

Maschinelles Lernen für intelligente Automatisierungssysteme mit dezentraler Datenhaltung am Anwendungsfall Predictive Maintenance

Machine learning for intelligent automation systems with decentralized data storage for a predictive maintenance use case

B. Maschler, M.Sc.; Dr.-Ing. **N. Jazdi**; Prof. Dr.-Ing. Dr. h.c. **M. Weyrich**, Institut für Automatisierungstechnik und Softwaresysteme (IAS) der Universität Stuttgart, Stuttgart;

Kurzfassung

Für eine hohe Ergebnisqualität sind Machine Learning Algorithmen auf eine breite Datenbasis angewiesen. Studien zeigen jedoch, dass viele Unternehmen nicht bereit sind, ihre Daten mit anderen Unternehmen, beispielsweise in Form einer gemeinsamen Daten-Cloud, zu teilen. Ziel sollte es daher sein, effizientes maschinelles Lernen mit einer dezentralen Datenhaltung, die den Verbleib vertraulicher Daten im jeweiligen Ursprungs-Unternehmen ermöglicht, zu ermöglichen. In diesem Artikel wird diesbezüglich ein neuartiges Konzept vorgestellt und hinsichtlich seiner Potentiale für intelligente Automatisierungssysteme am Beispiel des Anwendungsfalls Predictive Maintenance analysiert. Die Umsetzbarkeit des Konzepts unter Nutzung verschiedener bestehender Ansätze wird diskutiert, bevor schließlich auf potentielle Mehrwerte für Anlagenbetreiber sowie -hersteller unter besonderer Berücksichtigung der Perspektive kleiner und mittlerer Unternehmen eingegangen wird.

Abstract

Machine learning algorithms rely on a broad database for high quality results. However, studies show that many companies are not willing to share their data with other companies, for example in the form of a shared data cloud. Therefore, the goal should be to make efficient machine learning possible with decentralized data storage that allows confidential data to remain in the respective company of origin. This article presents a new concept in this respect and analyses its potential for intelligent automation systems taking predictive maintenance as an example. The feasibility of the concept using various existing approaches will be discussed, before potential benefits for plant operators and manufacturers, with particular consideration of the perspective of small and medium-sized companies, will be discussed.

1. Maschinelles Lernen als Werkzeug in der Automatisierungstechnik

Maschinelles Lernen ist ein aktueller Trend in der Automatisierungstechnik und darüber hinaus [1], [2], [3], [4]. Es kann in unterschiedlichen Phasen des Lebenszyklus für unterschiedliche Zwecke eingesetzt werden, bspw. für Fehleranalyse und Ausfallvorhersage [5], Ressourcenverbrauchsoptimierung [6], Testfallgenerierung und -priorisierung [7].

Ein wesentlicher Vorteil von auf maschinellem Lernen basierenden Ansätzen ist dabei die Möglichkeit zur Berücksichtigung von zur Entwurfszeit unbekanntem Einflüssen und Zusammenhängen bei den verschiedenen Anwendungen automatisierter Systeme wie z. B. Steuerung, Diagnose und Qualitätssicherung. Dieser wirkt sich insbesondere in solchen Anwendungsfällen aus, bei denen Daten Dritter, deren Verhalten von den Entwicklern nicht zu beeinflussen ist, erhoben werden.

Beispielhaft für einen solchen Anwendungsfall soll im Folgenden Predictive Maintenance für in Massenprodukten, wie bspw. Elektromotoren, betrachtet werden. Diese werden entsprechend konkreter Anforderungsprofile entwickelt und getestet, später jedoch vielfach auch in davon abweichenden Anordnungen durch Dritte betrieben. Eine präzise Ausfallvorhersage ist damit vor allem dann sinnvoll möglich, wenn auch zuvor unbekannte Einflüsse automatisch durch maschinelles Lernen in den Vorhersagealgorithmus integriert werden.

Für eine hohe Ergebnisqualität sind Algorithmen für maschinelles Lernen auf eine breite Datenbasis angewiesen [2], [4]. Im Anwendungsfall Predictive Maintenance bedeutet dies, dass möglichst hinreichend genau aufgelöste Daten über die überwachten Komponenten und ihre Umgebungen (d.h. die Anlagen, Prozesse, Gebäude usw.) im Besitz unterschiedlicher Unternehmen genutzt werden müssen, um Algorithmen mit einer hohen Ergebnisqualität zu trainieren. Dieser speicher- und rechenleistungsintensive Prozess findet üblicherweise auf einem zentralen Server statt, womit sie außerhalb der unmittelbaren Kontrolle der einzelnen Nutzer liegen. Man spricht dann von einem Cloud-basierten Ansatz.

