Mit dezentraler KI zu sichereren Prozessen

Am Beispiel der automatisierten Überwachung von Umspannanlagen für Energieversorger

Mirko Düssel, Samuel T. Stähle, ChatGPT 4.0 (Deutsch) am 2. Oktober 2024

Inhalt

Einleitung

Im September 2024 haben Samuel Stähle, CEO PowerBrain.Shop®, Mirko Düssel, Mirko Düssel & Co. Interdisziplinäre Unternehmensberater, und ChatGPT4o die Frage diskutiert, wie automatisierte Überwachung auf der Basis von KI-Lösungen zu effizienteren und sichereren Prozessen führt. Die Autoren haben bereits seit vielen Jahren Praxiserfahrungen bei der Realisierung von KI-Anwendungen in den Bereichen Maintenance, Process Engineering und Strategy gesammelt und helfen Unternehmen und Organisationen das konkrete Potenzial von künstlicher Intelligenz (KI) zu erkennen und zu nutzen. Die gewonnenen Erkenntnisse werden am Beispiel der Automatisierung von Umspannanlagen bei Energieversorgern reflektiert und mit ChatGPT diskutiert.

Die Anforderungen an Infrastrukturbetreiber wie Energieversorgungsunternehmen steigen stetig. So soll elektrische Energie möglichst überall und jederzeit verfügbar sein und auf Basis erneuerbarer Energieträger produziert werden können, in unbegrenzter Leistung und zu geringen Kosten. Der Bedarf an Energienetzautomatisierung steigt damit stetig. Wesentliche Treiber für echte Effizienzverbesserungen sind dabei u.a. Technologien basierend auf der wirksamen Nutzung künstlicher Intelligenz (KI).

Energieversorgungssysteme sind von entscheidender Bedeutung für Länder und Regionen und müssen stets zuverlässig funktionieren. Bei der Automatisierung dieser Systeme stellt sich die Frage, wie die Softwarearchitektur, die dabei zum Einsatz kommt, am besten strukturiert werden sollte, um höchste Zuverlässigkeit zu gewährleisten.

Es ist auch zu klären, ob es vorteilhafter ist, die künstliche Intelligenz zentral an einem Ort oder verteilt an mehreren dezentralen Standorten zu betreiben. Insbesondere diese Überlegung haben wir gemeinsam mit ChatGPT4.0 erörtert.

Da anspruchsvolle Software oft zunächst in großen Rechenzentren genutzt wird, ist es heutzutage üblich, künstliche Intelligenz (KI) zentral in solchen Einrichtungen zu betreiben.

Vorteile zentraler KI

Zentrale Künstliche Intelligenz (KI) hat eine Reihe von Vorteilen, die in bestimmten Szenarien sehr attraktiv sein können.

1. **Konzentration von Ressourcen**
   In einem zentralen System können erhebliche Rechenressourcen konzentriert werden, um komplexe Modelle zu trainieren und große Datenmengen zu verarbeiten. Dies ermöglicht die Nutzung leistungsfähiger Supercomputer und spezialisierter Hardware wie GPUs und TPUs.

2. **Einfacheres Management und Wartung**
   Ein zentrales System vereinfacht das Management und die Wartung, da alle Updates, Patches und Verbesserungen an einem zentralen Ort durchgeführt werden. Dies führt zu konsistenteren und besser kontrollierten Systemen.

3. **Effizienz und Konsistenz**
   Zentrale Systeme bieten eine einheitliche Plattform für die Datenverarbeitung und Modellentwicklung, was zu konsistenten Ergebnissen und effizienten Prozessen führt. Daten und Modelle müssen nicht mehrfach dupliziert oder synchronisiert werden.

4. **Zugang zu umfangreichen Datensätzen**
   Zentrale KI-Systeme haben oft Zugang zu großen, umfassenden Datensätzen, was zu genaueren und leistungsfähigeren Modellen führen kann. Zentralisierte Datenspeicherung ermöglicht eine umfassendere Datenanalyse und -nutzung.

