Veille Technologique

SAADAOUI Yasmine

L'intelligence artificielle

SOMMAIRE

I) Introduction

Une avancée technologique est en marche : l'intelligence artificielle (IA) un outil capable de "reproduire des comportements humains, tels que le

raisonnement, la planification et la créativité". Elle s'impose aujourd'hui comme une révolution dans l'industrie informatique, en particulier dans le domaine industriel. En exploitant des algorithmes avancés, l'IA aide à des tâches complexes, à la prédiction de tendance mais aussi à la prise de décision autonome.

Dans un contexte d'innovation, l'IA représente bien plus qu'un simple outil : elle créée des méthodes de travail, aide à l'interactions homme et machine. De la cybersécurité en passant par les services cloud et du développement de logiciel, son but principal est de subvenir aux besoins de son utilisateur et donc de fournir au client une qualité accrue de service.

Cependant, cette révolution ne va pas sans enjeux : l'éthique, la sécurité et de compétences émettent des préoccupations, tandis que les entreprises cherchent à adopter ces technologies de manière responsable et durable. Cette adoption impose une réflexion sur l'impact de l'IA sur l'emploi, la sécurité des systèmes et l'éthique des développeurs. Cette veille technologique examine l'évolution de l'IA, ses applications actuelles, ses enjeux et les futures perspectives pour répondre à cette problématique.

II) Applications actuelles de l'IA dans l'industrie informatique

A) L'histoire de l'intelligence artificielle, de 1950 à aujourd'hui

L’histoire de l’IA débute pendant l’Antiquité avec des histoires et des mythes avec des humains conçus et modifié par des artisanats. Des philosophes et scientifiques comme Leibniz (1646-1716) ont tenter d’illustrer le processus.

C'est après la seconde guerre mondiale et l’invention des ordinateurs programmables (un ordinateur qui traite des informations définies par Alan Turing et qui fonctionne par la lecture séquentielle d’un ensemble d’instructions organisées en programmes qui lui font exécuter des opérations logiques et arithmétiques) que l’IA se concrétise. C'est par un mathématicien : John McCarthy (1927-2011) qui lors de la conférence de Dartmouth en 1956, devient disciple scientifique que l’IA se nomme ainsi.

Dans les années 80 l’IA connait des périodes d’engouements avec les systèmes experts (conçus pour simuler le raisonnement humain en utilisant des règles logiques préprogrammées et de reproduire les mécanismes cognitifs d’un expert dans un domaine particulier) mais connait également deux périodes nommées “hivers de l’IA” (1974-1980 et 1987-1993) avec des désillusions et de gel des financements.

En 2010 l’IA connait des progrès avec l’arrivée de l'apprentissage profond (sous domaine de l’IA qui utilise des réseaux neuronaux ayant de nombreuses couches pour résoudre des tâches complexes), avec l’augmentation des données disponibles, avec l’utilisation de processeurs graphiques qui multiplient les capacités de calcul et avec l’introduction de l’architecture transformateur (introduit en 2017, elle est principalement utilisée dans le domaine du traitement automatique des langues).

B) L'essor des systèmes experts et de l’apprentissage automatique (machine learning)

L’histoire de l’apprentissage machine est souvent lié à celle de l’IA. Il est considéré comme un moyen technique qui s’inspire de l’intelligence biologique, qui dès ses débuts, pousse les scientifiques à la création d’ordinateurs dotés d’une capacité d’apprentissage et d’autoadaptation.

En 1959 le terme “machine learning” devient populaire grâce aux travaux du chercheur Arthur Samuel en présentant un programme capable de jouer aux dames et d’apprendre à mesure que le jeu évolue à partir de données stockées dans sa mémoire.

Dans les années 70 et 80, les systèmes experts ont marqué une avancée significative dans le domaine de l'IA. Cela repose sur deux phases : estimer un modèle à partir de données, ce sont les observations, disponibles en nombre infini lors de la phase de conception du système. Ceci consiste à résoudre une tâche : traduire un texte, estimer une probabilité, reconnaitre la présence d'un chat sur une photo. C'est une phase dite d'apprentissage. La deuxième phase est la mise en production : le modèle étant déterminé, de nouvelles données sont ajoutées pour correspondre à la tâche souhaitée.

III) L'impact des réseaux profonds et de l'IA générative (comme ChatGPT)

A) Les réseaux neuronaux profonds : une révolution dans le traitement des données

Les réseaux neuronaux constituent un modèle de machine learning qui prend des décisions de manière similaire au fonctionnement du cerveau humain pour analyser des problèmes et les résoudre. Les réseaux neuronaux sont constitués de nœuds, ou neurones avec une couche d'entrée et sortie. Ces réseaux se basent sur les données d'entrainement et une fois la précision optimale atteinte, ce sont de puissants alliés des domaines de l'informatique et de l'intelligence artificielle ; une tâche avec des recherches humaines qui pourrait prendre des heures, ne prendrait que quelques minutes. Google est un exemple parmi tant d'autre.

