

ChatGPT : Quand les erreurs de code se faufilent pour détruire nos logiciels

Une équipe de l'université américaine de Purdue vient de mettre en évidence les limites de ChatGPT dans la programmation. Les chercheurs appellent l'industrie et les DSI à mettre en place des garde-fous pour limiter les risques. Selon une récente étude d'une équipe de l'université américaine de Purdue (Indiana), ChatGPT donne des réponses erronées à des questions de programmation logicielle une fois sur deux.

CIO a interrogé les chercheurs Samia Kabir, Bonan Kou, David Udo-Imeh et le professeur assistant Tianyi Zhang à l'origine de cette étude encore en prépublication. Ces derniers ne prônent pas l'interdiction des IA génératives dans la programmation, mais invitent l'industrie du logiciel et les DSI à réfléchir aux garde-fous à mettre en place pour limiter les risques.

Les chercheurs ne sont pas surpris par les résultats de leur étude. Ils s'attendent à des erreurs factuelles et d'incohérences de la part de ChatGPT, car des études antérieures ont montré que ces modèles sont susceptibles de générer des réponses incorrectes. Il est tout de même surprenant qu'une partie non négligeable des participants à l'étude (34%) ait préféré ChatGPT en raison des informations complètes et d'apparence humaine que cet outil fournit. Cela pose des questions sur la qualité des réponses fournies par d'autres sites de questions/réponses en ligne, comme Stack Overflow, qui ont été critiqués pour leurs réponses toxiques et peu accueillantes.

La programmation étant un domaine déterministe, on pourrait

penser que les LLM s'en sortiraient mieux avec le langage naturel. Cependant, répondre à des questions de programmation est très différent de générer du code. Les questions de programmation sont rédigées en langage naturel et impliquent une expertise et une compréhension approfondie des concepts et du langage de programmation. Il est donc plus difficile de répondre à des questions de programmation qu'à des questions courantes.

Les utilisateurs accordent une telle confiance aux réponses de l'IA générative principalement parce qu'elles semblent plausibles, complètes et polies. Les réponses de ChatGPT sont plus formelles, analytiques et montrent des efforts pour atteindre les objectifs fixés, ce qui peut tromper les utilisateurs. Cependant, il est important de rester vigilant et de ne pas trop compter sur l'IA. Les développeurs de logiciels doivent passer plus de temps à examiner le code et les réponses générées.

L'IA générative entre de plus en plus dans le domaine de la programmation logicielle au sein des entreprises. Cela peut entraîner des erreurs dans les codes ou réponses générées par les LLM, comme l'utilisation d'API non sécurisées ou obsolètes. Les entreprises doivent donc développer des mécanismes de régulation et organiser des sessions de formation pour éduquer les développeurs sur les limites des outils basés sur l'IA.

L'introduction de l'IA générative dans les cursus universitaires orientés sur la programmation transforme l'enseignement. Les étudiants utilisent ChatGPT pour générer du code et répondre à des questions de programmation, rendant les connaissances plus accessibles. Cependant, l'évaluation des étudiants devient plus difficile, car il est difficile de déterminer si une solution est basée sur les réponses de ChatGPT ou non.

Malgré cela, les chercheurs ne sont pas inquiets quant à

l'apprentissage des étudiants. Les réponses de ChatGPT contenant souvent des erreurs, les étudiants doivent les inspecter et les corriger, ce qui les aide à apprendre. Les programmes universitaires devraient donc se concentrer davantage sur l'enseignement de concepts fondamentaux et créatifs que ChatGPT a du mal à comprendre. Les devoirs et examens de programmation devraient évaluer la capacité des étudiants à comprendre et résoudre des problèmes, plutôt que leur capacité à mémoriser des solutions et des règles de syntaxe.

Source : www.lemondeinformatique.fr