5. **Koordination und Zusammenarbeit**
   Ein zentrales System erleichtert die Koordination und Zusammenarbeit zwischen verschiedenen Teams und Abteilungen. Alle Beteiligten können auf dieselben Ressourcen und Informationen zugreifen, was Effizienz und Effektivität der Arbeit erhöht.
6. **Kosteneffizienz für bestimmte Anwendungen**
   Für bestimmte Anwendungen und Organisationen kann ein zentrales System kosteneffizienter sein, insbesondere wenn es darum geht, spezialisierte Hardware und Software zu nutzen, die nicht leicht auf verteilte Systeme übertragen werden können.
7. **Skalierbarkeit durch Cloud-Dienste**
   Zentrale KI kann durch die Nutzung von Cloud-Diensten leicht skaliert werden. Cloud-Anbieter bieten flexible und skalierbare Infrastrukturen, die es ermöglichen, die Rechenressourcen je nach Bedarf zu erweitern oder zu reduzieren.
8. **Schnellere Entwicklung und Bereitstellung**
   Da alle Ressourcen zentralisiert sind, können neue Modelle und Anwendungen schneller entwickelt und bereitgestellt werden. Dies ist besonders vorteilhaft in schnelllebigen Branchen, in denen Zeit ein kritischer Faktor ist.
9. **Qualitätssicherung der KI-Trainingsdatensätze**
   Da alle Trainingsdaten zentral gespeichert werden, können deren Eignung zur Erreichung eines Zielmodells oder seiner Qualität beeinflusst werden.

Diese Vorteile machen zentrale KI zu einer attraktiven Lösung für viele Organisationen, insbesondere in Szenarien, in denen große Datenmengen verarbeitet werden müssen und eine zentrale Steuerung von Vorteil ist.

Hieraus ergibt sich die Frage, was die Nachteile der zentralen KI-Nutzung für künstliche Intelligenz sein können.

Nachteile zentraler KI

Zentrale KI-Systeme bieten ohne Frage viele Vorteile. Doch welche Nachteile sind in Kauf zu nehmen bzw. zu beachten?

1. **Hohe Latenzzeiten**
   - **Verzögerungen bei der Datenübertragung:** Da Daten von den Endgeräten zu zentralen Servern und wieder zurück übertragen werden müssen, kann es zu Verzögerungen kommen, was insbesondere bei zeitkritischen Anwendungen problematisch ist.
   - **Abhängigkeit von Netzwerkverbindungen:** Die Leistung zentraler KI-Systeme hängt stark von der Qualität und Stabilität der Netzwerkverbindungen ab. Instabile oder langsame Verbindungen können die Reaktionszeit erheblich beeinträchtigen.

- **Cloudanwendungen und Abhängigkeit von Internetverfügbarkeit:** Werden die Netzwerkverbindungen über das Internet (fest und mobil) hergestellt, verschärfen sich die genannten Probleme.