2. Begrenzte Akzeptanz Cloud-basierter Ansätze für maschinelles Lernen im industriellen Umfeld

In diesem Kapitel werden die Probleme, die Cloud-basierte Ansätze des maschinellen Lernens in Bezug auf die Akzeptanz dieser Ansätze in der industriellen Praxis hervorrufen, herausgearbeitet. Dies geschieht auf Basis grundsätzlicher Betrachtungen der dafür nötigen Prozesse sowie empirischer Befunde.

Cloud-basierte Ansätze erfordern ein hohes Maß an Vertrauen der Nutzer in den jeweiligen Anbieter, denn den Daten wohnt ein erhebliches Missbrauchspotential inne: Studien zeigen, dass selbst vermeintlich anonymisierte, strukturierte Daten unterschiedlichen Typs über den Vergleich mit bereits öffentlich verfügbaren Daten einfach de-anonymisiert werden können [8], [9], [10]. Im Fall umfassender, de-anonymer Industriedatensätze ergeben sich dann vielfältige weitere Analysemöglichkeiten, die bspw. detaillierten Aufschluss über Auslastungen, Prozess oder auch Probleme einzelner Unternehmen liefern können [11], [12]. Ein unautorisierter Zugriff auf die erhobenen Daten kann somit erheblichen Schaden verursachen. Die Forschungsagenda Industrie 4.0 formuliert daher die Herausforderung, dass „[d]ie Wertschöpfungspartner [...] sich darauf verlassen können [müssen], durch die Bereitstellung ‚ihrer‘ Daten keine materiellen oder immateriellen Nachteile zu erleiden“ [13].

Studien zur Verbreitung von Predictive Maintenance Lösungen [14] zeigen nun, dass viele Unternehmen bisher nicht bereit sind, ihre Daten mit anderen Unternehmen, beispielsweise in Form einer gemeinsamen Daten-Cloud, zu teilen, obwohl sie vielfach die Vorteile der Technologie sehen und die dazu nötigen Daten bereits erfassen und auswerten (siehe **Bild 1**).

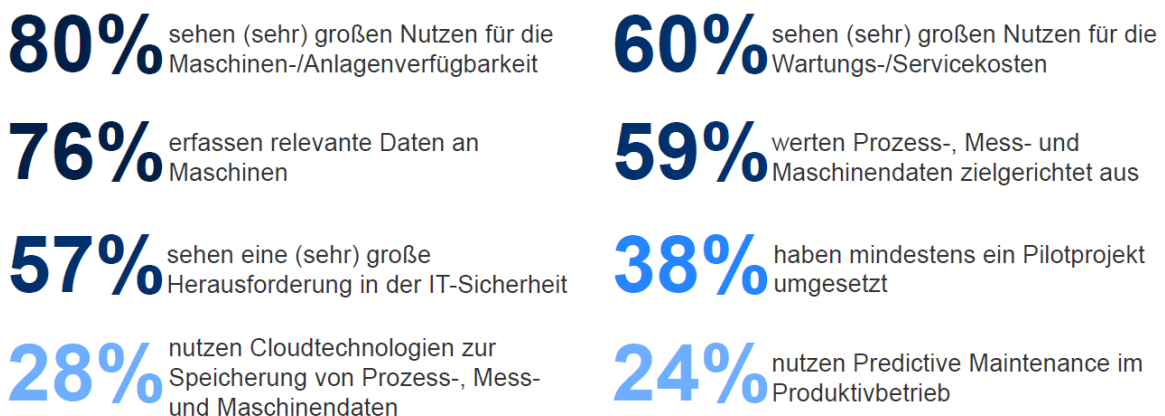


Bild 1: Ergebnisse einer Befragung zur Verbreitung von Predictive Maintenance Lösungen in der Industrie [14]

Es liegt also nahe, dass es die befürchteten Nachteile der Technologie sind, die einer breiteren Nutzung bisher im Wege stehen.

3. Maschinelles Lernen für intelligente Automatisierungssysteme mit dezentraler Datenhaltung am Anwendungsfall Predictive Maintenance

In diesem Kapitel wird ein Konzept vorgestellt, dass mittels nicht-Cloud-basierter Ansätze maschinellen Lernens eine Lösung des in Kapitel 2 herausgearbeiteten Akzeptanzproblems ermöglichen kann.

