

DIN EN ISO/IEC 23053



ICS 35.020

**Framework für Systeme der künstlichen Intelligenz (KI) basierend auf
maschinellern Lernen (ML) (ISO/IEC 23053:2022);
Deutsche Fassung EN ISO/IEC 23053:2023**

Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
(ISO/IEC 23053:2022);
German version EN ISO/IEC 23053:2023

Cadre méthodologique pour les systèmes d'intelligence artificielle (IA) utilisant
l'apprentissage machine (ISO/IEC 23053:2022);
Version allemande EN ISO/IEC 23053:2023

Gesamtumfang 47 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 23053:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 23053:2023 durch das Technische Komitee CEN/CLC/JTC 21 „Künstliche Intelligenz“ übernommen, dessen Sekretariat von DS (Dänemark) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-01-42 GA „DIN/DKE Gemeinschaftsarbeitsausschuss Künstliche Intelligenz“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokument wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 17789	siehe	DIN ISO/IEC 17789
ISO/IEC 22989	siehe	DIN EN ISO/IEC 22989

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 22989, *Informationstechnik — Künstliche Intelligenz — Konzepte und Terminologie der Künstlichen Intelligenz*

DIN ISO/IEC 17789, *Informationstechnik — Cloud Computing — Referenzarchitektur*

– Leerseite –

Deutsche Fassung

Framework für Systeme der künstlichen Intelligenz (KI) basierend auf maschinellem Lernen (ML) (ISO/IEC 23053:2022)

Framework for Artificial Intelligence (AI) Systems Using
Machine Learning (ML) (ISO/IEC 23053:2022)

Cadre méthodologique pour les systèmes d'intelligence
artificielle (IA) utilisant l'apprentissage machine
(ISO/IEC 23053:2022)

Diese Europäische Norm wurde vom CEN am 26. Juni 2023 angenommen.

Die CEN- und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN- und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
3.1 Modellentwicklung und -nutzung	7
3.2 Tools	8
3.3 Daten	8
4 Abkürzungen	9
5 Überblick	10
6 Maschinelles Lernsystem	10
6.1 Überblick	10
6.2 Aufgabe	11
6.2.1 Allgemeines	11
6.2.2 Regression	12
6.2.3 Klassifizierung	12
6.2.4 Clustering (Gruppenzuordnung)	13
6.2.5 Erkennung von Anomalien	13
6.2.6 Dimensionalitätsverringierung	13
6.2.7 Andere Aufgaben	13
6.3 Modell	14
6.4 Daten	14
6.5 Tools	16
6.5.1 Allgemeines	16
6.5.2 Datenaufbereitung	16
6.5.3 Kategorien von ML-Algorithmen	16
6.5.4 ML-Optimierungsverfahren	21
6.5.5 ML-Bewertungsmetriken	23
7 Ansätze für maschinelles Lernen	26
7.1 Allgemeines	26
7.2 Überwachtes maschinelles Lernen	27
7.3 Unüberwachtes maschinelles Lernen	29
7.4 Teilüberwachtes maschinelles Lernen	29
7.5 Selbstüberwachtes maschinelles Lernen	30
7.6 Bestärkendes maschinelles Lernen	30
7.7 Transfer-Learning	31
8 Pipeline des maschinellen Lernens	32
8.1 Allgemeines	32
8.2 Datenerfassung	33
8.3 Datenaufbereitung	34
8.4 Modellierung	36
8.5 Verifizierung und Validierung	37
8.6 Bereitstellung des Modells	38
8.7 Betrieb	38
8.8 Beispiel für einen maschinellen Lernprozess auf der Grundlage der ML-Pipeline	39
Anhang A (informativ) Beispielhafte Datenfluss- und Datenverwendungserklärungen für überwachte Lernprozesse	41
A.1 Allgemeines	41
A.2 Datenflüsse im Prozess des überwachten maschinellen Lernens	41
A.2.1 Allgemeines	41

