Future-Energy-Technologiescouting

Digitale Technologien für die Energiewende

Ausgabe 2

Future Energy Lab

dena
Deutsche Energie-Agentur

Das Future-Energy-Technologiescouting

Scouting (dt. Erkundung) ist vor allem aus dem Profisport oder der Personalbeschaffung großer Unternehmen bekannt. In diesen Fällen suchen sogenannte Talentscouts nach neuen Protegés und handeln dabei meist im Auftrag von Vereinen oder Konzernen oder selbstständig und motiviert durch eine potenzielle Teilhabe an den zukünftigen Verdiensten ihrer Funde. Doch gescoutet werden schon seit Langem nicht mehr nur talentierte Personen. Seit einiger Zeit hat sich in Unternehmen auch das Technologiescouting etabliert. Dabei wird nach Lösungen für konkrete Probleme, aber auch nach Innovationen und Disruptionen gesucht, die das Potenzial für neue Produkte und Geschäftsmodelle zur Sicherung des fortwährenden Unternehmenserfolgs unter Einfluss der stetigen wirtschaftlichen, technischen und gesellschaftlichen Veränderungen haben.

Das-Future-Energy-Technologiescouting unterscheidet sich von dem privater Unternehmen durch die Kombination der folgenden zwei Schwerpunkte. Erstens: Es zielt auf neue Softwarelösungen, Hardwarekomponenten und Digitalisierungsstrategien für die Energiewende ab. Darunter fallen zum einen Innovationen im Bereich der Datenerfassung, -übertragung, -speicherung und -verarbeitung, die die Einbindung einer großen Anzahl von Erneuerbare-Energien-Anlagen in das bestehende Energiesystem erleichtern und sicherer gestalten, und zum anderen digitale Technologien, die die Energieeffizienz der Digitalisierung selbst steigern können. Zweitens: Der Nutzen der Technologien dieses Scoutings maximiert sich erst bei ihrem flächendeckenden Einsatz. Daher werden die Ergebnisse nicht nur einzelnen, sondern allen Akteuren der Energiebranche und darüber hinaus zur Verfügung gestellt.

Für das Future-Energy-Technologiescouting strecken wir – das Future Energy Lab der dena – neben unserer Arbeit an Pilotprojekten, Studienvorhaben und der Pflege unserer Community unsere Fühler aus. Wir durchkämmen das Internet, studieren Trend-Reports und tauschen uns mit Expertinnen und Experten der Digital- und Energiebranche aus. Auf Basis der dabei gesammelten Informationen erstellen wir einen umfangreichen Pool von Talenten digitaler Technologien und wählen schließlich jene aus, die es in den Bericht des Future-Energy-Technologiescoutings schaffen.

In Steckbriefen der ausgewählten Technologien beschreiben wir die ursprünglichen Probleme, für deren Lösung sie konzipiert wurden, und geben einen Einblick in ihre Funktionalität. Darauf aufbauend leiten wir erste Impulse für die Verwendung der Technologien in der Energiewirtschaft ab. Weitere Einsatzmöglichkeiten werden Sie, liebe Leserinnen und Leser, da sind wir uns sicher, durch Ihre detaillierten Kenntnisse des Energiesystems und seiner Unternehmen identifizieren.

Wir wünschen Ihnen viel Spaß beim Lesen und sind gespannt, wann und wie die diesjährige Auswahl in Zukunft zum Einsatz kommen wird!

Ihr Team des Future Energy Lab

Für die Einschätzung des Nutzens der vier Technologien für die Digitalisierung erfolgt eine Visualisierung mittels Netzdiagrammen. Sie stellen die qualitative Bewertung auf Basis unserer Expertise dar und bilden unsere Einordnung in die sechs vorgegebenen Kategorien ab.

Die Angabe „Etablierung in … Jahren“ orientiert sich an den „Hype Cycles“ der Technologien. Sie beschreiben den Verlauf der öffentlichen Wahrnehmung einer Technologie. Ein Hype Cycle findet in fünf Phasen statt, die hier zum besseren Verständnis kurz umrissen werden sollen:

1. **Technologischer Auslöser**
   - Technologischer Durchbruch
   - Proof of Concept Stories + Medieninteresse = Öffentlichkeitswirkung
   - Produkte ohne definierte Anwendung
2. **Gipfel der überzogenen Erwartungen**
   - Erfolgsgeschichten und Misserfolge werden der Öffentlichkeit bekannt
   - Unternehmen reagieren
3. **Tal der Enttäuschung**
   - Stagnierendes öffentliches Interesse durch fehlende erfolgreiche Anwendungen
   - Rückgang von Investitionen
4. **Pfad der Erleuchtung**
   - Steigende Zahl an Anwendungsfällen (und Pilotprojekten) und besseres Verständnis für die Verwendung der Technologie
   - Produkte befinden sich bereits in höheren Generationen (z. B. 2. und 3.)
5. **Plateau der Produktivität**
   - Ankommen der Technologie im Mainstream
   - Erfolgreiche Marktanwendung

Der geschätzte Zeitraum, den eine Technologie für die Etablierung benötigt, bezieht sich in unserem Technologiescouting auf das Erreichen des „Plateaus der Produktivität“, also den Punkt, an dem der Nutzen einer Technologie klar abschätzbar ist. Wenn Sie beim Lesen auf Angaben wie „Etablierung in: 2–5 Jahren“ stoßen, wird damit prognostiziert, dass die Technologie innerhalb des angegebenen Zeitraums das „Plateau der Produktivität“ erreicht hat.

Die Auswahl des Future-Energy-Technologiescoutings

Quantenkommunikation

Seite 4

Vektordatenbanken

Seite 6

Explainable AI

Seite 8

AI for Cybersecurity

Seite 10

Quantenkommunikation

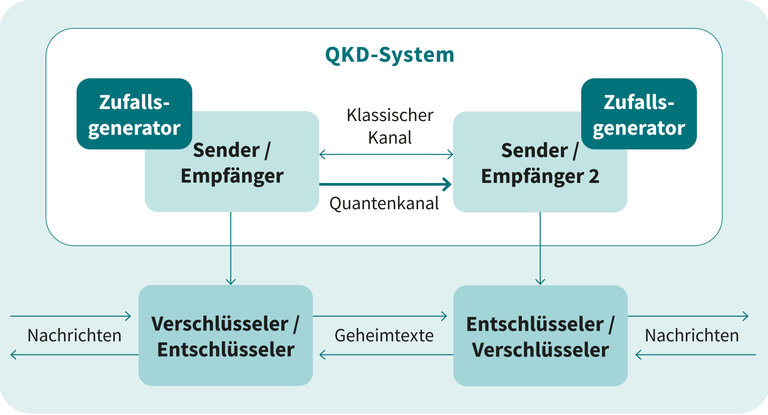
Technologietyp:	Software Konzept/Strategie	**Hardware**
Einfluss auf Daten:	Erfassung Speicherung	**Übertragung** Verarbeitung

Technology Readiness / Etablierung in:
2–5 Jahren[6]

Verwandte Themen:
- Qubits
- Quantencomputer
- Polarisation von Photonen
- RSA-Verfahren
- Shor-Algorithmus

Mit fortschreitender Digitalisierung gewinnt auch die Frage nach der Umsetzung von Informationssicherheit stetig an Relevanz. Eine verbreitete Variante der Verschlüsselung ist das RSA-Verfahren (Rivest-Shamir-Adleman), ein Public-Key-Verfahren, das beispielsweise bei der E-Mail-Verschlüsselung, sicheren Zahlungsvorgängen oder VPN-Verbindungen Anwendung findet.