Ziel soll es dabei sein, effizientes maschinelles Lernen für Automatisierungssysteme mit einer dezentralen Datenhaltung, die den Verbleib vertraulicher Daten im jeweiligen Ursprungs-Unternehmen ermöglicht, zu vereinbaren. Dabei kann die Lösung nach derzeitigem Wissensstand nicht eine Reduzierung der letztendlich für den Lernprozess genutzten Datenbasis sein, da dies die Ergebnisqualität erheblich verschlechtern würde.

Im Sinne der Forderung der Plattform Industrie 4.0 nach „[n]eue[n] Techniken und Verfahren, die einerseits die intensive Datenanalyse bzw. -nutzung erlauben und dabei andererseits die digitale Souveränität wahren“ [13] ist stattdessen eine Lösung vorzuziehen, die ein verteiltes Lernen auf der gesamten Datenbasis ermöglicht. Dafür müssen die bisher in der Cloud erbrachten Leistungen zukünftig in den vernetzten Automatisierungssystemen selbst ausgeführt werden (siehe **Bild 2**).

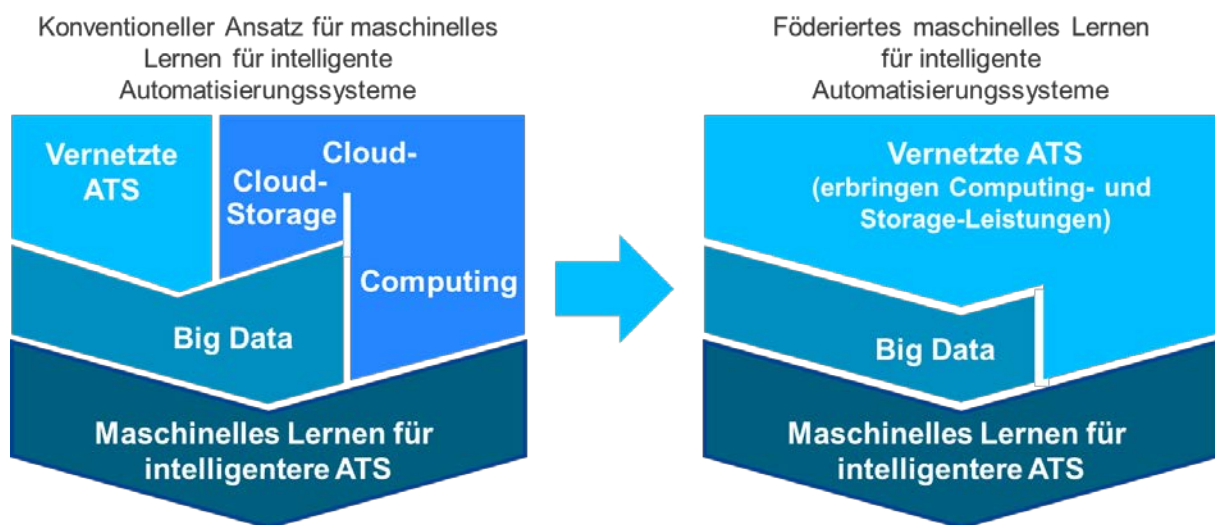


Bild 2: Schematische Darstellung der wesentlichen Bestandteile maschinell lernender Automatisierungssysteme (ATS) im Fall eines konventionellen, d.h. Cloud-basierten, (links) und eines föderierten (rechts) Ansatzes

Möglich ist dies mittels lokalen Lernens und einer auf einem Austausch der Lernergebnisse beruhenden iterativen Optimierung derselben.

Am Beispiel des Anwendungsfalls Predictive Maintenance ergibt sich für ein solches System folgender Ablauf:

Eine in verschiedenen Nutzungskontexten eingesetzte Anlage oder ein entsprechendes Anlagenteil (fortan „Komponente“) soll überwacht und ihr bzw. sein Verschleiß vorhergesagt werden, um den optimalen Austauschzeitpunkt zu bestimmen. Die zu überwachende Komponente ist in verschiedenen Unternehmen im Einsatz. Durch die unterschiedlichen Nutzungskontexte in unterschiedlichen Unternehmen ist eine Berücksichtigung von zur Entwurfszeit nicht bekannten Einflüssen durch eine datenbasierte Analyse zur Verbesserung der sonst eher groben Vorhersage wünschenswert.