A.2.2	Beschreibungen von Datenflüssen	41
A.3	Datennutzung beim maschinellen Lernen	42
A.3.1	Allgemeines	42
A.3.2	Beispiel für eine Datenverwendungserklärung A	42
A.3.3	Beispiel für eine Datenverwendungserklärung B	42
A.3.4	Beispiel für eine Datenverwendungserklärung C	42
	Literaturhinweise	43

Bilder

Bild 1	— Elemente eines ML-Systems	11
Bild 2	— Konzeptdiagramm: Daten und Datensätze	15
Bild 3	— Beispiele verschiedener Kategorien von ML-Algorithmen	17
Bild 4	— Kurve der Betriebseigenschaften des Empfängers	25
Bild 5	— Konfusionsmatrix	26
Bild 6	— ML-Verfahren, kategorisiert als überwachtes maschinelles Lernen, unüberwachtes maschinelles Lernen und bestärkendes maschinelles Lernen	27
Bild 7	— ML-Modellerstellung durch überwachtes maschinelles Lernen	28
Bild 8	— Typisches überwachtes maschinelles Lernen	28
Bild 9	— ML-Modellerstellung durch unüberwachtes maschinelles Lernen	29
Bild 10	— Typischer Prozess des bestärkenden maschinellen Lernens	31
Bild 11	— Typischer Prozess von Transfer-Learning	32
Bild 12	— Pipeline für maschinelles Lernen und Zuordnung zum Lebenszyklus von KI-Systemen	33
Bild 13	— Beispiel für einen überwachten maschinellen Lernprozess auf der Grundlage der ML-Pipeline	39

Europäisches Vorwort

Der Text von ISO/IEC 23053:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 23053:2023 durch das Technische Komitee CEN/CLC/JTC 21 „Künstliche Intelligenz“ übernommen, dessen Sekretariat von DS gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Dezember 2023, und etwaige entgegenstehende nationale Normen müssen bis Dezember 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 23053:2022 wurde von CEN-CENELEC als EN ISO/IEC 23053:2023 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder der IEC-Liste der erhaltenen Patenterklärungen (siehe patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. Bei IEC siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 42, *Artificial Intelligence* erarbeitet.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

Einleitung

Bei Systemen der künstlichen Intelligenz (KI) handelt es sich im Allgemeinen um technische Systeme, die Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen für eine bestimmte, von Menschen definierte Zielsetzung erzeugen. KI deckt ein breites Spektrum an Technologien ab, die unterschiedliche Ansätze zur Behandlung dieser komplexen Probleme widerspiegeln.

ML ist ein Zweig der künstlichen Intelligenz, der Computertechniken verwendet, um Systeme in die Lage zu versetzen, aus Daten oder Erfahrungen zu lernen. Mit anderen Worten: ML-Systeme werden durch die Optimierung von Algorithmen entwickelt, um sie an Trainingsdaten anzupassen oder ihre Leistung durch die Maximierung einer Belohnung zu verbessern. Zu den ML-Verfahren gehört das tiefe Lernen, das ebenfalls in diesem Dokument behandelt wird.

In diesem Dokument werden Begriffe wie Wissen, Lernen und Entscheidungen verwendet. Es ist jedoch nicht die Absicht, das maschinelle Lernen (ML) zu vermenschlichen.

Ziel dieses Dokuments ist es, ein Framework für die Beschreibung von KI-Systemen zu schaffen, die ML verwenden. Durch die Festlegung einer gemeinsamen Terminologie und eines gemeinsamen Konzepts für solche Systeme bietet dieses Dokument eine Grundlage für die eindeutige Erläuterung der Systeme und verschiedene Überlegungen, die für deren Technik und Verwendung gelten. Dieses Dokument richtet sich an eine breite Zielgruppe, darunter Experten und Nicht-Berufsangehörige. Einige der Abschnitte (die im Überblick in Abschnitt 5 aufgeführt sind) enthalten jedoch ausführlichere technische Beschreibungen.