Dieses Verschlüsselungsverfahren basiert auf dem sogenannten Faktorisierungsproblem, das aus Perspektive der Informationssicherheit sehr vorteilhaft ist. Danach ist kein klassischer Algorithmus in der Lage, eine längere Primzahl effizient in ihre Primfaktoren zu zerlegen.[1] Selbst bei Hochleistungsrechnern ist hier von Zeiträumen in einer Größenordnung von mehreren Jahren auszugehen.[2] Eine Entschlüsselung auf diesem Wege scheint also sehr unwahrscheinlich.



Und dennoch ist dieses Problem nicht unlösbar, was eine potenzielle Bedrohung der Informationssicherheit darstellen könnte. Mit dem Shor-Algorithmus wurde im Jahr 1994 eine Möglichkeit der Primfaktorzerlegung mittels Quantencomputern veröffentlicht, die auch für sehr große Zahlen effizient funktioniert.[3] Hierbei kann die Dauer je nach Hardware im Vergleich zu Computern mit einer Von-Neumann-Architektur drastisch reduziert werden. Die potenzielle Nutzung von Quantencomputern zur Entschlüsselung kryptografischer Verfahren stellt ein Sicherheitsrisiko dar, wenn diese hauptsächlich auf mathematischen Problemen basieren.

Eine Möglichkeit, diesem Risiko entgegenzuwirken, ist die Verlagerung der Sicherheitsfrage von einem mathematischen hin zu einem physikalischen Ansatz. Dafür könnte sich die Quantenkommunikation zukünftig eignen.

Die Quantenkommunikation basiert auf der Nutzung von Qubits (Quantenbits), die analog zu Bits die kleinstmögliche Informationseinheit in der Quanteninformatik darstellen.[4] Anders als klassische Bits repräsentieren Qubits allerdings nicht eine 0 oder 1, sondern einen Überlagerungszustand dieser beiden Werte.[5]

Qubits können mittels Photononen, Ionen und Elektronen erzeugt werden. In der Quantenkommunikation eignen sich Photonen am besten, da sie zwischen zwei weit entfernten Orten austauschbar sind (z. B. mittels optischer Leiter).

1 Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2021): Kryptografie quantensicher gestalten. Grundlagen, Entwicklungen, Empfehlungen
2 Fraunhofer-Institut für Algorithmen und Wissenschaftliches Rechnen (SCAI) & Mathematisches Institut der Universität Köln (2017): RSA-Primzahlen zur Verschlüsselung von Nachrichten
3 https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography (abgerufen: 02.12.2024)
4 https://www.chemie.de/lexikon/Qubit.html#Eigenschaften (abgerufen: 02.12.2024)
5 https://www.helmholtz.de/glossar/begriff/quantenkommunikation/ (abgerufen: 05.12.2024)
6 https://www.gartner.com/en/documents/5573927 (abgerufen: 21.02.2025)

Die zu übertragende Information (1 Bit) erhalten die Photonen bei ihrer Polarisation (Schwingungsrichtung). Durch die Überlagerung der verschiedenen Zustände des Photons wird diese Information erst bei seiner Messung eindeutig und die Überlagerung endet.

Bei einem Austausch von Photonen zwischen Sender und Empfänger kann der Zustand des empfangenen Photons mit einem Überlagerungsprotokoll abgeglichen werden, das Auskunft darüber gibt, ob der ursprüngliche Überlagerungszustand des Photons noch besteht oder nicht. Sollte bei der Übertragung eine Messung erfolgt sein, wird so bei einer erneuten Messung durch dieses Protokoll ein Fehler angezeigt. Dies würde signalisieren, dass die Information bereits ausgelesen wurde. Auch eine Kopie des Zustands eines Photons ist nicht möglich. Hintergrund hierfür ist das sogenannte No-Cloning-Theorem, das besagt, dass bei einem Kopierversuch der Zustand des Originals unweigerlich verändert werden würde und der Kopierversuch somit auch nachweisbar wäre.[7]

Anders als bei dem eingangs beschriebenen RSA-Verfahren können bei der Quantenkommunikation Informationen nicht durch reinen Rechenaufwand entschlüsselt werden. Außerdem ist ein Eingriff in den Kommunikationsweg nicht möglich, ohne dass er bemerkt wird.

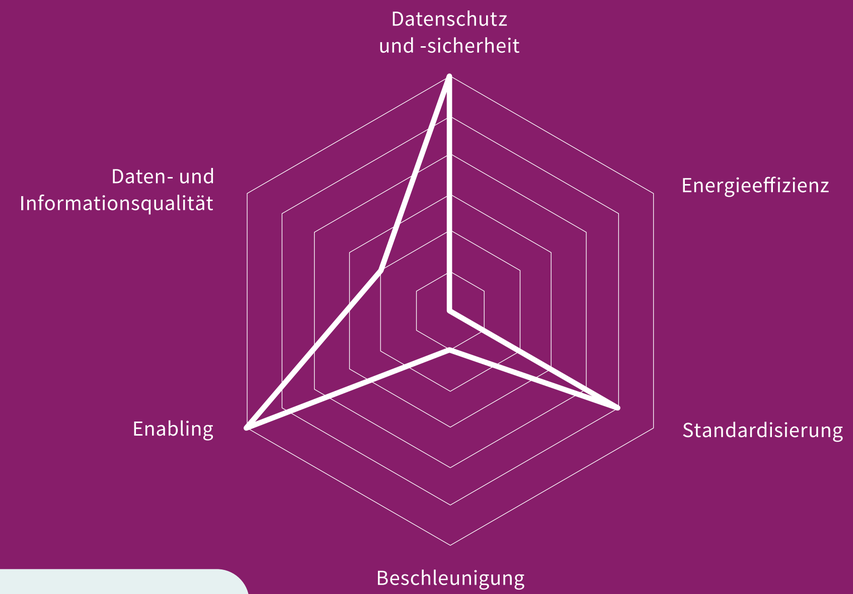
Als Anwendungsbeispiel für Quantenkommunikation eignet sich die Quantum Key Distribution (QKD). Grundvoraussetzung ist zunächst eine Verbindung von zwei Parteien mittels zweier Datenübertragungskanäle: eines klassischen Kanals und eines Quantenkanals. Der klassische Kanal dient der Versendung der zu übertragenden Daten in verschlüsselter Form. Über den Quantenkanal wird nun eine Reihe an polarisierten Photonen zwischen Sender und Empfänger versendet. Durch die Messung der Photonen erhält der Empfänger eine Bitfolge, aus der sich ein Schlüssel extrahieren lässt.[8] Mit ihm können die Daten entschlüsselt werden, die über den klassischen Kanal empfangen wurden.

