L'ECONOMISTE

Le Cercle des Experts

Sécuriser l'IA dans le Cloud : Enjeux et Bonnes Pratiques

Par Taieb DEBBAGH | Edition N° :6533 Le 08/06/2023 | Partager

Docteur en SI Paris-Dauphine, Ex. Secrétaire Général du département ministériel en charge des TI, il a été à l'origine de la mise en place du maCERT, de la loi 09-08 et de la CNDP. Taieb Debbagh a supervisé le Plan « Maroc Numeric 2013 » et en particulier sa composante « Confiance Numérique ». Lors du lancement en 2007, de l'initiative « Global Cybersecurity Agenda » (UIT), il a été membre du « High Level Expert Group » et a présidé la commission relative aux structures organisationnelles. Suite aux travaux de cette commission, il a proposé un référentiel de bonnes pratiques « National Cybersecurity Management System » adopté à l'unanimité lors de la conférence Plénipotentiaire de l'UIT – Mexique 2010. (Ph. TD)

L'intelligence artificielle (IA) joue un rôle croissant dans le domaine du cloud, offrant des avantages significatifs en termes d'efficacité, d'automatisation et de prise de décision. Cependant, avec l'adoption rapide de l'IA dans le cloud, il est essentiel de garantir la sécurité des algorithmes et des données. Cette tribune explore les défis spécifiques liés à la sécurisation de l'IA dans le cloud et propose des bonnes pratiques pour atténuer les risques.

I- Pas d'IA sans Cloud

Le Cloud et l'IA sont deux technologies distinctes mais interconnectées qui se complètent :

- Infrastructure pour l'IA : Le cloud fournit l'infrastructure évolutive nécessaire aux applications d'IA;

- Stockage et traitement des données : les algorithmes d'IA s'appuient fortement sur de grands ensembles de données pour la formation et l'inférence ;

- Évolutivité et élasticité : Le cloud permet de prendre en charge les besoins de l'IA en ressources en fonction de facteurs tels que la taille des données, la complexité du modèle et la demande des utilisateurs ;

- Développement et déploiement de l'IA : Les plateformes cloud offrent des services et des outils liés à l'IA, tels que des cadres de développement, des plateformes d'apprentissage automatique et des modèles pré-entraînés ;

- **Calcul distribué et parallélisme :** Les tâches de l'IA, en particulier la formation de modèles complexes, peuvent nécessiter beaucoup de temps et de calcul, qui sont offerts par le Cloud ;

- **Applications d'IA en temps réel :** Le cloud facilite le déploiement de modèles pour des applications en temps réel ;

- Optimisation des coûts : Le cloud permet d'éviter les investissements en matériel coûteux en utilisant le modèle SaaS (Software as a Service).

En bref, le Cloud fournit l'infrastructure, l'évolutivité, le stockage et les services nécessaires pour prendre en charge le développement, le déploiement et l'évolutivité des applications d'IA. Il permet aux organisations d'exploiter la puissance de l'IA sans avoir besoin d'investissements importants dans l'infrastructure, accélérant ainsi l'innovation et démocratisant l'accès aux capacités de l'IA.

Si l'intelligence artificielle joue un rôle croissant dans le domaine du cloud, son adoption rapide nécessite de garantir la sécurité des algorithmes et des données (Ph. AFP)

II- Les défis de la cybersécurité

Le déploiement de l'intelligence artificielle (IA) dans le cloud présente des défis de cybersécurité :

- Confidentialité des données : L'IA nécessite souvent l'accès à de grandes quantités de données, ce qui soulève des préoccupations concernant la confidentialité ;

- Intégrité des données : Les données utilisées pour entraîner les modèles d'IA peuvent être exposées à des risques de falsification ou de manipulation malveillante ;

- Vulnérabilités des modèles d'IA : Ils peuvent être vulnérables notamment aux attaques de perturbation, d'injection de données, et de biais.

- Accès non autorisé aux ressources : Lorsque l'IA est déployée dans le cloud, il est essentiel de s'assurer que seules les personnes autorisées ont accès aux ressources et aux données associées ;

- Conformité réglementaire : Le déploiement de l'IA dans le cloud peut être soumis à des réglementations spécifiques, telles que la loi 05-20 (Cybersécurité), la loi 09-08 (Protection des données personnelles, le RGPD (Règlement général sur la protection des données). Il est important de s'assurer que les activités d'IA dans le cloud sont conformes à ces réglementations.

III- Comment lever ces défis ?

Pour améliorer la sécurité de l'IA dans le cloud, plusieurs techniques et technologies peuvent être mises en œuvre :

- Chiffrement des données : En chiffrant les données stockées ou en transit dans le cloud, on réduit les risques d'accès non autorisé et on protège la confidentialité ;

- Gestion des identités et des accès : En mettant en place des mécanismes d'authentification forte, de contrôle des privilèges et de suivi des accès, on limite les risques d'accès non autorisé aux ressources de l'IA ;

- Vérification et traçabilité des modèles d'IA : En enregistrant et en suivant les différentes étapes du processus de développement et de déploiement des modèles d'IA, on peut détecter toute manipulation ou altération indésirable ;

- Détection des attaques et des anomalies : L'utilisation de techniques de « Machine Learning » pour analyser les schémas d'utilisation, les journaux d'événements et les anomalies de comportement peut aider à détecter les attaques potentielles ;

- Formation et sensibilisation des utilisateurs : Elles sont essentielles pour réduire les risques liés à l'IA dans le cloud. Les utilisateurs doivent être conscients des meilleures pratiques de sécurité, de l'importance de la protection des données sensibles et des risques associés à l'IA.