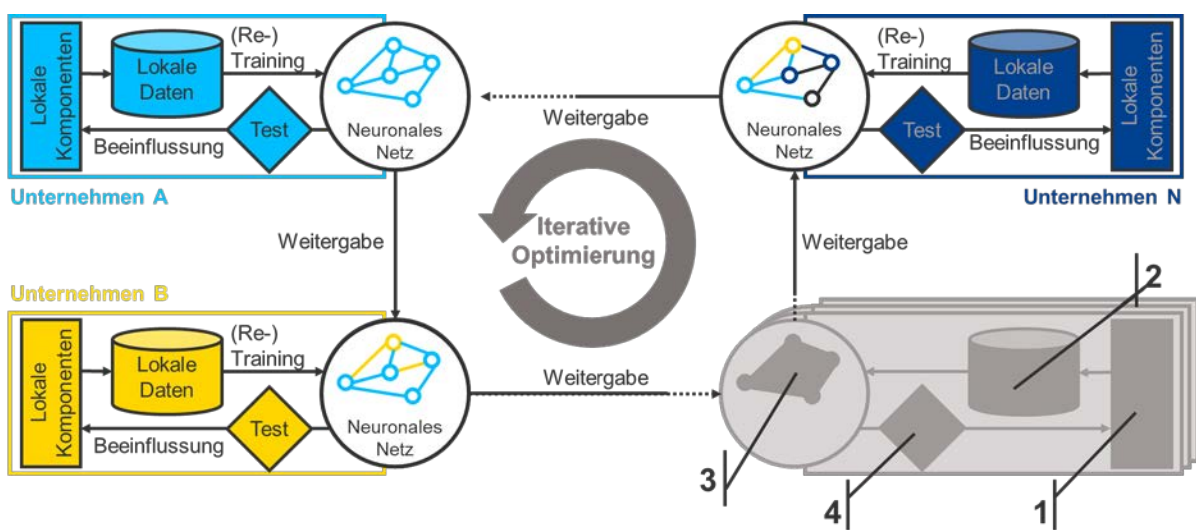


Bild 3: Konzeptskizze „Föderiertes maschinelles Lernen mit dezentraler Datenhaltung am Anwendungsfall Predictive Maintenance“ (1: Komponenten gleichen Typs; 2: Lokale Datenbank, deren Datenbestand die Komponente und ihre Umwelt beschreibt; 3: Neuronales Netz, das das Komponentenverhalten vorhersagt (bspw. den Verschleiß); 4: Test, der die Vorhersagegüte des neuronalen Netzes ermittelt)

In jedem Unternehmen werden die Komponente sowie ihre Umgebung mittels Sensoren überwacht. Die dabei entstehenden Daten werden beispielsweise über Rückschlüsse aus dem Systemverhalten oder über Nutzereingaben gelabelt und lokal gespeichert (siehe **Bild 3**).

Auf Basis dieser lokalen Datensätze werden lokal neuronale Netze trainiert (siehe **Bild 3**, Vorgänge in „Unternehmen A“). Ist die Ergebnisqualität (d.h. die Genauigkeit der Verschleißvorhersage ermittelt mit historischen Daten) gut genug, wird das neuronale Netz fortan zur Beeinflussung der lokalen Komponente (d.h. zur Bestimmung des Austauschzeitpunkts) genutzt. In regelmäßigen Abständen werden lokal trainierte neuronale Netze an andere Teilnehmer weitergegeben (siehe **Bild 3**, Vorgänge in „Unternehmen B“). Dort werden die neuronalen

Netze auf Basis der lokalen Datensätze weitertrainiert. Ist die Ergebnisqualität des neuen neuronalen Netzes besser als die des vorherigen neuronalen Netzes, so wird letzteres verworfen (relative Evaluation). Ist die Ergebnisqualität gut genug, wird das neue neuronale Netz fortan zur Beeinflussung der lokalen Komponente genutzt (absolute Evaluation).

Über die Zeit werden so vielversprechende neuronale Netze auf immer neuen, lokalen Daten weitertrainiert und gleichzeitig evaluiert. Es findet somit eine iterative Optimierung statt, die nach und nach die Nachteile des durch die Beschränktheit der lokalen Datensätze ebenfalls in seiner Ergebnisqualität beschränkten lokalen Lernens aufhebt. Konkret lernt also ein häufig genug weitergegebenes neuronales Netz die Vorhersage des Austauschzeitpunkts einer Komponente basierend nicht nur auf den Begebenheiten an einem Standort, sondern auf denen vieler Standorte – ähnlich einer Cloud-basierten Lösung.