2. **Hohe Infrastruktur- und Betriebskosten**
   - **Kosten für Rechenzentren:** Der Betrieb und die Wartung großer zentraler Rechenzentren ist teuer. Dies umfasst Kosten für Hardware, Strom, Kühlung und Personal.
   - **Bandbreitenkosten:** Die Übertragung großer Datenmengen zwischen Endgeräten und zentralen Servern kann hohe Bandbreitenkosten verursachen.
3. **Skalierungsprobleme**
   - **Begrenzte Skalierbarkeit:** Zentrale Systeme haben oft Schwierigkeiten, mit einer schnell wachsenden Anzahl von Endgeräten und Nutzern zu skalieren, was zu Leistungseinbußen führen kann.
   - **Engpässe:** Zentralisierte Architektur kann zu Engpässen führen, wenn die Nachfrage die Kapazität der zentralen Server übersteigt.
4. **Datensicherheits- und Datenschutzprobleme**
   - **Zentralisierte Angriffsziele:** Zentralisierte Rechenzentren sind attraktive Ziele für Cyberangriffe. Ein erfolgreicher Angriff kann große Mengen sensibler Daten kompromittieren und viele Nutzer gleichzeitig von der Nutzung ausschließen.
   - **Datenschutzrisiken:** Die Übertragung sensibler Daten an zentrale Server kann Datenschutzrisiken erhöhen, insbesondere wenn die Daten über internationale Grenzen hinweg gesendet werden.
5. **Eingeschränkte Anpassungsfähigkeit**
   - **Langsame Anpassung an lokale Bedingungen:** Zentrale KI-Systeme haben Schwierigkeiten, sich schnell an spezifische lokale Anforderungen und Bedingungen anzupassen, da die Modelle zentral trainiert und verwaltet werden.
   - **Mangelnde Flexibilität:** Änderungen und Anpassungen erfordern oft umfangreiche Änderungen an der zentralen Infrastruktur, was zeitaufwändig und teuer sein kann.
6. **Abhängigkeit von zentralen Diensten**
   - **Single Point of Failure:** Zentrale Systeme stellen einen einzigen Ausfallpunkt dar. Ein Problem oder Ausfall im zentralen Rechenzentrum kann die Verfügbarkeit der Dienste insgesamt beeinträchtigen.
   - **Serviceverfügbarkeit:** Die Verfügbarkeit der zentralen Dienste kann durch externe Faktoren wie Naturkatastrophen oder Netzwerkstörungen massiv gefährdet werden.

7. Regulatorische und rechtliche Herausforderungen

- **Datenspeicherung und -übertragung:** Die Speicherung und Übertragung von Daten über internationale Grenzen hinweg kann regulatorische und rechtliche Herausforderungen mit sich bringen, insbesondere im Hinblick auf Datenschutzgesetze wie die DSGVO (Datenschutz-Grundverordnung) oder DSA (Digital Services Act).

Diese Nachteile zentraler KI-Systeme lassen sie in vielen Fällen weniger geeignet erscheinen. Insbesondere gilt dies für Anwendungsfälle der Energie-Automatisierung, die sehr schnelle Reaktionszeiten, hohe Flexibilität und starke Datenschutzanforderungen erfordern.

In solchen Szenarien kann eine dezentrale Architektur die bessere Alternative sein.

Beispiel Umspannanlage

Aus Sicht der Betreiber von investitionsintensiven Umspannanlagen, welche zumeist im einstelligen Millionen Euro-Bereich liegen, ist die Überwachung in Echtzeit von großer Bedeutung. Die oben genannten Latenzen und Bandbreitenbegrenzungen beim Echtzeit-Streaming beispielsweise von 10 infrarot Videokameras und parallel 10 optischen Videokameras in nur eine zentrale KI über Mobilfunk sind hierbei besonders problematisch. Insbesondere in Regionen ohne entsprechend sehr breitbandige Kommunikationsinfrastruktur.

Entwickelt beispielsweise ein Transformator unnormale Temperatur-Hotspots aufgrund kurzzeitiger Überlastung, Abnutzung, unzureichender Wartung, Kurzschlüsse aufgrund defekter externer Isolatoren, Anschlüssen oder defekter internen Wicklungen, Blitzeinschlägen, unzureichender Erdung, Korrosion oder lockerer Stellen insbesondere an Verbindungen der Hochspannungsleiter bzw. -Seile oder auch Vandalismus usw., gilt es dies sehr zeitnah zu detektieren. Nur so können etwaige Sofortmaßnahmen eingeleitet werden, bevor Anlagen oder Komponenten Schaden nehmen und das Investitionsgut Leistungstransformator beispielsweise in einem großen Feuerball abbrennt.

