou l'innovation dans les services financiers. Il est important d'identifier les bénéfices attendus liés à chaque objectif, qu'ils soient quantitatifs (réduction des coûts, augmentation des revenus) ou qualitatifs (satisfaction cliente, image de marque) pour avoir une base comparative.

2. Cartographie des processus et fonctionnalités améliorées par l'IAG :

Cette étape implique l'analyse détaillée des processus opérationnels et des services où l'IAG est ou sera intégrée. L'objectif sera de cartographier comment l'IAG contribue spécifiquement à améliorer chaque processus ou service (ex : création de contenus, optimisation de services..), facilitant ainsi la mesure des bénéfices.

3. Analyse des données :

À cette étape, les données seront collectées via l'ETL qui a été mis en place pour évaluer l'impact réel de l'IAG sur les processus et services identifiés. Cela inclura des métriques tels que la performance opérationnelle, des enquêtes de satisfaction client, et des indicateurs financiers. L'analyse de ces données permettra par la suite de mesurer les bénéfices effectifs de l'IAG, fournissant une base solide pour l'évaluation.

4. Quantification des bénéfices :

Sur la base des analyses faites à l'étape précédente, cette étape visera à quantifier les bénéfices de l'intégration de l'IAG. Cela implique l'utilisation de modèles statistiques et économiques pour attribuer une valeur tangible aux améliorations observées, telles que l'augmentation des revenus ou la réduction des coûts opérationnels.

5. Évaluation des bénéfices en fonction des risques :

Pour conclure la méthode, une évaluation comparative des bénéfices et des risques devra être effectuée pour déterminer si l'intégration de l'IAG présente un avantage net pour la banque. Cette évaluation devra prendre en compte les coûts de mitigation des risques identifiés lors de l'évaluation des risques IT.

En adoptant une méthode structurée pour évaluer les bénéfices, les décideurs pourront à leur tour prendre des décisions éclairées sur l'intégration de l'IAG dans leurs opérations, en s'assurant que les avantages dépassent les risques potentiels et inhérents. Cette approche permet également d'identifier les domaines où l'IAG peut apporter une plus grande valeur ajoutée, orientant ainsi les futurs investissements en technologie de manière stratégique.

7. DISCUSSION DES CHOIX MÉTHODOLOGIQUES

La méthodologie adoptée au cours de ce protocole expérimental, combine l'analyse de données via des outils ETL et de BI avec l'évaluation des risques et bénéfices à l'aide de méthodes structurées comme EBIOS Risk Manager, cela a pour objectif d'offrir une approche qui se veut "par les risques" afin d'examiner l'intégration de l'IA générative. Cette démarche permet de capturer à la fois les avantages opérationnels potentiels et les risques IT/techniques associés, fournissant une vue équilibrée des implications de l'IA dans le secteur bancaire.

A. Implications des résultats

Notons ici que le protocole expérimental proposé ici est encore purement théorique sur l'intégration de l'intelligence artificielle générative dans le secteur bancaire et n'a donc pas encore été mené jusqu'à son terme en situation réelle, il est judicieux de reconnaître que les discussions autour des résultats et des implications sont purement spéculatives à ce stade. Cette démarche théorique sert à poser les bases pour une future recherche empirique autour de cette problématique.

Toutefois, cette étude a quand même eu pour but de soulever l'importance d'avoir une approche transversale et robuste pour pouvoir suivre les avantages potentiels qu'apporterait l'IAG ainsi que les risques associés. L'absence de données de par son caractère théorique doit renforcer la vigilance auprès des experts souhaitant s'en servir comme base d'étude.

B. Limites de l'approche méthodologique

Une des principales limites réside dans la dépendance aux données historiques et actuelles pour l'analyse. Cette approche proposée peut aussi ne pas capturer pleinement les potentielles évolutions futures de l'IAG et ses impacts sur les risques IT dans le secteur bancaire, étant donné la rapidité avec laquelle la technologie avance. Par ailleurs, la méthodologie pourrait sous-estimer les dimensions qualitatives, telles que l'effet de l'intégration de l'IAG sur la culture organisationnelle des banques ou la perception des clients.

D'autres limites sont à soulever aussi sur la pertinence et l'exhaustivité des indicateurs proposés permettant à la mesure des impacts de l'IAG, la présence de facteurs quantitatifs et qualitatifs est-elle suffisante pour pouvoir pleinement encadrer l'étude.