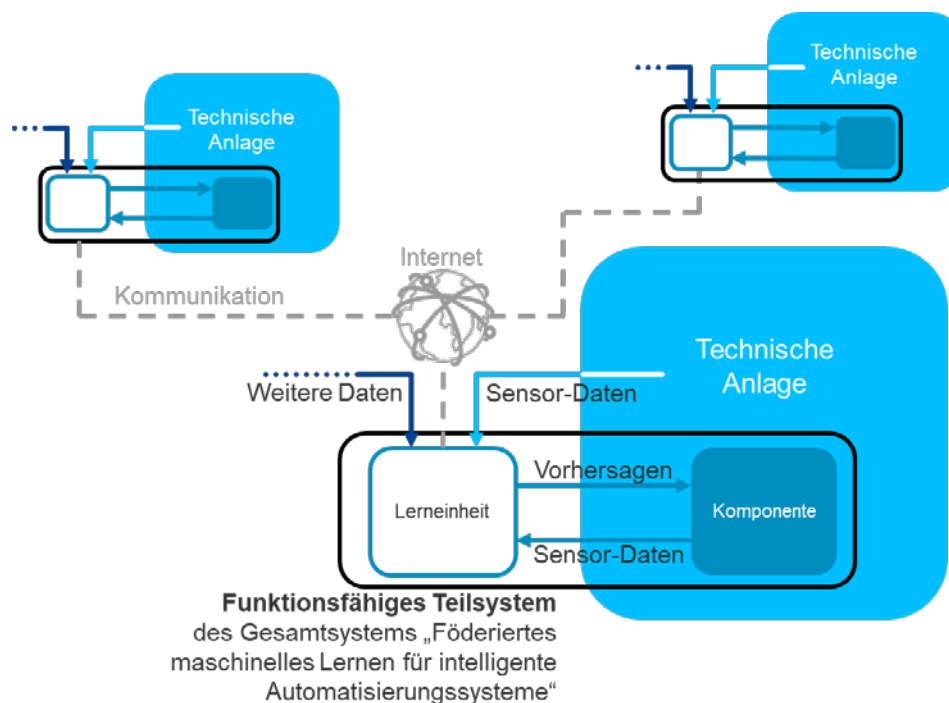


Bild 4: Systemstruktur „Föderiertes maschinelles Lernen für intelligente Automatisierungssysteme mit dezentraler Datenhaltung am Anwendungsfall Predictive Maintenance“

Ein System zur Realisierung dieses Konzeptes kann entsprechend **Bild 4** folgendermaßen aufgebaut sein:

Eine oder mehrere zu überwachende Komponenten haben eine Lerneinheit zugeordnet. Die Lerneinheit pflegt den lokalen Datensatz mittels Schnittstellen zu Sensoren in der Komponente, in der die Komponente umgebenden technischen Anlage sowie zu weiteren Datenquellen. Auch das Training und der Test von neuronalen Netzen finden in der Lerneinheit statt. Die

Lerneinheit kann auf dieser Grundlage eine Vorhersage des Austauschzeitpunkts der Komponente(n) erstellen.

Eine Lerneinheit und ihre Komponente(n) bilden ein prinzipiell funktionsfähiges Teilsystem des Gesamtsystems. Das Gesamtsystem besteht aus mehreren dieser Teilsysteme, die über das Internet miteinander verbunden sind. Sie tauschen die vortrainierten neuronalen Netze untereinander aus und ermöglichen so das Lernen auf den lokalen Datensätzen verschiedener Teilsysteme, d.h. die iterative Optimierung.

Die Hauptherausforderung bei der Implementierung dieses Konzepts liegt in der Entwicklung eines Algorithmus, der auch auf den kleinen Datenmengen der lokalen Datensätze ein sinnvolles Training neuronaler Netze erlaubt und gleichzeitig das Weiter-Trainieren bereits vortrainierter neuronaler Netze auf anderen lokalen Datensätzen ohne „Überschreiben“ des bisher Gelernten ermöglicht.

4. Vielversprechende Methoden für föderiertes maschinelles Lernen für intelligente Automatisierungssysteme

In diesem Kapitel werden konkrete Implementierungsansätze vorgestellt, die eine Umsetzung des in Kapitel 3 vorgestellten Konzepts eines nicht-Cloud-basierten maschinellen Lernens ermöglichen könnten.