Ebenso zeitkritisch ist beispielsweise die Überwachung zur Vorbeugung der Explosion von Spannungswandlern (Potential Transformern (PT)) oder Stromwandlern (Current Transformern (CT)). Durch fehlerhafte Isolation und das Eindringen von Feuchtigkeit und Staub, durch den Austritt von Öl, durch ein überlastetes Dielektrikum, durch lockere oder korrodierte Verbindungen zu Hochspannungsseilen können sich schnell und spontane Hitzestellen entwickeln welch zeitnahes Erkennen und sofortigen Eingriff zur Schadensvermeidung erfordern.

So wird bspw. vermieden, dass Keramikteile des äußeren Isolators in Stücke gesprengt und die Trümmer über einen Bereich von bis zu 200 m verstreut niederschlagen und weitere Komponenten der Umspannanlage beschädigen und das Problem weiter eskaliert, bis im schlimmsten Fall Gefahren für Leib und Leben entstehen.

Diese Beispiele verdeutlichen, dass zeitnahes Erkennen und Reagieren in der Energiewirtschaft essenziell sind.

Wie kann künstliche Intelligenz dezentralisiert werden?

Die Dezentralisierung von künstlicher Intelligenz (KI) kann auf verschiedenen Wegen erreicht werden, um die Kontrolle, Verteilung und Sicherheit der Technologie zu verbessern. Hier sind einige der Hauptansätze:

1. **Edge Computing**: KI-Modelle werden direkt auf lokalen Geräten oder in der Nähe des Datenursprungs ausgeführt, anstatt in zentralen Rechenzentren. Dies reduziert Latenzzeiten, verbessert die Datensicherheit (da Daten nicht an zentrale Server gesendet werden müssen) und ermöglicht eine schnellere Verarbeitung.
2. **Federated Learning**: Dabei werden KI-Modelle auf vielen dezentralen Geräten oder Servern trainiert, wobei nur die Modellaktualisierungen und nicht die Rohdaten ausgetauscht werden. Dies schützt die Privatsphäre der Nutzer, da ihre Daten auf ihren eigenen Geräten verbleiben.
3. **Peer-to-Peer (P2P) Netzwerke**: In einem P2P-Netzwerk wird die KI auf viele gleichwertige Knoten verteilt, die zusammenarbeiten. Jeder Knoten trägt zur Verarbeitung und zum Lernen bei, ohne dass ein zentraler Server benötigt wird. Dies erhöht die Redundanz und Sicherheit, da das System weniger anfällig für einzelne Ausfälle ist.
4. **Dezentrale Cloud-Infrastrukturen**: Anstelle von zentralen Rechenzentren können KI-Modelle auf einer verteilten Cloud-Infrastruktur ausgeführt werden, die über verschiedene geografische Standorte verteilt ist. Dies erhöht die Robustheit und Sicherheit des Systems, da es keine zentrale Abhängigkeit gibt.
5. **Hybrid-Modelle**: Eine Kombination aus zentralisierten und dezentralisierten Ansätzen, bei der einige Teile der KI-Infrastruktur zentralisiert bleiben, während andere dezentralisiert werden. Dies kann eine Balance zwischen Effizienz, Kontrolle und Sicherheit bieten.

Jeder dieser Ansätze zur Dezentralisierung hat seine eigenen Vorteile und Herausforderungen und kann je nach Anwendungsfall und spezifischen Anforderungen eingesetzt werden.

Mit Edge Computing KI dezentralisieren

Die konsequenteste und effizienteste Dezentralisierung erfolgt mit Edge Computing. Hier werden die Daten (nah) am Ort der Entstehung verarbeitet. Gewissermaßen am „Rand" (Edge) des Netzwerkes. Ziel ist es, die Latenzzeiten zu minimieren und die Effizienz der Datenverarbeitung zu verbessern, indem die Verarbeitungsressourcen näher oder direkt an den Geräten platziert werden, die Daten erzeugen oder nutzen. Bekannte Beispiele sind autonomes Fahren, Verkehrserkennung und -leitung in Smart Cities oder Anwendungen im Kontext von Industrie 4.0.