Ein zentrales Problem in der Quantenkommunikation ist die Dekohärenz, also die Wechselwirkung von Quanten mit ihrer Umgebung. Quanten sind äußerst anfällig für äußere Einflüsse wie Vibration oder Temperaturänderungen, die den fragilen Überlagerungszustand beeinträchtigen können.[9] Für die Quantenkommunikation bedeutet das eine Verschlechterung der Informationsübertragung. Bei der Nutzung von Photonen in optischen Leitern wie Glasfaser ist die Dekohärenz gering. Dennoch treten bei der Übertragung ab einer Entfernung von hundert Kilometern Verlusteffekte auf.[10] Für das Überwinden dieses Problems gibt es verschiedene Ansätze, wie zum Beispiel den Einsatz von Quantenrepeatern oder Satellitentechnik.[11]

Eine Verwendung der Quantenkommunikation ist in jeder Umgebung mit hohen Sicherheitsanforderungen bei der Informationsübertragung denkbar, wie zum Beispiel beim Datenverkehr von Einrichtungen der Kritischen Infrastruktur. Bei der Digitalisierung der Energienetze gilt dies gerade in Bezug auf die Steuerungstechnik. Vor diesem Hintergrund könnten die Quantenkommunikation und speziell die QKD die Möglichkeiten der externen Einwirkung auf Akteure des Energiesektors stark begrenzen.[12]

Einordnung des Nutzens für die Digitalisierung

Für eine Beschreibung der Funktionskategorien siehe Seite 12



+

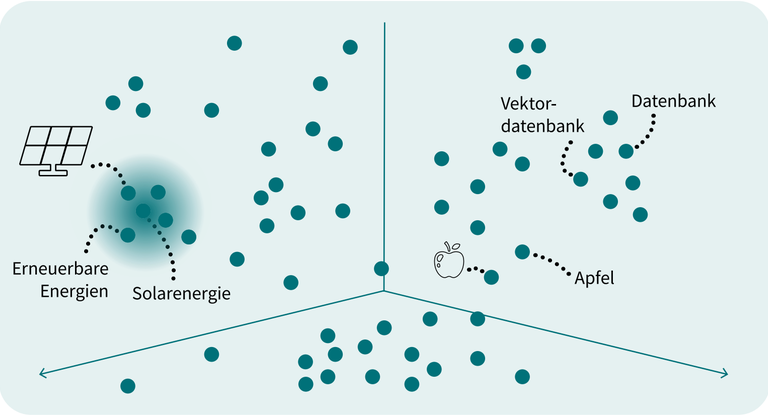
Alle, die mehr zum Thema Quantentechnologien in der Energiewirtschaft erfahren wollen, sind hier genau richtig.

7 Fraunhofer-Institut für System- und Innovationsforschung (ISI) & Universität des Saarlandes (2024): Monitoring Bericht 1. Quantenkommunikation
8 Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2021): Kryptografie quantensicher gestalten. Grundlagen, Entwicklungen, Empfehlungen
9 https://www.chemie.de/lexikon/Dekoh%C3%A4renz.html (abgerufen: 05.12.2024)
10 https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube (abgerufen: 21.02.2025)
11 https://quantenrepeater.link/ (abgerufen: 05.12.2024), siehe auch https://www.uni-jena.de/234982/satelliten-fuer-die-quantenkommunikation (abgerufen: 05.12.2024)
12 https://www.iof.fraunhofer.de/de/presse-medien/pressemitteilungen/2024/Projekt-MANTIS-Cyberangriffe-auf-Gasleitsysteme-verhindern.html (abgerufen: 05.12.2024), siehe auch https://qunet-initiative.de/ (abgerufen: 05.12.2024)

Vektordatenbanken

Die Menge an unstrukturierten Daten, zu denen Audio-, Video-, Text- und viele andere Dokumente gehören, wächst stetig. Laut einigen Einschätzungen sind 80 bis 90 Prozent aller Informationen heutzutage unstrukturiert.[1] Ihre Menge und Vielfalt bringen große organisatorische und sicherheitstechnische Herausforderungen mit sich.

Als zentrale Werkzeuge für die Verwaltung, Speicherung und Organisation von großen Datenmengen dienen Datenbanken. Die Verarbeitung unstrukturierter Daten für die Speicherung in traditionellen relationalen Datenbanksystemen gestaltet sich jedoch oft aufwendig und ineffizient. Eine vielversprechende Alternative bieten Vektordatenbanken. Im Gegensatz zu relationalen Datenbanken, die primär für die Verarbeitung strukturierter Daten in Tabellen konzipiert sind, können Vektordatenbanken auch unstrukturierte oder semistrukturierte Daten effizient verarbeiten.[2]



Aus technischer Sicht sind die Vektordatenbanken speziell für die Speicherung, Verwaltung und Abfrage hochdimensionaler Vektoren optimiert.[3] Jede Dimension stellt eine Dateneigenschaft dar, sodass hochdimensionale Vektoren komplexe und vielfältige Informationen kodieren können. Vektoren repräsentieren einen spezifischen Datentyp, bei dem Daten in Form geordneter Arrays – üblicherweise bestehend aus Gleitkommazahlen – gespeichert werden. Diese Zeichenreihen können unterschiedliche Elemente wie zum Beispiel Objekte, Sätze, Wörter oder Bilder darstellen und ermöglichen die Gruppierung von Datenelementen basierend auf Ähnlichkeiten.

Um die Verarbeitung und das Verständnis der Informationen in Vektorform zu verbessern, werden diese Elemente in sogenannte Einbettungen (engl. Embeddings) umgewandelt. Dabei handelt es sich um mehrdimensionale Datensätze, die die Elemente in numerischer Form darstellen und somit ihre Merkmale und Beziehungen mathematisch abbilden.[4]

Technologietyp: **Software** | Hardware | Konzept/Strategie

Einfluss auf Daten: Erfassung | Übertragung | **Speicherung** | **Verarbeitung**

Technology Readiness / Etablierung in:
5–10 Jahren[5]

Verwandte Themen:
- Maschinelles Lernen
- Natural Language Processing
- Large Language Model (LLM)
- Retrieval-Augmented Generation (RAG)

1 https://www.all-about-security.de/alles-ueber-unstrukturierte-daten/ (abgerufen: 31.10.2024)

2 https://www.ibm.com/de-de/topics/vector-database (abgerufen: 31.10.2024)

3 Reinking, E., & Becker, M. (2024): Large Language Modelle und unternehmenseigene Daten – Genauere Abfrageergebnisse dank effizientem Datenmanagement und verbesserten technischen Verfahren. IUCF Working Paper, No. 3/2024. ZBW – Leibniz Information Centre for Economics, Kiel, Hamburg [online]. Verfügbar unter: https://www.econstor.eu/bitstream/10419/285313/1/Reinking-Becker-Large-Language-Modelle.pdf (abgerufen: 04.11.2024)

4 https://aws.amazon.com/de/what-is/embeddings-in-machine-learning/ (abgerufen: 01.11.2024)

5 https://www.gartner.com/en/documents/5573927 (abgerufen: 31.01.2025)

Auf diese Weise können große Datenmengen basierend auf Ähnlichkeiten geclustert werden, wodurch die Erfassung von Bedeutung und Kontext komplexer Objekte ermöglicht wird. Die Vektoreinbettungen werden mithilfe von Algorithmen indexiert und abgefragt.[6] Dieses Darstellungsprinzip ist vergleichbar mit einer Karte, auf der Objekte in räumlicher Nähe zueinander dargestellt werden. Das ermöglicht eine effiziente Suche, weil dabei der zeitaufwendige Schritt-für-Schritt-Vergleich einzelner Zahlen entfällt. Stattdessen wird ein Algorithmus verwendet, der systematisch und effizient nach Zahlen in räumlicher Nähe sucht. Zu den Methoden der Berechnung von Ähnlichkeits- oder Distanzmetriken gehören unter anderem die Kosinus-Ähnlichkeit oder die euklidische Distanz. Grundsätzlich gilt: Je näher zwei Vektoren beieinanderliegen, desto größer ist ihre Ähnlichkeit.[7]