B) L’IA générative : la création automatisée de contenu

L’IA générative est une technologie capable de créer des contenus à partir de modèle d’apprentissage profond aidé par un grand nombre de modèle. Ces modèles génèrent de nouvelles données et grâce à l’IA discriminative, tri les données. Aujourd’hui cette avancée est utilisée pour générer du texte ou des images, du code etc... De nos jours beaucoup d’IA générative ont vus le jour (ChatGPT, DALL-E d’OpenAI, GitHub CoPilot) pour automatiser les tâches courantes pour gagner en efficacité et aider les développeurs à créer des contenus plus facilement (rédaction d’article ou même de code informatique).

C) Les impacts et défis de l’IA générative

L’IA générative transforme de nombreux secteurs d’activité : santé, finance, recherche et la sécurité. C'est aussi un défi dans le monde de l’éducation. Toutefois, ces avancées ne sont pas sans relever de nombreuses questions :

- L'impact sur les emplois : l’automatisation créative pourrait transformer des professions dans le domaine de la création de contenu.

- Défis éthiques et biais : les modèles comme GPT peuvent reproduire des biais présents dans leur données d’entrainement.
  Exemple : si un modèle est formé sur des textes où les femmes sont associées à des métiers comme le secrétariat et les hommes à des métiers scientifiques, il risque de reproduire cette association lorsqu’on lui demande des prédictions ou des réponses sur les professions

- Sécurité et désinformation : la capacité à générer du texte réaliste pourrait être utilisée pour des campagnes de désinformations

- Les couts énergétiques et environnementaux sur lesquels elle repose. Une seule requête ChatGPT-4 consomme près de 233g de CO_2, la création d’une image en haute définition par une IA consomme autant d’énergie

VI) L’IA et la cybersécurité : enjeux et défis

A) Les enjeux de l’IA dans la cybersécurité

L’utilisation de l’IA en cybersécurité est une avancée majeure pour protéger les systèmes informatiques de certaines menaces. Nos outils traditionnels ne permettent plus de suivre le rythme, l’IA permet de renforcer cette sécurité. L’IA à travers le “machine learning”, analyse des tonnes de données en temps réel et :

- Détecte les comportements suspects
- Identifie les anomalies et anticipes les attaques
- Apprend et adapte les défens

Au lieu d’attendre l’intervention humaine, l’IA s’occupe du problème pour éviter la propagation d’un malware. Les systèmes peuvent améliorer la gestion des droits d’accès en utilisant des méthodes biométriques comme la reconnaissance faciale, empreintes digitales... Mais malgré ses avantages l’IA possède de nombreux défis. Les attaquants utilisent aussi l’IA pour rendre leurs attaques plus efficaces :

- Phishing automatisé : la création de courriels de phishing très réalistes et pouvant être pérsonalisés
- Malware polymorphe : Grâce à des algorithmes, les malwares peuvent s’adapter pour échapper aux systèmes de détection

Le système de sécurité d’une IA peut créer des alertes de faux positifs, une alerte entrainant une interruption de processus inutile. Si les modèles sont baisés cela peut entrainer le négligemment provenant de certaine menace. Ces systèmes aussi, nécessitent une grande quantité de données pour être prêt à toute menace. Cela pose un problème sur la confidentialité des données utilisées et la transparence des décisions prises par des algorithmes.

IV) Conclusion

L’IA est devenue un moteur innovant dans l’industrie informatique et au-delà, transformant des domaines aussi variés que la santé, les transports, les finances et la cybersécurité. Ses applications actuelles vont de la reconnaissance au service client.

L’essor des réseaux neuronaux a marqué une avancée en permettant aux machines de traiter des informations comme les images et le langage humain. Les modèles génératifs vus précédemment représentent une avancée avec leurs capacités à générer du texte, des images et même de la musique pouvant révolutionner les métiers créatifs et d’en augmenter la productivité. Cependant cela entraine des défis tel que l’éthique, de biais et de sécurité.

En cybersécurité l’IA est un outil pour la détection de malware et automatise la réponse aux attaques mais cela nécessite une vigilance accrue en vue des défaillances qu'il pourrait y avoir.

En conclusion l’IA continue d’évoluer apportant des bénéfices mais également de nouvelles responsabilités. Il est tout de même impératif à mesure que les recherche avance de minimiser les risques de l’IA.

https://www.enseignementsup-recherche.gouv.fr

https://drane-versailles.region-academique-idf.fr

https://www.freelance-informatique.fr

https://fr.wikipedia.org

https://www.ibm.com

https://www.redhat.com

https://www.techniques-ingenieur.fr