Da die oben genannten Varianten 2-5 letztlich alle hybride Ansätze sind, konzentrieren wir uns bei den folgenden Betrachtungen auf Edge Computing.

Vorteile dezentraler Edge KI

Dezentrale KI (Künstliche Intelligenz), im Englischen bekannter als Edge AI, bietet mehrere Vorteile gegenüber zentralisierten Systemen:

1. **Datenschutz und Sicherheit**: Durch die Verteilung der Datenverarbeitung auf mehrere Knoten wird das Risiko von Datenschutzverletzungen reduziert. Sensible Daten bleiben lokal und müssen nicht an zentrale Server gesendet werden, was das Risiko von Datendiebstahl verringert. Zeitgleich wird so die Möglichkeit der zentral kompromittierenden Einflussnahme verringert.
2. **Robustheit und Zuverlässigkeit**: Dezentrale Systeme sind weniger anfällig für Ausfälle, da keine einzelne Fehlerquelle besteht. Selbst wenn ein Teil des Systems ausfällt, können die übrigen Teile weiterhin funktionieren.
3. **Skalierbarkeit**: Dezentrale Systeme können leichter skaliert werden, da neue Knoten hinzugefügt werden können, ohne dass eine zentrale Infrastruktur überlastet wird. Dies ermöglicht eine flexiblere Anpassung an steigende Anforderungen.
4. **Geringere Latenz**: Da die Verarbeitung näher am Ort der Datenerfassung stattfindet, können Verzögerungen minimiert werden. Dies ist besonders wichtig für Echtzeitanwendungen wie autonome Fahrzeuge, Industrie 4.0 oder visuelle Überwachung.
5. **Kostenreduktion**: Dezentrale Systeme können kostengünstiger sein, da sie oft weniger zentrale Infrastruktur und Wartung erfordern. Darüber hinaus können vorhandene lokale Ressourcen genutzt werden.
6. **Datensouveränität**: Organisationen und Einzelpersonen behalten die Kontrolle über ihre Daten, was besonders in sensiblen Bereichen wie dem Gesundheitswesen oder bei persönlichen Daten von Bedeutung ist.
7. **Anpassungsfähigkeit**: Dezentrale Systeme können leichter an spezifische lokale Anforderungen angepasst werden. Unterschiedliche Regionen oder Branchen können ihre eigenen Optimierungen und Anpassungen vornehmen.
8. **Innovation und Wettbewerb**: Dezentralisierung fördert Innovationen, da verschiedene Akteure unabhängig voneinander an Lösungen arbeiten können. Dies führt zu einem wettbewerbsfähigen Umfeld, in dem neue und verbesserte Technologien entstehen können.

Diese Vorteile machen dezentrale KI zu einer attraktiven Option für viele Anwendungsbereiche, insbesondere dort, wo Datenschutz, Skalierbarkeit und Zuverlässigkeit von besonderer Bedeutung sind.

Robustheit und Ausfallsicherheit

Mit besonderem Blick auf die Energieautomatisierung, insbesondere die hier geforderte Robustheit und Zuverlässigkeit, ist festzustellen, dass **Edge Computing** die Robustheit und Zuverlässigkeit von künstlicher Intelligenz (KI) durch mehrere konkrete Mechanismen zu verbessern vermag:

1. Lokale Datenverarbeitung:
    - **Unabhängigkeit von Netzwerkverbindungen:** Da die Datenverarbeitung vor Ort stattfindet, sind KI-Systeme weniger abhängig von stabilen und schnellen Internetverbindungen. Dies ist besonders nützlich in abgelegenen oder schlecht vernetzten Gebieten.
2. Verteilte Architektur:
    - **Fehlertoleranz:** Durch die Verteilung der Datenverarbeitung auf viele Edge-Geräte kann das System auch dann weiterarbeiten, wenn einzelne Geräte ausfallen oder beeinträchtigt werden. Diese Verteilung erhöht die Fehlertoleranz und die Robustheit des Gesamtsystems.
    - **Lastverteilung:** Die Verarbeitungslast kann auf mehrere Geräte verteilt werden, wodurch die Wahrscheinlichkeit von Überlastungen und Ausfällen reduziert wird. Dies führt zu einer stabileren und zuverlässigeren Performance.