IV– IA, Cloud et Sécurité

En résumé, le cloud est essentiel pour l'IA en raison de sa capacité à fournir des ressources évolutives, des capacités de calcul puissantes et une infrastructure flexible. Cependant, il est important de garantir la sécurité de l'IA dans le cloud. En suivant les bonnes pratiques citées plus haut, vous pouvez améliorer la sécurité de l'IA dans le cloud et minimiser les risques potentiels associés à son déploiement. Il est important de noter que la sécurité de l'IA dans le cloud est un effort continu, nécessitant une vigilance constante et une adaptation aux nouvelles menaces.

*Dans ma précédente tribune (cf. **www.leconomiste.com**), Ghita Mezzour, ministre de la Transition numérique et de la Réforme de l'Administration, en abordant l'IA et le cloud, a déclaré « ce sujet est positionné comme un axe majeur et transverse dans la nouvelle stratégie digitale 2030 » (Ph. DR)*

Cloud et Transition Numérique

Le cloud est essentiel pour une transition numérique réussie, offrant aux entreprises une infrastructure IT agile, évolutive et sécurisée. Avec un marché mondial estimé à près de 1.000 milliards de dollars d'ici 2025, l'adoption du cloud permettra au Maroc et à l'Afrique de renforcer leur compétitivité. Cette transition requiert le soutien du top management des entreprises et des partenaires de confiance pour une expertise et un accompagnement adapté.
Orange Maroc propose sa solution de cloud de confiance, basée sur des Data centers locaux certifiés et sécurisés ainsi que le support des 3000 experts d'Orange Cyberdéfense, un leader mondial en services de cybersécurité. En tant que partenaire de confiance, Orange accompagne les entreprises marocaines à chaque étape de leur migration vers le cloud.

Déclaration de M. Brahim Sbai – vice-président Sales – Orange Maroc (recueillie par TD, le 5 juin 2023)

Adoption de l'IA passe par la sécurité du Cloud

Un état des lieux du digital au Maroc permet de dégager d'importants acquis réalisés, et de mettre le doigt sur des freins rencontrés. Aux enjeux et challenges de la transition numérique s'ajoutent désormais une accélération de l'adoption des technologies émergentes telles que l'intelligence artificielle (IA) qui démontre un grand potentiel aux domaines d'application multiples : santé, sécurité, transport, performance des services administratifs, éducation…
L'adoption de l'IA ne pourra se faire pleinement tant que les enjeux fondamentaux de la sécurité et de souveraineté du cloud n'auront pas été mis en œuvre. Celle-ci reposera sur la capacité des organisations de créer la confiance quant à son usage : éthique, confiance des informations générées par l'IA, sécurité des données…PwC prévoit d'investir 1 milliard de dollars dans l'IA générative d'ici 2026. Cette transition nécessite un effort significatif permettant l'adoption en toute maîtrise de ses technologies : recrutement et formation des collaborateurs, déploiement des technologies, définition de cadres de gouvernance et de contrôle…

Déclaration de Jamal Basrire, Associé Leader Cloud Transformation & Cyber pour la France et le Maghreb - PwC (recueillie par TD, le 5 juin 2023)

La sécurité des systèmes d'IA dans le cloud

Le déploiement des technologies basées sur l'intelligence artificielle (IA) dans le cloud introduit inévitablement de nouvelles vulnérabilités spécifiques. En effet, l'IA est sensible à différents types d'attaques qui lui sont propres, tels que les attaques d'empoisonnement, de manipulation et d'inférence d'appartenance. Il est donc important de réduire ces vulnérabilités pour protéger les systèmes d'IA et assurer la confiance.
Pour aider à faire face à cette problématique, l'Université du Québec en Outaouais (UQO) a intégré dans ses programmes de formation des cours axés sur la sécurité de l'infonuagique (Cloud) et sur la conception de systèmes intelligents sécurisés. Son Laboratoire de recherche en sécurité informatique (LRSI), dirigé par Kamel Adi, traite en particulier la cybersécurité des systèmes à base d'IA, l'utilisation de l'IA pour construire des systèmes autonomes de cyberdéfense. Le professeur Stéphane Gagnon étudie de son côté l'automatisation des processus décisionnels en gestion, surtout par l'utilisation des règles et du raisonnement sémantique, ainsi que les ontologies et les graphes de connaissances pour modéliser et comprendre les risques complexes. Dans tous ces travaux, la sécurité des systèmes d'IA est centrale, et leur implémentation requièrent l'intégration de solutions cloud.

Déclaration de Reda Bensouda, conseiller en innovation numérique et cybersécurité, Université du Québec en Outaouais (recueillie par TD, le 5 juin 2023)