Sophos stellt Tuning-Tool für große Sprachmodelle als Open-Source-Programm zur Verfügung

Große Sprachmodelle (Large Language Models, LLMs) haben das Potenzial, die Arbeitslast zu automatisieren und zu reduzieren, einschließlich der von Cybersicherheitsanalysten und Incident Respondern. Generischen LLMs fehlt jedoch das domänenspezifische Wissen, um diese Aufgaben gut zu bewältigen. Auch wenn sie mit Trainingsdaten erstellt wurden, die Cybersicherheitsressourcen enthalten, reicht dies oft nicht aus, um spezialisiertere Aufgaben zu übernehmen, die aktuelles und in einigen Fällen auch proprietäres Wissen erfordern, um sie gut auszuführen – Wissen, das den LLMs bei ihrer Ausbildung nicht zur Verfügung stand.

Es gibt mehrere bestehende Lösungen für das Tuning von „Standard"-LLMs (unveränderte LLMs) für bestimmte Arten von Aufgaben. Doch leider waren diese Lösungen für die Anwendungsarten von LLMs, die Sophos X-Ops verwendet, unzureichend. Aus diesem Grund hat das SophosAI-Team ein Framework zusammengestellt, das DeepSpeed nutzt, eine von Microsoft entwickelte Bibliothek, mit der die Inferenz eines Modells mit (theoretisch) Billionen von Parametern trainiert und abgestimmt werden kann. Dabei wird die Rechenleistung und die Anzahl der beim Training verwendeten Grafikprozessoren (GPUs) erhöht. Das Framework steht unter Open-Source-Lizenz zur Verfügung und ist in der GitHub-Repository von Sophos zu finden.

Framework-Version als Open Source verfügbar

Damit ein LLM seine volle Wirkung entfalten kann, müssen alle seine Parameter vorab trainiert werden, um das firmeneigene Wissen eines Unternehmens zu erlernen. Dieses Unterfangen kann ressourcenintensiv und zeitaufwendig sein. Deshalb hat Sophos sich für sein Trainingsframework, das in Python implementiert wurde, an DeepSpeed gewandt. Die Version des Frameworks, die Sophos als Open Source freigibt, kann im Amazon Web Services SageMaker Service für maschinelles Lernen ausgeführt aber auch an andere Umgebungen angepasst werden. Trainingsframeworks (einschließlich DeepSpeed) ermöglichen die Skalierung großer Modelltrainingsaufgaben durch Parallelität.

Obwohl viele Teile des Frameworks nicht neu sind und auf bestehende Open-Source-Bibliotheken zurückgreifen, hat das SophosAI-Team einige der wichtigsten Komponenten zusammengefasst, um die Nutzung zu erleichtern. Zum Zeitpunkt seiner Erstellung war dieses Tool-Repository das erste, das Training und beide DeepSpeed-Inferenztypen (DeepSpeed-Inferenz und ZeRO-Inferenz) in einem konfigurierbaren Skript kombiniert. Es war auch das erste Repository, das einen benutzerdefinierten Container für die Ausführung der neuesten DeepSpeed-Version auf dem SageMaker von Amazon Web Service erstellte. Und es war das erste Repository, das verteilte Skripte ausführt.

Weitere technische Details sind im folgenden Sophos-Artikel aufgeführt: DeepSpeed: a tuning tool für large language models

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de