Dieses Dokument bildet auch die Grundlage für weitere Normen, die sich mit bestimmten Aspekten von ML-Systemen und deren Komponenten befassen.

1 Anwendungsbereich

Dieses Dokument legt ein Framework für künstliche Intelligenz (KI) und maschinelles Lernen (ML) zur Beschreibung eines generischen KI-Systems mit ML-Technologie fest. Das Framework beschreibt die Systemkomponenten und ihre Funktionen im KI-Ökosystem. Dieses Dokument ist für alle Arten und Größen von Organisationen, einschließlich öffentlicher und privater Unternehmen, öffentlicher Stellen und gemeinnütziger Organisationen anwendbar, die KI-Systeme implementieren oder nutzen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 22989 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1 Modellentwicklung und -nutzung

3.1.1

Klassifizierungsmodell

<maschinelles Lernen> maschinelles Lernmodell, dessen erwartete Ausgabe für eine festgelegte Eingabe einer oder mehreren Klassen entspricht

3.1.2

Regressionsmodell

<maschinelles Lernen> maschinelles Lernmodell, dessen erwartete Ausgabe für eine festgelegte Eingabe einer kontinuierlichen Variablen entspricht

3.1.3

Verallgemeinerung

<maschinelles Lernen> Fähigkeit eines trainierten Modells, korrekte Vorhersagen für bis dahin unbekannte Eingabedaten zu treffen

Anmerkung 1 zum Begriff: Ein maschinelles Lernmodell, das sich gut verallgemeinern lässt, verfügt über eine akzeptable Vorhersagegenauigkeit, wenn es bis dahin unbekannte Eingabedaten verwendet.

Anmerkung 2 zum Begriff: Verallgemeinerung ist eng mit Überanpassung verbunden. Ein überangepasstes maschinelles Lernmodell lässt sich nicht gut verallgemeinern, da das Modell zu genau an die Trainingsdaten angepasst ist.

3.1.4

Überanpassung

<maschinelles Lernen> Erstellung eines Modells, das sich zu genau an die Trainingsdaten anpasst und nicht auf neue Daten verallgemeinert werden kann

Anmerkung 1 zum Begriff: Eine Überanpassung kann auftreten, weil das trainierte Modell aus unwesentlichen Merkmalen in den Trainingsdaten gelernt hat (d. h. Merkmale, die sich nicht zu nützlichen Ergebnissen verallgemeinern lassen), weil die Trainingsdaten übermäßig verrauscht sind (z. B. eine übermäßige Anzahl von Ausreißern) oder weil das Modell zu komplex für die Trainingsdaten ist.

Anmerkung 2 zum Begriff: Eine Überanpassung kann festgestellt werden, wenn ein erheblicher Unterschied zwischen den an den Trainingsdaten und den an separaten Test- und Validierungsdaten gemessenen Fehlern besteht. Die Leistung von überangepassten Modellen wird besonders dann beeinträchtigt, wenn eine erhebliche Diskrepanz zwischen Trainingsdaten und Produktionsdaten besteht.

3.1.5

Unteranpassung

<maschinelles Lernen> Erstellung eines Modells, das den Trainingsdaten nicht genau genug entspricht und bei neuen Daten falsche Vorhersagen macht

Anmerkung 1 zum Begriff: Unteranpassung kann auftreten, wenn die Merkmale schlecht ausgewählt sind, die Trainingszeit nicht ausreicht oder das Modell aufgrund einer begrenzten Modellkapazität (d. h. Ausdrucksstärke) zu einfach ist, um aus umfangreichen Trainingsdaten zu lernen.

3.2 Tools

3.2.1

Backpropagation

Trainingsverfahren für neuronale Netze, bei dem der Fehler in der Ausgabeschicht verwendet wird, um die Gewichte für die Verbindungen der aufeinanderfolgenden vorherigen Schichten anzupassen und zu optimieren

3.2.2

Lernrate

Schrittweite für ein Gradientenverfahren

Anmerkung 1 zum Begriff: Die Lernrate bestimmt, ob und wie schnell ein Modell zu einer optimalen Lösung konvergiert, und ist daher ein wichtiger Hyperparameter für neuronale Netze.