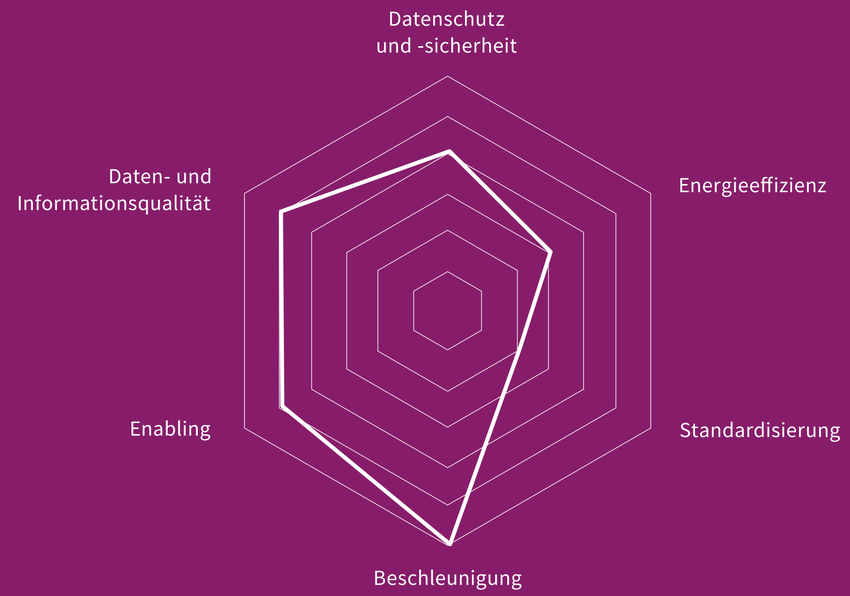
Auf dem Markt gibt es heutzutage zahlreiche Vektordatenbanklösungen, darunter Pinecone, Weaviate, ChromaDB, Qdrant, Vespa und andere. Zwar ist diese vielversprechende Technologie schon im Einsatz, sie bringt im Vergleich zu traditionellen Datenbanken allerdings einige Herausforderungen mit sich. Der Betrieb von Vektordatenbanken ist mit einem hohen Rechenaufwand verbunden, was eine entsprechend leistungsfähige Infrastruktur erfordert. Zudem kann die datenschutzrechtliche Frage bei der Überarbeitung und Speicherung der sensiblen Informationen ein Problem darstellen. Weiterhin ist die Anzahl der Elemente bei der Suche unvorhersehbar, sodass die Suchergebnisse für Menschen in manchen Fällen schwer verständlich sein können.[8] Darüber hinaus müssen auch einige technische Aspekte von Vektordatenbanken wie Sicherheit, Resilienz oder Betriebsunterstützung weiterentwickelt werden, um die Technologie für die öffentliche Nutzung zu implementieren.[9]

Mehrdimensionale Vektordatenbanken werden vor allem für die Speicherung großer Datenmengen sowie für die Suche nach Ähnlichkeiten benutzt, zum Beispiel ähnliche Konzepte, Bilder oder Dokumente.[10] Neben diesen standardmäßigen Anwendungsfeldern bieten diese Datenbanken eine Reihe weiterer Einsatzmöglichkeiten.

Vektordatenbanken können generative KI-Modelle ergänzen und sind für maschinelles Lernen, die Verarbeitung natürlicher Sprache (Natural Language Processing) und andere KI-Aufgaben, die auch in der Energiewirtschaft Anwendung finden, unerlässlich. Sie können eine externe Wissensbasis für KI bereitstellen und gewährleisten, dass sie vertrauenswürdige Informationen enthält.[11] Da die Vektordatenbanken die Speicherung und Suche von Datenpunkten in Form von Vektoren ermöglichen, sind sie für die Effizienz und Genauigkeit von RAG-Systemen (Retrieval-Augmented Generation) und Large Language Models (LLMs) entscheidend. Beide werden beispielsweise für Prognosen, Effizienzsteigerung und Predictive Maintenance in der Energiewirtschaft genutzt.[12] Darüber hinaus können die Vektordatenbanken Datenräume bereichern, indem sie semantische Suchmechanismen, KI-gestützte Analysen und personalisierte Datenverarbeitung ermöglichen.

Einordnung des Nutzens für die Digitalisierung

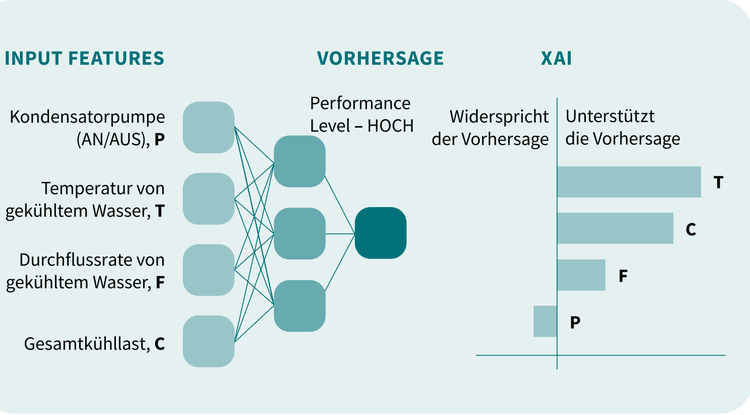
Für eine Beschreibung der Funktionskategorien siehe Seite 12



6 https://www.elastic.co/de/what-is/vector-database (abgerufen: 08.11.2024)
7 https://learn.microsoft.com/de-de/fabric/real-time-intelligence/vector-database (abgerufen: 11.11.2024)
8 https://digitaleprofis.de/kuenstliche-intelligenz/wiki/was-sind-vektordatenbanken/#:~:text=Trotz%20ihrer%20Vorteile%20gibt%20es,ben%C3%B6tigt%20entsprechende%20Infrastruktur%20%E2%80%93%20oder%20Budget (abgerufen: 06.11.2024)
9 https://aws.amazon.com/de/what-is/vector-databases/ (abgerufen: 13.11.2024)
10 https://aiti.ai/vektordatenbanken-in-der-datenwelt/ (abgerufen: 13.11.2024)
11 https://aws.amazon.com/de/what-is/vector-databases/ (abgerufen: 11.11.2024)
12 https://stxnext.com/blog/future-of-informed-decision-making-in-energy-sector (abgerufen: 14.11.2024)

Explainable AI (XAI)

Die Nachvollziehbarkeit der Ergebnisse von auf Künstlicher Intelligenz (KI) basierenden Algorithmen stellt eine große Herausforderung dar. Die hohe Komplexität vieler Modelle resultiert in einem nicht interpretierbaren Blackbox-Prozess. So ist für Menschen nicht ersichtlich, warum gewisse Entscheidungen getroffen werden. Gerade in kritischen Anwendungen können maschinelle Fehlentscheidungen gravierende Auswirkungen mit sich bringen, wie beispielsweise die Wiedergabe von strukturellem Rassismus aufgrund von systematischen Fehlern (Bias) in Trainingsdaten.[1] Um dieser fehlenden Transparenz zu begegnen, werden unter dem Begriff **Erklärbare KI (Explainable Artificial Intelligence, XAI)** Methoden entwickelt, die die Ergebnisse und Ausgaben von Algorithmen des maschinellen Lernens (ML) für Menschen verständlich aufarbeiten sollen. Das Ziel besteht darin, durch das Aufzeigen interner Prozesse zu erläutern, wie das Modell Entscheidungen trifft.[2]