Eine Gruppe von Algorithmen, die maschinelles Lernen für intelligente Automatisierungssysteme mit dezentraler Datenhaltung für die Automatisierungstechnik ermöglichen können, wird derzeit unter dem Begriff des „Continual Learning“ erforscht. Continual Learning zielt dabei auf die Schaffung Multi-Tasking-fähiger Algorithmen, die zum Erlernen neuer Tasks keinen erneuten Zugriff auf die Daten bereits erlernter Tasks benötigen. Diese Anforderung lässt sich gut auf die Herausforderung maschinellen Lernens bei dezentraler Datenhaltung für die Automatisierungstechnik übertragen: Anstatt verschiedener Probleme soll lediglich ein einzelnes Problem gelöst werden, wobei jeweils nur Teile des Gesamtdatensatzes zur Verfügung stehen. Continual Learning Ansätze gliedern sich in drei Gruppen:

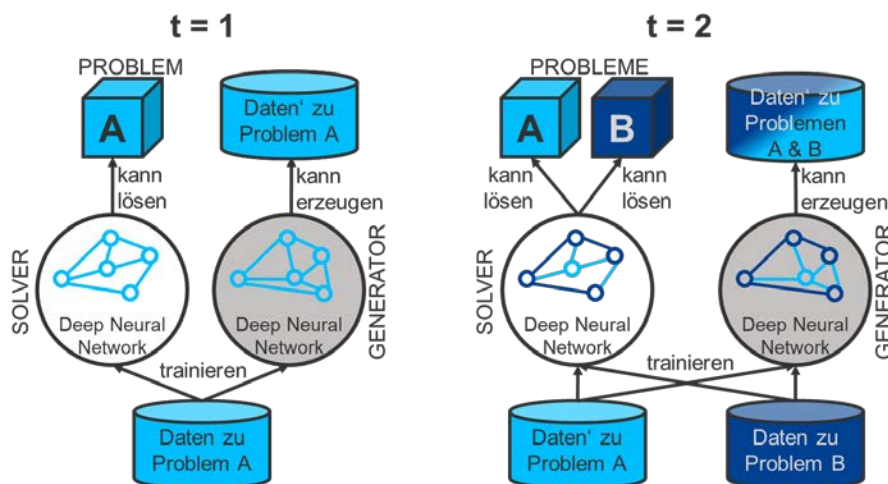


Bild 5: Funktionsweise des Generative Replay (Generierte Pseudo-Daten sind mit einem ' gekennzeichnet.)

- Generative Replay:** In dieser Gruppe wird das Fehlen des Zugriffs auf Daten vergangener, bereits erlernter Tasks als zentrale Herausforderung interpretiert. Die Lösung erfolgt daher über das parallele Training eines Pseudo-Datengenerators, der beim Erlernen neuer Tasks eigens generierte Pseudo-Daten vergangener Tasks in den jeweils aktuellen Datensatz einmischt, und eines Problem-Solvers, der das konkrete Problem löst [15] (siehe **Bild 5**). So stehen immer repräsentative Daten für alle Tasks zur Verfügung, ohne die Daten für bereits erlernte Tasks explizit speichern zu müssen. Nachteilig ist dabei, dass zwei Netze trainiert und optimiert werden müssen und dass eine zu gute Generator-Leistung die gewünschte Vertraulichkeit der Originaldaten gefährden könnte.