3.3 Daten

3.3.1

Klasse

vom Menschen definierte Kategorie von Elementen, die Teil des Datensatzes sind und gemeinsame Attribute haben

BEISPIEL „Telefon“, „Tisch“, „Stuhl“, „Kugellager“ und „Tennisball“ sind Klassen. Die Klasse „Tisch“ umfasst: einen Arbeitstisch, einen Esstisch, einen Schreibtisch, einen Couchtisch, eine Werkbank.

Anmerkung 1 zum Begriff: Klassen sind üblicherweise Zielvariablen und werden durch einen Namen bezeichnet.

3.3.2

Cluster

automatisch ausgelöste Kategorie von Elementen, die Teil des Datensatzes sind und gemeinsame Attribute haben

Anmerkung 1 zum Begriff: Cluster haben nicht unbedingt einen Namen.

3.3.3

Merkmal

<maschinelles Lernen> messbare Eigenschaft eines Objekts oder Ereignisses in Bezug auf eine Reihe von Merkmalen

Anmerkung 1 zum Begriff: Merkmale spielen beim Training und bei der Vorhersage eine Rolle.

Anmerkung 2 zum Begriff: Merkmale bieten eine maschinenlesbare Möglichkeit, die relevanten Objekte zu beschreiben. Da der Algorithmus nicht auf die Objekte oder Ereignisse selbst zurückgreift, sind die Merkmalsdarstellungen so gestaltet, dass sie alle nützlichen Informationen enthalten.

3.3.4

Abstand

<maschinelles Lernen> gemessene Nähe zweier Punkte im Raum

Anmerkung 1 zum Begriff: Beim maschinellen Lernen wird üblicherweise der euklidische bzw. geradlinige Abstand verwendet.

3.3.5

unmarkiert

Eigenschaft eines Samples, das keine Zielvariable enthält

4 Abkürzungen

KI	künstliche Intelligenz
API	Anwendungsprogrammierschnittstelle (en: application programming interface)
AUC	Fläche unter der Kurve (en: area under the curve)
BM	Boltzmann-Maschinen
CapsNet	neuronales Kapselnetz (en: capsule neural network)
CG	konjugierter Gradient (en: conjugate gradient)
CNN	faltendes neuronales Netz (en: convolutional neural network)
DBN	tiefe Vertrauensnetze (en: deep belief networks)
DCNN	tiefes faltendes neuronales Netz (en: deep convolutional neural network)
FFNN	neuronales Vorwärtsnetz (en: feed forward neural network)
FNR	Falsch-Negativ-Rate
FPR	Falsch-Positiv-Rate
GRU	Gated Recurrent Unit
LSTM	langes Kurzzeitgedächtnis (en: long short-term memory)
MAE	mittlerer absoluter Fehler (en: mean absolute error)
MEP	Markow-Entscheidungsprozess
ML	maschinelles Lernen
NN	neuronales Netz
NNEF	Datenaustauschformat für künstliche neuronale Netze (en: neural network exchange format)
NPV	negativer Vorhersagewert (en: negative predictive value)
ONNX	offenes Format zur Darstellung von Deep-Learning-Modellen (en: open neural network exchange)
PCA	Hauptkomponentenanalyse (en: principal component analysis)
PHI	persönliche oder geschützte Gesundheitsinformationen (en: personal or protected health information)

pbD	personenbezogene Daten
PPV	positiver Vorhersagewert (en: positive predictive value)
REST	repräsentative Zustandsübertragung (en: representational state transfer)
RNN	rekurrentes neuronales Netz
ROC	Betriebseigenschaften des Empfängers (en: receiver operating characteristics)
SGD	stochastischer Gradientenabstieg (en: stochastic gradient descent)
SVM	Stützvektormaschine
TNR	Richtig-Negativ-Rate (en: true negative rate)
TPR	Richtig-Positiv-Rate (en: true positive rate)

