Edgeless Systems

Confidential Computing & AI für Sicherheit und Verteidigung

Sensible Daten in Cloud und KI-Anwendungen nachweisbar schützen.

Problemstellung

IT-Sicherheit und Datenschutz sind zentrale Hürden für die Nutzung von Cloud- und KI-Diensten im Bereich Sicherheit und Verteidigung.

Moderne Cloud-Infrastrukturen bedeuten, dass IT-Dienste aus Rechenzentren Dritter bereitgestellt werden. Diese Infrastruktur wird mit anderen Nutzern geteilt und – auch bei deutschen Clouds – von vielen, häufig unbekannten, Personen verwaltet.

Herkömmliche Sicherheitskonzepte basieren auf Zugriffskontrollen und der Verschlüsselung von Daten während Speicherung und Übertragung. Diese Maßnahmen verhindern jedoch keinen Zugriff Dritter über die (Cloud-)Infrastruktur, weil Daten für die Verarbeitung im Klartext vorliegen müssen. Anbieter und potenzielle Angreifer könnten daher Zugriff auf die Daten erlangen. Ein Cloud-Administrator könnte beispielsweise seinen Zugriff missbrauchen oder ein Mitnutzer könnte Sicherheitslücken ausnutzen und unbefugt auf Daten anderer Mandanten zugreifen.

Die Nutzung von Cloud-Diensten ist wegen Skalierbarkeit, Effizienz und Redundanz – insbesondere im Kontext von KI-Anwendungen – zentral für die Digitalisierung in sicherheitskritischen Bereichen. Wie können sie nachweisbar sicher genutzt werden?

Lösung

Confidential Computing ermöglicht eine nachweisbar vertrauliche Datenverarbeitung – sogar für KI-Anwendungen und in der Cloud.

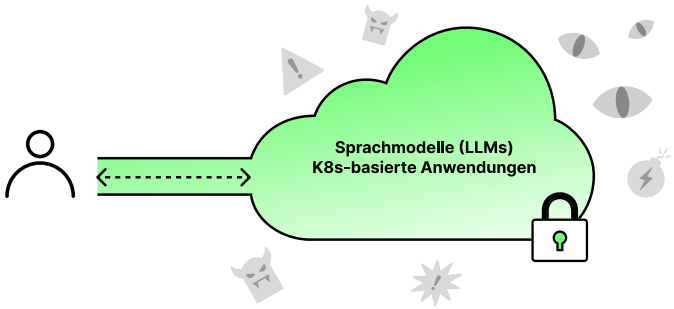
Confidential Computing kombiniert Funktionen moderner CPU- und GPU-Hardware mit optimierter Software. Der Prozessor verhindert ein Auslesen der Daten durch durchgehende Verschlüsselung, auch während der Verarbeitung (Laufzeitverschlüsselung) und stellt ein kryptografisches Zertifikat aus, das Vertraulichkeit, Integrität und Authentizität der Daten bestätigt (Fernattestierung).

Laut einem aktuellen Datenschutzgutachten kann Confidential Computing bei richtiger Umsetzung als Methode zur Anonymisierung personenbezogener Daten betrachtet werden.

Die Confidential-Computing-Software von Edgeless Systems sorgt dafür, dass Vertraulichkeit und Attestierbarkeit lückenlos, einfach und skalierbar einsetzbar sind – beispielsweise für Kubernetes-basierte Anwendungen oder für Sprachmodelle (LLMs) „as-a-service“ aus der Cloud.

Confidential Computing schützt sensible Daten vor

- **Kompromittierter Infrastruktur**, etwa Bedrohungen durch kompromittierte Hosts
- **Insider Bedrohungen**, z.B. bei Zugriff durch Rechenzentrumsadministratoren oder Co-Tenants
- **Bösartigen Updates**, da Fernattestierung verifizierte Software-Updates ohne Manipulation sicherstellt
- **Physischem Verlust**, z.B. bei Verlust oder Beschlagnahmung von Hardware/mobiler Einheiten.



Ausgewählte Produkte und Referenzen

AIRBUS

Sichere KI-gestützte Kommando- und Kontrollsysteme für den Einsatz im Gefechtsfeld

Für die Digitalisierung moderner Streitkräfte arbeitet Airbus an einem dezentralen, KI-gestützten IT-System für den Einsatz im Combat Cloud-Kontext. Ziel ist es, missionskritische, sensible Daten in Echtzeit zwischen verschiedenen Plattformen wie Fahrzeugen, Drohnen oder Gefechtsständen sicher auszutauschen – auch unter schwierigen Bedingungen am taktischen Rand des Einsatzgebietes. In einem gemeinsamen Proof of Concept mit Edgeless Systems wurde eine containerisierte Kommando- und Kontrollanwendung (C2-System) in einer Confidential-Computing-Umgebung abgesichert. Selbst bei physischem Verlust der Hardware in mobilen Rechenzentren bleibt die Vertraulichkeit der Daten gewahrt.

Privatemode AI: LLMs mit Ende-zu-Ende-Verschlüsselung

Für den Einsatz von KI-Sprachmodellen (LLMs) in sicherheitsrelevanten Bereichen zahlreiche Anwendungsfälle – etwa die automatisierte Auswertung von Meldungen oder die Erstellung bzw. Übersetzung sicherheitsrelevanter Dokumente. Cloud-Dienste sind aus Geheimhaltungs- und Datenschutzgründen häufig ausgeschlossen, während On-Prem-Installationen teuer und komplex sind.

Privatemode AI ist der erste KI-Dienst, mit dem Daten immer und nachweisbar verschlüsselt sind – Cloud-Anbieter, Service-Provider und Entwickler der Modelle haben keinen Zugriff. Privatemode bietet führende Modelle und kann einfach via API integriert oder als Desktop-App verwendet werden.

Confidential Computing für datenschutzkonforme Cloud-Anwendungen

Die BWI möchte (KI-) Anwendungen sicher in der Cloud betreiben können. Bisher müssen die meisten Anwendungen aus Sicherheits- und Datenschutzgründen auf eigener Infrastruktur gehosted werden. Mit Confidential Computing Software von Edgeless Systems wurden deshalb zwei containerisierte Kollaborations-Tools (BWmessenger, Collaboard) testweise auf der Azure Cloud betrieben. Es konnte gezeigt werden, dass Funktionalität und Performance der Anwendungen durch die zusätzliche Verschlüsselung nicht beeinträchtigt werden. Ein von der BWI beauftragtes Datenschutzgutachten zeigt zudem, dass Daten mit Confidential Computing de facto anonym in der Cloud verarbeitet werden.

Weitere Informationen finden Sie unter edgeless.systems

Über Edgeless Systems

Edgeless Systems ist ein deutsches Cybersecurity-Unternehmen, das die Public Cloud zum sichersten Ort für sensible Daten macht. Mit weltweit führenden Lösungen für Confidential Computing hebt Edgeless Systems Datensicherheit für Cloud- und KI-Anwendungen auf ein neues Niveau und ermöglicht die verschlüsselte Verarbeitung sensibler Daten mit hoher Skalierbarkeit.

Edgeless Systems arbeitet mit renommierten Firmen wie Capgemini, IBM, Adesso, Nvidia und der Schwarz Gruppe zusammen. Das Unternehmen veranstaltet die jährliche Open Confidential Computing Conference (OC3), u.a. mit den CTOs von Microsoft, AMD und Intel, und ist Mitglied des Confidential Computing Consortiums.