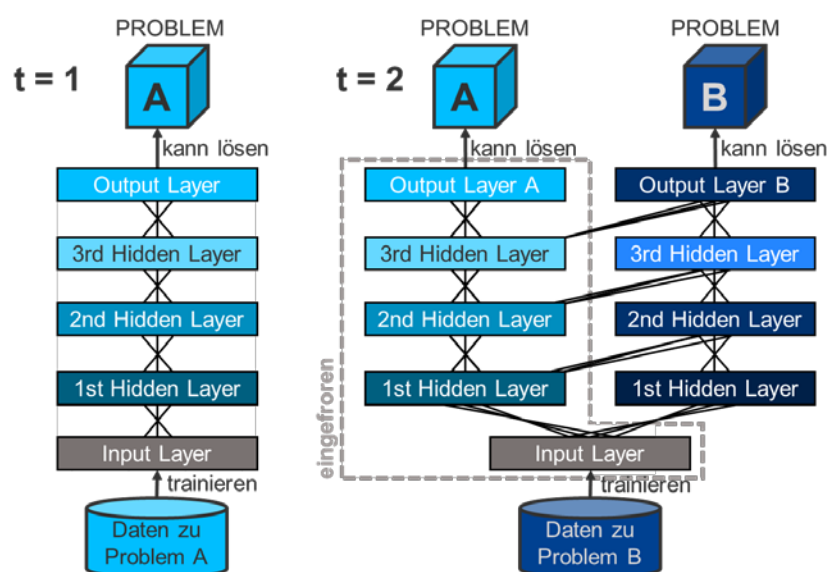


Bild 6: Funktionsweise von Progressive Networks

- **Progressive Networks:** In dieser Gruppe wird das Überschreiben bereits erlernter Zusammenhänge als zentrale Herausforderung interpretiert. Die Lösung erfolgt daher über die Erweiterung des Netzes um eine weitere „Säule“ (entspricht dem Basis-Netz des ersten Problems) pro Problem mit jeweils vorwärts gerichteten Querverbindungen zwischen den einzelnen Säulen, wobei nur die jeweils aktuelle Säule durch Training verändert werden kann [16] (siehe **Bild 6**). So bleibt gewährleistet, dass einmal gelernte Zusammenhänge nicht überschrieben werden können. Nachteilig ist dabei, dass das Netz mit jeder neuen Aufgabe(-variante) weiterwächst, wobei hier regelmäßige Pfadanalysen in Verbindung mit einer Bereinigung wenig relevanter Pfade Abhilfe schaffen kann.
- **Weight Consolidation:** Auch in dieser Gruppe wird das Überschreiben bereits erlernter Zusammenhänge als zentrale Herausforderung interpretiert. Die Lösung erfolgt jedoch anders als bei Progressive Networks über die Anpassung der Lernrate abhängig von der Relevanz eines Kantengewichts für bereits erlernte Probleme. Umso wichtiger also ein gewisser Pfad für bekannte Probleme ist, umso schwieriger lässt er sich zur Bewältigung neuer Probleme verändern [17], [18]. So bleibt gewährleistet, dass einmal gelernte Zusammenhänge nicht überschrieben werden können.

Ein anderer Ansatz ist das kommunikationseffiziente föderierte Lernen aus dem Bereich der Smartphone-Apps. Der Fokus liegt hier bereits auf maschinellem Lernen bei dezentraler Datenhaltung, jedoch wird weiterhin eine Cloud als zentraler Server eingesetzt. Ein Anwendungsfall ist hier beispielsweise das lokale und damit Daten schützende Lernen von Autovervollständigungen während der Texteingabe, dessen Datenbasis auf dem Endgerät des Nutzers verbleibt und mit dessen trainierten lokalen Netz lediglich ein Update des zentralen Netzes in der Cloud vorgenommen wird [19]. Der Server dient in diesem Szenario der Steuerung des Lernvorgangs und der Entlastung der einzelnen Endgeräte. Prinzipiell ist jedoch auch eine Übertragung des Ansatzes auf die Herausforderung maschinellen Lernens bei dezentraler Datenhaltung für die Automatisierungstechnik unter Verzicht auf einen zentralen Server denkbar.

Es existieren also bereits verschiedene Ansätze, die für sich oder in Kombination erhebliche Potentiale für einen Transfer auf die Herausforderung maschinelles Lernen mit dezentraler Datenhaltung aufweisen. Weitere Untersuchungen werden klären müssen, welche Anordnungen sich in der Domäne Automatisierungstechnik optimal einsetzen lassen.

5. Konzeptionelle Bewertung

In diesem Kapitel werden die Vorteile und Nachteile des Konzepts föderierten maschinellen Lernens in intelligenten Automatisierungssystemen am Beispiel des Anwendungsfalls Predictive Maintenance dargestellt.

Wie bereits in Kapitel 1 motiviert, bietet der Einsatz von maschinellem Lernen für intelligente Automatisierungssysteme unabhängig von der Frage der Cloud-Nutzung Vorteile hinsichtlich der automatischen Berücksichtigung von zur Entwurfszeit unbekanntem Zusammenhängen. Ein weiterer Aspekt ist dabei insbesondere aus der Perspektive kleiner und mittelgroßer (Zulieferer-) Unternehmen vorteilhaft:

- **Geringerer Bedarf an Wissen über das Gesamtsystem:** Durch den datenbasierten Ansatz ist eine Überwachung zugelieferter Anlagenkomponenten auch ohne Kenntnis des Gesamtsystems möglich – entsprechende Datenbasis vorausgesetzt. Dies erlaubt zudem, derartige Funktionen mit geringem Aufwand nachzurüsten, da weder Änderungen an der Funktionsweise der aufnehmenden Anlage noch an der des Überwachungssystems erforderlich sind. Insbesondere können vielfach bereits in der Anlage und ihrer Umgebung bestehende Sensorsysteme integriert werden.