    Im konkreten Fall der AI PowerBrain™ KI-Technologie von PowerBrain.Shop wird beispielsweise ein AI PowerBrain™ pro Kamera pro Embedded System installiert, um die Robustheit sicherzustellen.
3. Lokal optimierte Modelle:
    - **Anpassung an lokale Bedingungen:** KI-Modelle können auf Edge-Geräten spezifisch an die lokalen Bedingungen und Daten angepasst werden. Dies führt zu präziseren und relevanteren Ergebnissen, da die Modelle auf die spezifischen Anforderungen und Umgebungen zugeschnitten sind.
    - **Kontinuierliche Verbesserung:** Edge-Geräte können kontinuierlich neue Daten sammeln und Modelle lokal verbessern, was zu einer stetigen Optimierung und Anpassung der KI führt.

    Dies hilft beispielsweise bei der Qualitätssicherung, indem mehrere Datenquellen durch Triangulation miteinander abgeglichen werden, um beispielsweise eine beobachtete Störung mehrfach zu bestätigen und damit Fehlalarme zu minimieren.
4. Energieeffizienz:
    - **Lokale Verarbeitung spart Energie:** Die Reduktion des Datenverkehrs zu zentralen Servern spart Energie, da die Daten lokal verarbeitet werden. Dies kann besonders in Umgebungen mit begrenzten Energieressourcen von Vorteil sein.

- **Optimierte Ressourcennutzung:** Edge-Geräte können ihre Energie- und Rechenressourcen effizient nutzen, um die KI-Modelle auszuführen, was zu einer insgesamt zuverlässigeren und stabileren Leistung führt.

Beispielsweise werden die Embedded Systems, die AI PowerBrains™ zur optischen Videoüberwachung betreiben, bei fehlender Beleuchtung zur Nachtzeit automatisch „schlafen gelegt", sodass deren Energieverbrauch reduziert wird.

5. Sicherheit und Datenschutz:
   - **Weniger Anfälligkeit für Angriffe:** Durch die lokale Verarbeitung und Speicherung von Daten sind Edge-Geräte weniger anfällig für zentrale Angriffe, die die Verfügbarkeit und Zuverlässigkeit des gesamten Systems beeinträchtigen könnten.
6. Echtzeit-Überwachung und -Wartung:
   - **Proaktive Fehlererkennung:** Edge-Geräte können kontinuierlich überwacht werden, um potenzielle Fehler oder Probleme frühzeitig zu erkennen und zu beheben, bevor sie die Systemleistung beeinträchtigen.

Durch diese Ansätze kann Edge Computing die Robustheit und Zuverlässigkeit von KI-Systemen erheblich verbessern, indem es die Abhängigkeit von zentralen Ressourcen reduziert und eine flexiblere, anpassungsfähigere und sicherere Infrastruktur bereitstellt.

Latenzzeit Minimierung

Aus operativer Sicht eines Energieversorgungsunternehmens (EVU) ist die höchst zeitnahe Erkennung und Reaktion auf Probleme in einer Umspannanlage entscheidend, um Schaden an Menschen, Anlagen und Energienetzen minimieren zu können.

Edge Computing kann die Latenzzeit von künstlicher Intelligenz (KI) auf mehrere Weisen verringern:

1. Lokale Datenverarbeitung:
   - **Direkte Verarbeitung am Ort der Datenerfassung:** Durch die Verarbeitung der Daten direkt auf dem Edge-Gerät, wo sie erfasst werden, entfällt die Notwendigkeit, Daten an entfernte zentrale Server zu senden und die Ergebnisse zurückzuerhalten. Dies reduziert die Latenz erheblich.
   - **Echtzeitverarbeitung:** Edge-Geräte können Daten in Echtzeit verarbeiten, was die Verzögerungen minimiert und schnelle Entscheidungen ermöglicht. Dies ist besonders wichtig für zeitkritische Anwendungen wie autonome Fahrzeuge, industrielle Steuerungssysteme und Gesundheitsüberwachung.