Für die Ausgaben solcher Erklärungsmethoden existieren verschiedene Darstellungsmöglichkeiten, abhängig davon, ob eine einzelne Entscheidung oder das Modell an sich erklärt werden soll. Viele gängige Methoden basieren beispielsweise auf dem Aufzeigen der Relevanz einzelner Modell-Merkmale (Features) für eine bestimmte Entscheidung. Dadurch kann nachvollzogen werden, welche Features am stärksten zur erzielten Modellentscheidung beigetragen haben. Expertinnen und Experten können dann anhand dieser Erkenntnisse die tatsächliche Relevanz dieser Features überprüfen. Hat das Modell das gelernt, was man ihm beibringen wollte, oder kommt es aufgrund einer Überanpassung (Overfitting) an die Trainingsdaten zu falschen Rückschlüssen? Die Erkennung solcher Fehler, wie die unzureichende Generalisierung von trainiertem Wissen, hilft KI-Entwicklerinnen und -Entwicklern bei der Optimierung von Modellen.[3]

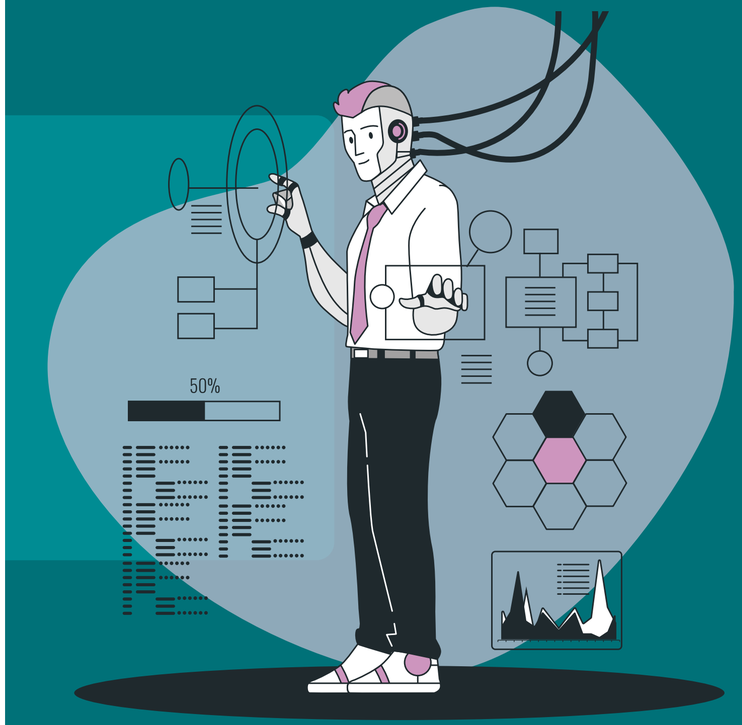
Da die Ausgabe von ML-Modellen auf der Extrahierung von Korrelationen zwischen verschiedenen Features basiert, Korrelation jedoch nicht automatisch Kausalität impliziert, ist das Finden von kausalen Zusammenhängen bzw. die Plausibilisierung der erlernten Muster ein wichtiges Ziel von XAI. Durch das Testen der Übertragbarkeit von Modellen können die Grenzen des Anwendungsbereichs aufgezeigt werden. Um die Vertrauenswürdigkeit von KI-Systemen zu erhöhen, müssen ihre Funktionsweise und ihre Gütekriterien wie Robustheit, Stabilität und Reproduzierbarkeit bestmöglich für die Nutzerinnen und Nutzer aufgearbeitet werden.

Technologietyp: **Software** | Hardware | Konzept/Strategie

Einfluss auf Daten: Erfassung | Übertragung | Speicherung | **Verarbeitung**

Technology Readiness / Etablierung in:
2–5 Jahren[4]

Verwandte Themen:
- Overfitting (Überanpassung)
- Shapley Additive Explanations (SHAP)
- Local Interpretable Model-Agnostic Explanations (LIME)



1 Angwin, J., Larson, J., Mattu S., & Kirchner, L.: Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks [online]. Verfügbar unter: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (abgerufen: 31.10.2024)

2 https://www.ibm.com/de-de/topics/explainable-ai (abgerufen: 31.10.2024)

3 Schaaf, N., Wiedenroth, S. J., & Wagner, P. (2021): Erklärbare KI in der Praxis: Anwendungsorientierte Evaluation von XAI-Verfahren. Fraunhofer IPA

4 https://www.gartner.com/en/articles/hype-cycle-for-artificial-intelligence (abgerufen: 31.01.2025)

Ein KI-Modell lernt nicht mehr als das, was es aus seinen Trainingsdaten extrahieren kann, weshalb auch das Aufdecken eines möglichen Bias einen wichtigen Faktor bei der Beurteilung von Modellentscheidungen darstellt.[5] Es sei jedoch darauf hingewiesen, dass auch für XAI die Gefahr von böswilligen Manipulationen mit dem Ziel der Täuschung von Nutzerinnen und Nutzern besteht. Entsprechende Methoden zur Abwehr derartiger Angriffe (Adversarial Attacks) existieren bereits und sollten gegebenenfalls berücksichtigt werden.[6]

Für den Gesundheitssektor wird die Integration einer hinreichenden Erklärbarkeit in weiten Teilen als Grundvoraussetzung für die Etablierung von KI-Anwendungen angesehen. Doch auch die Energiebranche sieht einen hohen Bedarf an Erklärbarkeit. Als Kritische Infrastruktur erfordert das Energiesystem einen hohen Grad an Zuverlässigkeit integrierter Technologien. Fehlendes Vertrauen in KI-basierte Entscheidungen oder Empfehlungen hindert daher oft deren praktischen Einsatz. In Anwendungen zur Analyse der Systemstabilität in Stromnetzen, wie der Spannungs- oder Frequenzhaltung, kann XAI wichtige Erklärungen zu Modellprognosen liefern, um deren Nachvollziehbarkeit zu erhöhen. Bei Last- und Erzeugungsprognosen kann XAI dabei helfen, die Relevanz einzelner Features zu verstehen und dadurch die Modellgenauigkeit zu steigern. Weitere Anwendungen finden sich in Energiemanagementsystemen von Gebäuden, in der Netzüberwachung und -regelung, im Cybersecurity-Monitoring und in vielen weiteren Fällen, in denen der Einsatz von KI trotz hervorragender Ergebnisse bisher gehemmt wird.[7]

Die beiden meistgenutzten XAI-Methoden im Energiesystem sind SHAP (Shapley Additive Explanations) und LIME (Local Interpretable Model-Agnostic Explanations).[7] SHAP ist ein spieltheoretischer Ansatz, bei dem die Relevanz einzelner Features anhand der Betrachtung aller möglichen Feature-Kombinationen ermittelt wird. Das Prinzip von LIME basiert auf einer lokalen Annäherung eines komplexeren Modells, sodass konkrete Ergebnisbereiche vereinfacht dargestellt werden können.[8]

