Edgeless Systems

Confidential Computing & AI für das Gesundheitswesen

Sensible Daten nachweisbar sicher in der Cloud

Problemstellung

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

Public Clouds bedeuten, dass IT-Dienste aus Rechenzentren Dritter bereitgestellt werden. Diese Infrastruktur wird mit anderen Nutzern geteilt und – auch bei deutschen Clouds – von 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 und Effizienz – insbesondere im Kontext von KI-Anwendungen – zentral für die Digitalisierung der Gesundheitsbranche. Wie können sie nachweisbar sicher genutzt werden?

Lösung

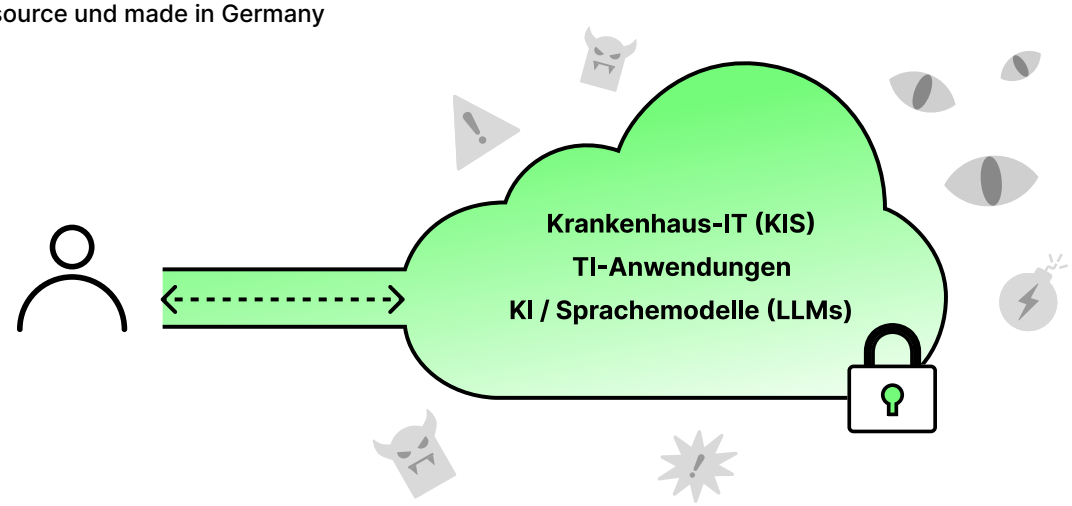
Confidential Computing ermöglicht eine nachweisbar vertrauliche Datenverarbeitung in der Cloud – auch für KI.

Confidential Computing kombiniert Funktionen moderner 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. Edgeless Systems bietet:

- Daten immer verschlüsselt (sogar “in use”)
- Nachweisbarer Betreiberausschluss
- Gematik-zugelassen in der E-Patientenakte
- Cloud-agnostisch, ohne Anbieter Lock-in
- Open-source und made in Germany



Anwendungsbeispiele

Elektronische Patientenakte: Sichere Daten für Millionen Versicherte

In Deutschland muss jede Krankenkasse ihren Kunden eine elektronische Patientenakte (ePA) bereitstellen. Über eine App sind alle Daten, wie Medikationshistorien und Untersuchungsberichte, zugänglich. Aufgrund der Sensibilität dieser Daten fordert die Gematik einen strikten Betreiberausschluss mittels „vertrauenswürdiger Ausführungsumgebung“. Durch den Einsatz von Confidential-Computing-Hardware und Software von Edgeless Systems wird gewährleistet, dass Backend-Infrastrukturanbieter auf keine Patientendaten zugreifen können.

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

Für den Einsatz von KI-Sprachmodellen (LLMs) gibt es im Gesundheitswesen viele Anwendungsfälle, z. B. die automatisierte Arztbrieferstellung oder das Übersetzen von Patientenakten. Cloud-Dienste sind aus Datenschutzgründen meist ein No-Go und On-Prem-Installationen sind teuer und komplex.

Privatemode AI ist der erste KI-Dienst, mit dem alle 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.

Jetzt 14 Tage kostenlos testen!

privatemode.ai

Universitätsklinikum Freiburg: In der Public Cloud mit Confidential Kubernetes

Das eigene Rechenzentrum hat Kapazitätsgrenzen erreicht und insbesondere für den Einsatz von GPUs für KI-Anwendungen sind Cloud-Lösungen im Fokus. Patientendaten müssen in der Cloud bestmöglich vor unbefugtem Zugriff geschützt werden. Daher setzt das Klinikum auf Constellation, das vollständig verschlüsselte Kubernetes von Edgeless Systems. Mit der CNCF-zertifizierten Kubernetes-Lösung können Anwendungen wie ein FHIR-Server in verschiedenen Clouds skaliert werden, während Patientendaten nachweisbar vor Angriffen aus der Cloud geschützt.

Mit der neuen Spezifikation Healthcare Confidential Computing (HCC) hat die Gematik den Grundstein dafür gelegt, standardisierte TI-Anwendungen zukünftig mit VAU sogar aus Public Clouds bereitzustellen.

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.