2. Reduzierte Netzwerkabhängigkeit:
    - **Minimierung von Datenübertragungen:** Da große Datenmengen nicht über das Netzwerk übertragen werden müssen, verringert sich die Abhängigkeit von Netzwerkbandbreite und -qualität. Dies reduziert die Latenz, die durch Netzwerküberlastungen oder langsame Verbindungen verursacht wird.
3. Optimierte Datenverarbeitung:
    - **Vorverarbeitung der Daten:** Edge-Geräte können Daten vorverarbeiten und nur relevante Informationen an zentrale Server senden, wodurch die Menge der übertragenen Daten reduziert und die Effizienz gesteigert wird. Dies beschleunigt die gesamte Datenverarbeitungskette.
4. Direkte Interaktion und Rückmeldung:
    - **Lokale Entscheidungsfindung:** Edge-Geräte können lokale Entscheidungen treffen, ohne auf die Rückmeldung von zentralen Servern warten zu müssen. Dies ist besonders nützlich in Situationen, die schnelle Reaktionen erfordern, wie z.B. bei der Verarbeitung von Sensor- oder Videoüberwachungsdaten.
5. Intelligente Datenweiterleitung:
    - **Edge Gateways:** Edge Gateways können als Vermittler fungieren, die Daten intelligent weiterleiten und nur die notwendigen Informationen an zentrale Server senden. Dies reduziert die Latenz, indem unnötige Datenübertragungen vermieden werden.
6. Optimierung der Rechenressourcen:
    - **Ressourcenmanagement:** Dynamisches Ressourcenmanagement auf Edge-Geräten kann sicherstellen, dass kritische Anwendungen priorisiert und Ressourcen optimal genutzt werden, was die Verarbeitungszeit verkürzt.

Herausforderungen bei der Nutzung von Edge AI

Edge KI bietet viele obengenannte Vorteile. Einigen Aspekten sind bei ihrer Nutzung besondere Beachtung zu schenken:

1. Begrenzte Rechenressourcen:
    - **Eingeschränkte Hardwarekapazitäten:** Dezentrale Systeme (Edge Computer) haben oft weniger Rechenleistung und Speicherkapazität im Vergleich zu zentralen Großrechenzentren, was die Komplexität und Größe der KI-Modelle begrenzt.
    - **Leistungsfähigkeit:** Die Durchführung aufwändiger Berechnungen oder das Training sehr großer KI-Modelle auf sehr großen Trainingsdatensätzen dauert auf Edge-Computern deutlich länger.