5 Überblick

ISO/IEC 22989 definiert ML als den Prozess zur Optimierung von Modellparametern durch computergestützte Verfahren, so dass das Verhalten des Modells den Daten oder Erfahrungen entspricht. Seit den frühen 1940er Jahren werden die Modellierung von Neuronen (d. h. neuronalen Netzen) und die Entwicklung von Computerprogrammen, die aus Daten lernen können, erforscht. ML ist ein expandierendes Gebiet, mit dem Aufkommen neuer Anwendungen in einem breiten Spektrum von Industriezweigen. Dieser Fortschritt wird durch die Verfügbarkeit von großen Datenmengen und Rechenressourcen ermöglicht. Zu den ML-Verfahren gehören neuronale Netze und tiefes Lernen.

In ISO/IEC 22989 wird ein KI-Ökosystem in Form von Funktionsschichten dargestellt, und ML ist eine wichtige Komponente dieses KI-Ökosystems. Bild 1 veranschaulicht das ML-System, das sich in die Komponenten Modell, Software-Tools und -Techniken sowie Daten aufgliedert.

In Abschnitt 6 dieses Dokuments werden die verschiedenen Komponenten des ML-Systems näher beschrieben.

In Abschnitt 7 dieses Dokuments werden verschiedene ML-Ansätze beschrieben und ihre Abhängigkeit von Trainingsdaten erläutert.

In Abschnitt 8 dieses Dokuments wird eine ML-Pipeline beschrieben: die Prozesse, die mit der Entwicklung, dem Einsatz und dem Betrieb eines ML-Modells verbunden sind.

6.5 und Abschnitt 7 sind technischer als der Rest des Dokuments. Ein fundierter technischer Hintergrund kann dem Leser helfen, diese Inhalte besser zu verstehen.

6 Maschinelles Lernsystem

6.1 Überblick

In Bild 1 sind die Elemente eines ML-Systems dargestellt. Sie legen die Rollen und deren ML-spezifische Funktionen fest, die von verschiedenen Entitäten (z. B. verschiedenen Anbietern) implementiert werden können. Die in Bild 1 dargestellten Beispiele sind nicht als erschöpfende Liste zu verstehen. Weitere Erläuterungen zu den einzelnen Rubriken von Bild 1 befinden sich in Abschnitt 6.