8. CONCLUSION

Pour conclure notre étude portant sur la problématique du caractère profitable de la balance bénéfice-risque de l'intégration de l'intelligence artificielle générative dans des processus métiers du secteur bancaire. Le but de cette étude a été de proposer un protocole expérimental utilisant des concepts de Business Intelligence ainsi que des méthodes d'analyse de risques (EBIOS RM) afin d'apporter une réponse à notre problématique initiale. Notre démarche, bien que théorique encore et non mise en pratique, jette les bases pour de futures recherches empiriques et offre un cadre pour l'évaluation des impacts de l'IAG.

L'intérêt principal de ce protocole expérimental ne réside pas uniquement dans son application au secteur bancaire et aux risques IT, mais aussi dans son potentiel d'adaptation à d'autres types de risques et à divers domaines d'activité. Par exemple, les organisations telles que la santé, la logistique, ou le commerce, où l'IAG gagne également du terrain, pourraient bénéficier d'une approche similaire pour évaluer et gérer les risques liés à l'intégration de l'IA dans leurs opérations. Cette adaptabilité souligne la valeur de la démarche comme un outil polyvalent pour la gestion des risques dans l'ère de la transformation numérique de notre société.

De plus, en mettant en lumière les bénéfices potentiels de l'IAG tout en identifiant de manière proactive les risques, notre étude encourage une intégration plus consciente et stratégique de l'IA dans les processus manipulant des données sensibles. Cela implique non seulement une évaluation continue des risques et des avantages à mesure que de nouvelles données deviennent disponibles, mais aussi une adaptation des stratégies de gestion des risques pour refléter les évolutions technologiques et réglementaires.

Enfin, cette réflexion pourra ouvrir des pistes pour de futures recherches, notamment sur l'importance d'approches interdisciplinaires intégrant des compétences en IA, en cybersécurité, en éthique, et en gestion des risques. L'exploration de ces domaines contribuera à une compréhension avancée et nuancée de l'intégration de l'IAG, facilitant ainsi la prise de décisions éclairées pour les acteurs du secteur bancaire et au-delà.

La perspective de rendre cette méthode applicable à d'autres familles de risques et secteurs activités enrichit son potentiel comme outil de référence dans la gestion des risques liés à l'IA, offrant une contribution significative au corpus de connaissances sur l'intégration de technologies émergentes dans divers secteurs économiques.

9. RÉFÉRENCES

[1] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2020. Generative adversarial networks. Commun. ACM 63, 11 (November 2020), 139–144. https://doi.org/10.1145/3422622

[2] Shabir, Ghualm. (2023). The Role of Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation.

[3] MANJALY, Joel, VARGHESE, Ranjana Mary, et VARUGHESE, Philip. Artificial Intelligence in the Banking Sector—A Critical Analysis. Shanlax International Journal of Management, 2021, vol. 8, no S1, p. 210-216.

[4] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial Intelligence for Cybersecurity : Literature Review and Future Research Directions. Information Fusion, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[5] MHLANGA, David. Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. International journal of financial studies, 2021, vol. 9, no 3, p. 39. https://doi.org/10.3390/ijfs9030039

[6] MIN, Alfonso. ARTIFICIAL INTELLIGENCE AND BIAS: CHALLENGES, IMPLICATIONS, AND REMEDIES. Journal of Social Research, 2023, vol. 2, no 11. https://doi.org/10.55324/josr.v2i11.1477

[7] Tad, M. C. S., Mohamed, M. S., Samuel, S. F., & J, D. M. (2023). Artificial Intelligence and Robotics and their Impact on the Performance of the Workforce in the Banking Sector. Revista de Gestão Social e Ambiental, 17(6), Article e03410. https://doi.org/10.24857/rgsa.v17n6-012

[8] BHARADIYA, Jasmin Praful. A comparative study of business intelligence and artificial intelligence with big data analytics. American Journal of Artificial Intelligence, 2023, vol. 7, no 1, p. 24.

[9] GEETHA, Keval. Param (2020). Data Analysis and ETL Tools in Business Intelligence. International Research Journal of Computer Science (IRJCS), 2020, vol. 7, p. 127-131.