2. Komplexität der Implementierung:
    - **Verteilte Infrastruktur:** Der Verwaltung und Wartung einer sehr großen Anzahl von Edge-Computern wohnt u. U. eine Komplexität inne, die mittels spezialisierter Software-Update und Wartungs-Werkzeugen sowie ihnen entsprechende Prozesse adressiert werden sollte.
3. Datensynchronisation und Konsistenz:
    - **Inkonsistente Daten:** Das Sicherstellen der Datenkonsistenz und -synchronisation über viele dezentrale Geräte hinweg ist eine Herausforderung. Unterschiedliche Geräte können unterschiedliche Versionen von Daten und KI-Modellen nutzen.
    - **Latenz bei der Synchronisation:** Die Zeit, die benötigt wird, um Daten zwischen Geräten zu synchronisieren, kann zu Verzögerungen und Inkonsistenzen führen.
4. Sicherheitsrisiken:
    - **Angreifbare Endpunkte:** Da viele Geräte in einem dezentralen System als Endpunkte fungieren, erhöht sich die Anzahl der potenziellen Angriffspunkte. Jedes Gerät ist einzeln zu sichern – was die Ausfallsicherheit des Gesamtsystems erhöht und die Kosten und Aufwände für einen etwaigen Angreifer ebenfalls erhöht.
    - **Physische Sicherheit:** Edge-Computer oder Embedded Systems befinden sich oft in weniger geschützten Umgebungen als zentrale Rechenzentren, was sie anfälliger für physische Angriffe macht. Sie sind in dementsprechend sicheren Umgebungen zu verwahren und zu betreiben.
5. Eingeschränkte Datenverfügbarkeit:
    - **Lokale Daten:** Edge-Geräte haben lokal nur Zugriff auf vor Ort verfügbare Daten, was die Menge und Vielfalt der Daten einschränken kann, die für das Training und die Ausführung von KI-Modellen zur Verfügung stehen. Daher sind sie bei Bedarf mit zusätzlichen Trainingsdatensätzen auszurüsten, bspw. über zeitlich begrenzte Datenverbindungen und Fernzugriffe.
    - **Fehlende globale Sicht:** Die dezentralisierte Natur von Edge AI kann es schwieriger machen, eine umfassende globale Sicht auf alle Daten zu erhalten. Für einen regelmäßigen Austausch etwaig relevanter Daten ist daher zu sorgen.
6. Netzwerkabhängigkeit:
    - **Verbindungsprobleme:** Obwohl Edge Computing darauf ausgelegt ist, die Abhängigkeit von zentralen Netzwerken zu reduzieren, können viele Anwendungen dennoch eine gewisse Netzwerkkonnektivität für die Synchronisation und Datenübertragung benötigen. Instabile oder langsame Verbindungen können die Leistung beeinträchtigen.

- **Datenübertragungskosten:** Die etwaige Synchronisation und Datenaustausch zwischen vielen Edge-Geräten und/oder zentralen Systemen können zusätzliche Bandbreitenkosten verursachen.

7. Komplexität bei der Verwaltung von Modellen:
   - **Modellverteilung:** Die Verteilung und Aktualisierung von KI-Modellen auf vielen Edge-Geräten ist komplex und kann zu Versionierungsproblemen führen.
   - **Föderiertes Lernen:** Obwohl föderiertes Lernen Vorteile bietet, ist es komplex zu implementieren und erfordert robuste Mechanismen für die Aggregation und Synchronisation von Modellupdates.

Fazit

Die vorhergehenden Ausführungen zeigen, dass dezentrale Edge-KI-Architekturen große Vorteile für zeitkritische Anwendungen bieten. Sie erfüllen höchste Anforderungen an Ausfallsicherheit und Cyber-Sicherheit, insbesondere in der Energiewirtschaft. Um diese Technologien erfolgreich zu implementieren, sind durchdachtes Softwaredesign und sorgfältige Verwaltung der dezentralen Systeme notwendig. Der Einsatz geeigneter Software-Werkzeuge ist entscheidend. So kann Edge-KI-Technologie auf dem erforderlichen Qualitätsniveau der Energiewirtschaft beherrscht werden.

Angesichts der wachsenden Rechenleistung und Speicherkapazität dezentraler Systeme, zusammen mit sinkenden Marktpreisen, wird die Verbreitung von Edge-KI-Anwendungen rasant zunehmen. Diese Entwicklung wird die Effizienz steigern und Prozesse sicherer machen. Indem Sie die Potenziale von Edge-KI nutzen, schaffen Sie Lösungen, die den Herausforderungen der Zukunft gewachsen sind.

Autoren

Mirko Düssel

Geschäftsführer von Mirko Düssel & Co., einer Strategie- und Marketingberatung in Kaarst.

E-Mail info@duessel.com
Web www.duessel.com

Samuel T. Stähle

CEO bei PowerBrainShop Holding Corp., ein Software Technologie Lieferant von „Plug and Play“ künstlicher Intelligenz (B2B).

E-Mail samuel.staehle@powerbrain.shop
Web https://powerbrain.shop