+

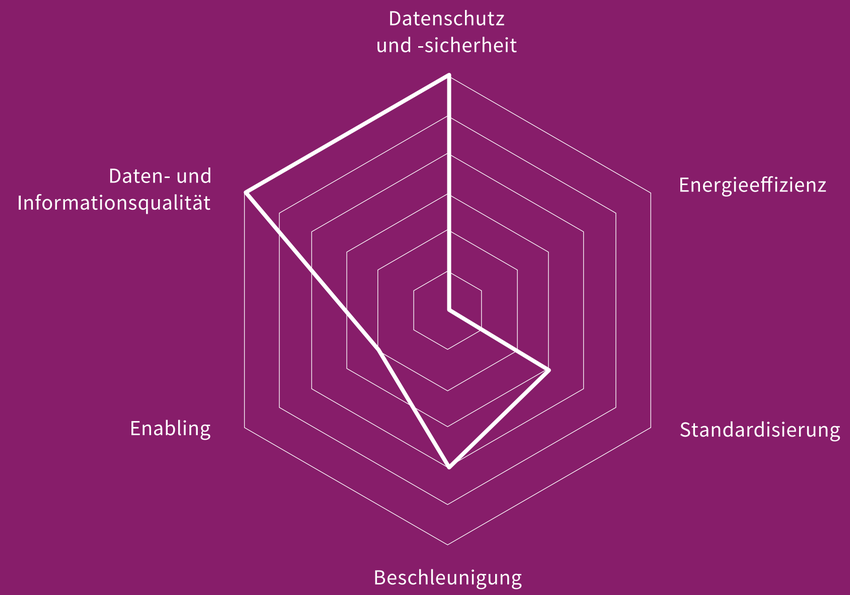
Für weitere Infos zum Thema KI können Sie gern auch noch hier vorbeischauen:

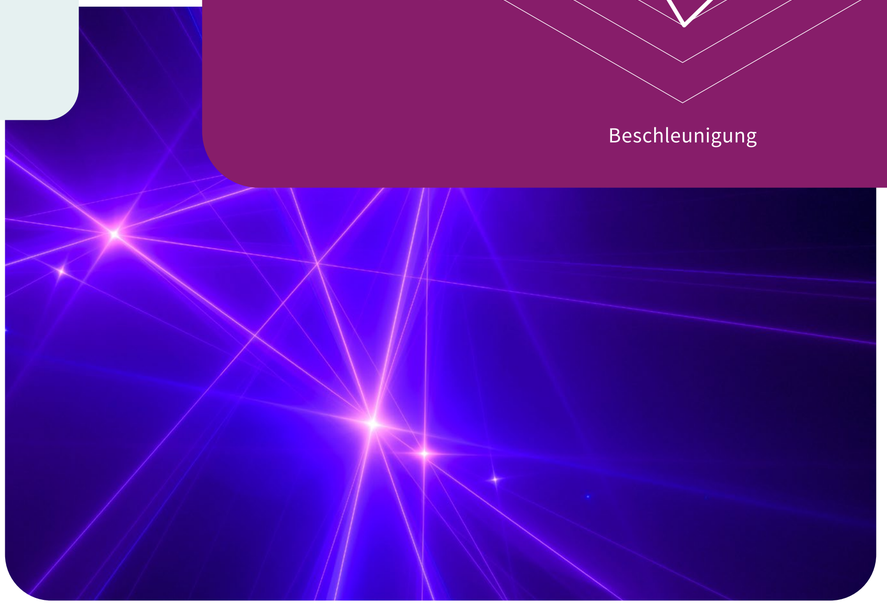
Energieeffiziente KI

KI in Fernwärme

Einordnung des Nutzens für die Digitalisierung

Für eine Beschreibung der Funktionskategorien siehe Seite 12





5 Kraus, T., Ganschow, L., Eisenträger, M., & Wischmann, S. (2021): Erklärbare KI: Anforderungen, Anwendungsfälle und Lösungen

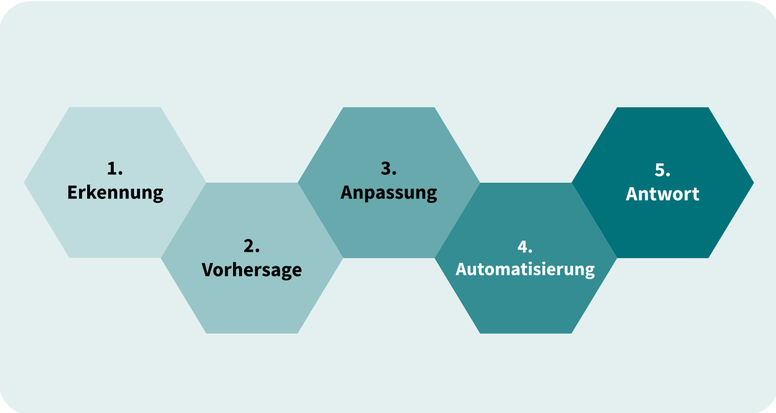
6 Baniecki, H., & Biecek, P. (2024): Adversarial attacks and defenses in explainable artificial intelligence: A survey. Information Fusion, 102303

7 Machlev, R., Heistrene, L., Perl, M., Levy, K. Y., Belikov, J., Mannor, S., & Levron, Y. (2022): Explainable Artificial Intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities. Energy and AI, 9, 100169

8 Baniecki, H., & Biecek, P. (2024): Adversarial attacks and defenses in explainable artificial intelligence: A survey. Information Fusion, 102303

AI for Cybersecurity

Die stark fortschreitenden Entwicklungen in der Künstlichen Intelligenz (KI) werden auch zunehmend von Cyberkriminellen ausgenutzt, um ihre Angriffe zu optimieren. Beispiele hierfür sind die KI-basierte Automatisierung von Cyberangriffen, die Erstellung qualitativ hochwertiger Phishing-Mails, die Entwicklung schwer erkennbarer Malware oder die Erforschung und Identifizierung von Angriffszielen. Obwohl KI dadurch einerseits für kriminelle Zwecke missbraucht werden kann, kann sie andererseits auch zum Schutz vor Cyberangriffen eingesetzt werden. AI for Cybersecurity (KI für Cybersicherheit) nutzt Algorithmen des maschinellen Lernens (ML), um große Mengen an Daten aus IT-Systemen zu analysieren, Muster zu erkennen und anormales Verhalten zu identifizieren. Auf Basis dessen können weitere (menschliche) Untersuchungen oder bestenfalls automatisierte Gegenmaßnahmen eingeleitet werden. Generative KI kann Cyberbedrohungen nach der Bedrohungsanalyse in Form von Texten oder Bildern aufbereiten, visualisieren und darstellen und so die Spezialistinnen und Spezialisten im Bereich Cybersicherheit bei der schnelleren Identifizierung und Behebung von Angriffen unterstützen.[1]



Zur Aufdeckung und Prävention von bereits bekannten Cyberbedrohungen eignen sich ML-Modelle des überwachten Lernens (Supervised Learning), die mit klassifizierten Datensätzen trainiert werden. Zuvor unbekannte Cyberbedrohungen können mittels Methoden des unüberwachten Lernens (Unsupervised Learning) erfasst werden, indem das Modell Muster in unsignierten Daten identifiziert und außergewöhnliche Aktivitäten feststellt. Auch wenn KI Cybersicherheitsexpertinnen und -experten nicht ersetzen kann, kann sie die Bearbeitung gewisser Aufgaben automatisieren. Auf diese Weise werden Freiräume für das Personal entstehen, sich stärker auf strategische Fragen zu fokussieren. Dadurch können vermehrt proaktive Ansätze im Umgang mit Cyberbedrohungen verfolgt werden. Weiterhin bietet KI die Möglichkeit, Reaktionszeiten zu verkürzen und Fehleralarme zu reduzieren.[ebd.]