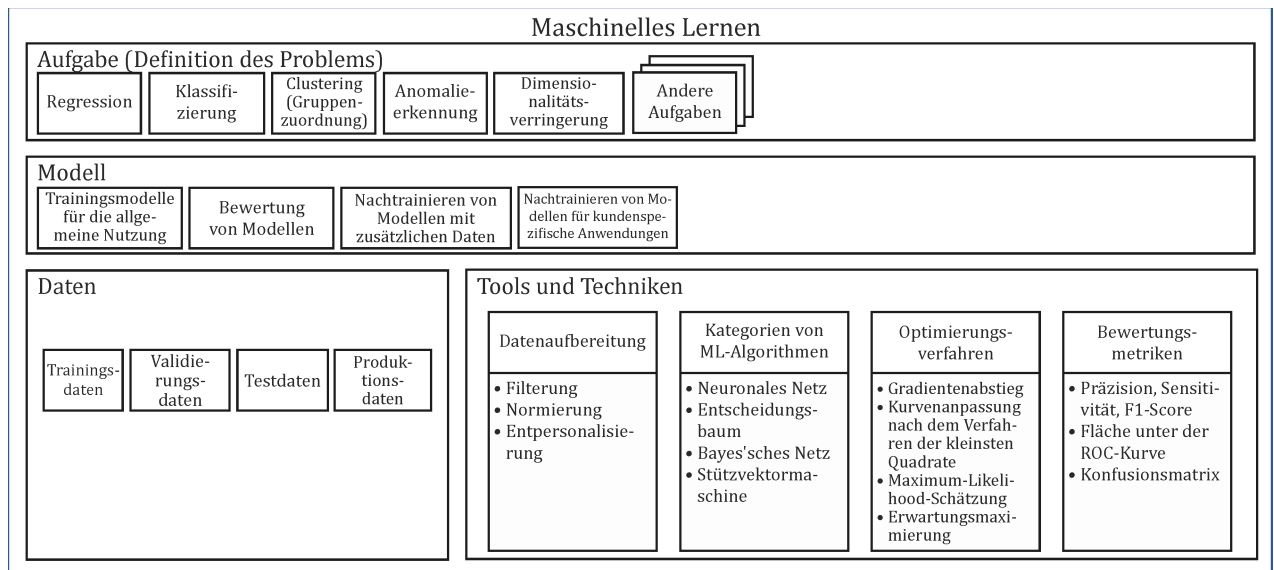


Bild 1 — Elemente eines ML-Systems

In Bild 1 können die Unterelemente der Modellentwicklung und -nutzung als ein mehrschichtiger Ansatz betrachtet werden, d.h. Anwendungen werden aus Modellen aufgebaut, die zur Lösung von Aufgaben verwendet werden. Die Entwicklung und Verwendung von Modellen hängt wiederum von Software-Tools und -Techniken sowie von Daten ab.

Ein einzelnes ML-System kann aus mehreren ML-Modellen bestehen, die in Kombination verwendet werden. Die Systemkomponenten können anhand ihrer Eingaben, ihrer Ausgaben und ihrer Absicht oder Funktion beschrieben werden. Die Komponenten können unabhängig voneinander geprüft werden.

ML-Modelle erzeugen bei ihrem Einsatz Ergebnisse wie Vorhersagen oder Entscheidungen. Ein vortrainiertes Modell ist ein ML-Modell, das bereits trainiert wurde, als es erhalten wurde. In einigen Fällen kann das entwickelte Modell auf eine ähnliche Aufgabe in einer anderen Domäne angewendet werden. Transfer-Learning ist eine Technik zur Modifizierung eines vortrainierten ML-Modells, um eine andere verwandte Aufgabe zu erfüllen.

In diesem Dokument bezieht sich der Begriff Anwendung sowohl auf die beabsichtigte Verwendung eines oder mehrerer ML-Modelle als auch auf die konkrete Software, die diese Verwendung implementiert. ML-Modelle werden üblicherweise mit anderen Softwarekomponenten integriert, um Anwendungen zu erstellen. Anwendungen, die ML verwenden, unterscheiden sich durch die Art der Eingabedaten, die sie verarbeiten, und durch die Art der Aufgaben, die sie ausführen. In einigen Anwendungen trifft ML Vorhersagen oder Entscheidungen auf hoher Ebene, während ML in anderen Anwendungen Antworten auf eng definierte Probleme liefert.

Unterschiede bei den Eingabedaten und Aufgaben sowie Faktoren wie Einsatzmöglichkeiten, Genauigkeit und Zuverlässigkeit führen zu unterschiedlichen Anwendungsgestaltungen. KI-Anwendungen können proprietäre benutzerdefinierte Gestaltungen verwenden oder domänenspezifischen Gestaltungsmustern folgen.

Die Anwendungslogik wird durch das Format der Eingabedaten, die Ausgabedaten und möglicherweise die Transformation und den Datenfluss zwischen den verwendeten ML-Modellen bestimmt. In allen Fällen wird die Wahl der ML-Algorithmen und Datenaufbereitungstechniken auf die Aufgaben der Anwendung zugeschnitten.

6.2 Aufgabe

6.2.1 Allgemeines

Der Begriff „Aufgabe“ bezieht sich auf Aktionen, die zur Erreichung eines bestimmten Ziels erforderlich sind. Bei ML bedeutet dies, dass ein Problem ermittelt wird, das mit Hilfe des ML-Modells gelöst werden soll. Für