Der Schutz vor Cyberangriffen im Energiesektor stellt eine besondere Herausforderung dar. KI kann als Ergänzung zu menschlicher Expertise bei der Erkennung und Verhinderung verschiedener Angriffsarten sowie bei der Reaktion darauf einen wichtigen Beitrag zur Erhöhung der Cybersicherheit leisten. Angriffe können beispielsweise darauf abzielen, Zugriff auf vertrauliche Informationen sowie die Steuerung von Energieerzeugung und -verteilung zu erlangen. Integritätsangriffe versuchen, Messdaten von Netzkomponenten zu verändern (False Data Injection), um Schäden im System zu verursachen und Vertrauen zu untergraben. Auch Angriffe auf die Verfügbarkeit sind gängige Methoden, um autorisierten Personen den Zugang zu bestimmten Diensten zu erschweren oder zu

1 https://www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity (abgerufen: 29.11.2024)

Technologietyp: **Software** Hardware Konzept/Strategie

Einfluss auf Daten: Erfassung Übertragung Speicherung **Verarbeitung**

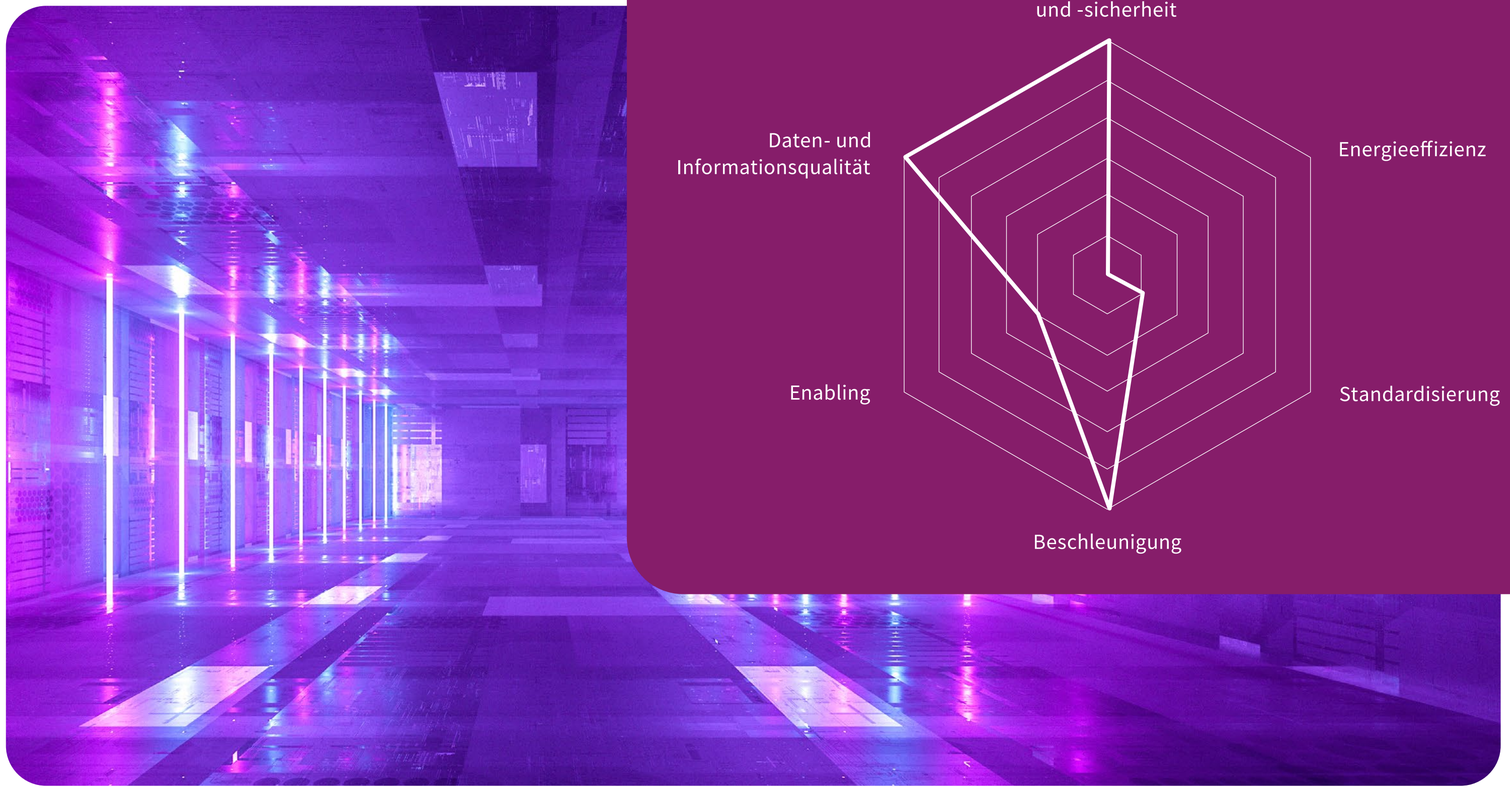
Technology Readiness / Etablierung in:
5–10 Jahren

Verwandte Themen:
- False Data Injection Attacks (FDIA)
- Graph Convolutional Network (GCN)
- Supervised Learning
- Unsupervised Learning

verweigern.[2] Die Hauptaufgaben eines KI-Modells umfassen dabei die Identifizierung von Schwachstellen im System oder die Erkennung von auffälligen Mustern, die auf einen möglichen Cyberangriff hindeuten.[3] Der Einsatz von XAI-Methoden kann wiederum dabei helfen, Angriffe auf KI-Systeme zu identifizieren.[4]

Aufgrund der großen Menge an Daten im Energiesystem, die zur Systemüberwachung herangezogen werden können, zeigen insbesondere Deep-Learning-Modelle vielversprechende Ergebnisse bei der Identifizierung komplexer Cyberbedrohungen.

False Data Injection Attacks (FDIAs) gelten als eine der häufigsten Cyberangriffsarten in Energienetzen. Eine Manipulation von Messdaten kann die Systemsicherheit massiv beeinträchtigen, wenn Netzbetreiber Entscheidungen auf Basis einer falschen Netzzustandsschätzung treffen. Mit ausreichend netztechnischer Expertise können Messwerte von Betriebsparametern wie Spannung, Phasenlage oder Wirk- und Blindleistungsflüssen unbemerkt beeinflusst werden. Zur Identifizierung derartiger Bedrohungen eignen sich Ansätze, die die Netztopologie und damit die räumlichen Korrelationen der Stromnetzdaten einbeziehen. Mittels Modellierung des Stromnetzes mit seinen Leitungsadmittanzen als gewichtetem Graph kann ein Graph Convolutional Network (GCN) zur Erkennung von FDIAs trainiert werden. Als Eingangsdaten in das GCN dienen die Wirk- und Blindleistungswerte an den Netzknoten. Das Modell wird mit klassifizierten Daten trainiert, die entweder einen unveränderten oder einen manipulierten Zustand indizieren. Ein einsatzbereites Modell kann daraufhin Angriffe auf die Integrität von Messdaten innerhalb weniger Millisekunden mit einer hohen Aufdeckungsrate und einer niedrigen Anzahl an Fehlalarmen erfassen.[5] Es ist zu erwarten, dass die Weiterentwicklung effektiver und robuster KI-basierter Abwehrmechanismen wie diesem mit zunehmender Digitalisierung des Energiesystems weiter an Bedeutung gewinnen wird.



Einordnung des Nutzens für die Digitalisierung

Für eine Beschreibung der Funktionskategorien siehe Seite 12

2 Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022): Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. International Journal of Critical Infrastructure Protection, 38, 100547

3 Sarker, I.H. (2024): AI for Critical Infrastructure Protection and Resilience. In: AI-Driven Cybersecurity and Threat Intelligence. Springer, Cham

4 Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F., & Dong, Z. Y. (2023): Deep learning for cybersecurity in smart grids: Review and perspectives. Energy Conversion and Economics, 4(4), 233-251

5 Boyaci, O., Narimani, M. R., Davis, K., & Serpedin, E. (2022): Cyberattack detection in large-scale smart grids using chebyshev graph convolutional networks. In: 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE) (pp. 217-221). IEEE

Zusammenfassung

Für die von uns vorgestellten Technologien gilt gleichermaßen, dass sie zu einem Umdenken auf ihren jeweiligen Gebieten und zu wegweisenden Veränderungen führen können.

Quantenkommunikation ermöglicht durch die Verwendung von Qubits eine andere Herangehensweise bei der Umsetzung von Informationssicherheit und löst eines der größten Probleme gängiger Verschlüsselungsverfahren: effizientere Entschlüsselung durch eine Veränderung der Rechnerarchitektur. Zudem sorgt sie auch für eine bessere Nachvollziehbarkeit von Eingriffen in die Datenübertragung. Dadurch hebt sie bisher unerschlossene Potenziale bei der Sicherheit der Datenübertragung, insbesondere für die Kritische Infrastruktur und möglicherweise auch darüber hinaus.

Um der steigenden Qualität von Cyberangriffen angemessen begegnen zu können, ist eine Verbesserung der Sicherheitsmaßnahmen notwendig. Diese gewährleistet AI for Cybersecurity durch die Identifikation von anormalem Verhalten und Schwachstellen in IT-Systemen. Mittels einer verständlicheren Darstellung von Bedrohungen und der Automatisierung von Arbeitsschritten ermöglicht sie außerdem eine schnellere Reaktion auf Angriffe und erleichtert die Arbeit des Cybersecurity-Personals. Im Energiesektor schafft AI for Cybersecurity damit die Grundlage für eine hohe Versorgungssicherheit.

Mit der steigenden Relevanz und Vielseitigkeit des Einsatzes von KI ist auch eine Stärkung des Vertrauens in diese Technologie notwendig. XAI ist für die Erreichung dieses Ziels ein vielversprechender Ansatz. Durch die Erklärung einzelner Entscheidungen bis hin zu Entscheidungskriterien von Modellen wird deren Überprüfbarkeit gewährleistet. Dies eröffnet in Kombination mit einer nachvollziehbaren Darstellung der gelernten Muster der Modelle neue Perspektiven für die transparente Gestaltung von KI-Modellen mit neuen Erkenntnissen und einem bewussten Umgang ihrer Nutzerinnen und Nutzer. Großes Anwendungspotenzial gibt es besonders im Kontext von Prognosen zur Energieerzeugung, zu Netzlasten und zur Netzstabilität.

In diesem Zusammenhang stellt sich auch die Frage nach dem Umgang mit großen Datenmengen, insbesondere wenn Daten unstrukturiert vorliegen. Eine mögliche Antwort bieten Vektordatenbanken. Durch die räumliche Nähe ähnlicher Objekte innerhalb einer Datenbank lassen sich Suchoperationen effizienter gestalten. Somit bilden Vektordatenbanken eine wichtige Grundlage für maschinelles Lernen und die Bereitstellung von Daten für generative KI.

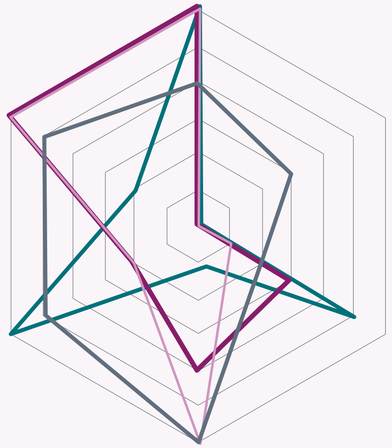
Zusammenfassung und Beschreibung der Funktionskategorien

Datenschutz und -sicherheit

Datenschutz bezieht sich auf die Verhinderung der missbräuchlichen Verwendung personenbezogener Daten nach rechtlichen Vorgaben und die Ermöglichung der Selbstbestimmung über die eigenen Informationen der betroffenen Person. Datensicherheit gewährleistet den Schutz von Daten vor Verlust, Verfälschung, Beschädigung oder unautorisiertem Zugriff.

Daten- und Informationsqualität

Die Qualität von Daten und Informationen bemisst sich an der Passgenauigkeit für ihre vorgesehene Anwendung. Die dabei vordergründig relevanten Merkmale der Daten und Informationen sind die Vollständigkeit, Aktualität und Einheitlichkeit sowie die Widerspruchs- und Fehlerfreiheit.



Energieeffizienz

Energieeffizienz ist das Verhältnis eines Nutzens (z. B. einer Anzahl durchgeführter Berechnungen eines Computers) zu der dazu notwendigen Energie. Durch eine erhöhte Energieeffizienz kann bei gleichbleibendem Nutzen Energie eingespart oder bei gleichem Energieverbrauch der Nutzen erhöht werden (Rebound-Effekt).

Enabling

Durch disruptive Innovationen und Technologien können die Voraussetzungen für vollkommen neue oder signifikant veränderte Produkte oder Prozesse geschaffen werden. Beispielsweise sind Bike- oder Carsharing-Angebote in ihrer heutigen Flexibilität nur durch digitale Ortungsdienste möglich geworden.

Standardisierung

Standardisierung beschreibt die Festlegung von gemeinsamen Spezifikationen für Produkte, Dienstleistungen und Prozesse mehrerer Personen oder Institutionen. Dadurch können die Interoperabilität und Vergleichbarkeit der standardisierten Elemente erhöht werden.

Beschleunigung

Beschleunigung beschreibt die Zunahme der Geschwindigkeit von beispielsweise administrativen Prozessen, der Datenübertragung oder computergestützten Berechnungen.

Quantenkommunikation | Vektordatenbanken | Explainable AI | AI for Cybersecurity

Impressum

HERAUSGEBER:
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699
E-Mail: info@dena.de

www.future-energy-lab.de
www.dena.de

AUTORINNEN UND AUTOREN:
Lukas Huttny, dena
Leon König, dena
Maximilian Scholz, dena
Anna Sibirtceva, dena
Jasmin Wagner, dena

KONZEPTION & GESTALTUNG:
The Ad Store GmbH

BILDNACHWEISE:
Titel – Freepik
S. 2 – Freepik/rawpixel
S. 3, 4, 6, 8, 10 – dena
S. 5 – Shutterstock
S. 7 – GettyImages/MR.Cole_Photographer
S. 9 – GettyImages/Baac3nes
S. 11 – GettyImages/Gremlin

STAND:
01 / 2025

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

BITTE ZITIEREN ALS:
Deutsche Energie-Agentur (Hrsg.) (dena, 2025):
Future-Energy-Technologiescouting –
Digitale Technologien für die Energiewende

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.


Future Energy
Lab
dena
Deutsche Energie-Agentur