Das in Kapitel 3 vorgestellte Konzept föderierten maschinellen Lernens für intelligente Automatisierungssysteme bietet jedoch verglichen mit einer konventionellen, Cloud-basierte Implementierung weitere Vorteile, die den Ansatz insbesondere für kleine und mittlere Unternehmen attraktiv machen:

- **Geringerer Vertrauensvorschuss:** Durch die dezentrale Datenhaltung und stark standardisierte Kommunikation vergrößert sich die Zahl der Angriffsvektoren durch einen Einsatz des Systems kaum. Insbesondere ist die Zahl neuer Angriffsvektoren außerhalb des Einflussbereichs des Kunden/Nutzers (bspw. in Form von Cloud-Hardware/Software) gering (siehe auch [19]).
- **Geringerer Unterhaltsaufwand:** Durch seine Abgeschlossenheit und die Peer-to-Peer-Struktur ist das System auf wenig bis keinen externen Unterhalt angewiesen. Es werden insbesondere keine externen (d.h. bei Dritten gehostete) Speicher- oder Rechenressourcen benötigt, deren langfristige Bereitstellung erhebliche Kosten verursachen kann.

Diesen Vorteilen gegenüber steht eine gegenüber Cloud-basierten Ansätzen potentiell reduzierte Vorhersagegenauigkeit, da dem zu trainierenden neuronalen Netz in der Cloud immer

alle Daten zur Verfügung stehen, wohingegen die einzelnen Einheiten des föderierten Systems jeweils nur Ausschnitte der Gesamtdaten zu Verfügung haben. Der Einsatz föderierten maschinellen Lernens für intelligente Automatisierungssysteme wird sich also auf diejenigen Anwendungsfälle konzentrieren, in denen die Vorhersagegenauigkeit auch auf lokalen Daten bereits vergleichsweise hoch ist und die besondere Anforderungen hinsichtlich des Schutzes dieser lokalen Daten erheben.

6. Zusammenfassung und Ausblick

In diesem Artikel wurde gezeigt, dass Cloud-basiertes maschinelles Lernen für intelligente Automatisierungssysteme ein Akzeptanzproblem hat. Am Beispiel des Anwendungsfalls Predictive Maintenance wurde daraufhin ein Konzept für ein föderiertes maschinelles Lernen für intelligente Automatisierungssysteme mit dezentraler Datenhaltung entwickelt. Es wurde gezeigt, dass bereits verschiedene Ansätze zur Realisierung des Konzepts vorliegen und dass der Einsatz eines solchen Systems erhebliche Vorteile – insbesondere für kleine und mittelgroße Unternehmen – bieten würde, weil sich der Vertrauensvorschuss von Nutzerseite und der Unterhaltsaufwand von Anbieterseite reduzieren würden.

Die nächsten Schritte zur Umsetzung föderierten maschinellen Lernens für intelligente Automatisierungssysteme mit dezentraler Datenhaltung sind die Auswahl eines geeigneten Ansatzes, die Implementierung eines dazu passenden zielgerichteten, iterativen Optimierungsprozesses sowie von Sicherheitsfunktionalitäten zur Manipulationsvorbeugung. In einem weiteren Schritt ist die Implementierung von Clustering-Verfahren zur Anpassung des Vorhersage-Algorithmus an unterschiedliche Anlagen-Gruppen zu untersuchen.

7. Literaturverzeichnis

- [1] M. Sharp, R. Ak, and T. Hedberg, "A survey of the advancing use and development of machine learning in smart manufacturing," *Journal of Manufacturing Systems*, 2018.
- [2] J. Wang, Y. Ma, L. Zhang, R. X. Gao, and D. Wu, "Deep learning for smart manufacturing: Methods and applications," *Journal of Manufacturing Systems*, vol. 48, pp. 144–156, 2018.
- [3] S. Fosso Wamba, S. Akter, A. Edwards, G. Chopin, and D. Gnanzou, "How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study," *International Journal of Production Economics*, vol. 165, pp. 234–246, 2015.
- [4] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," (eng), *Science (New York, N. Y.)*, vol. 349, no. 6245, pp. 255–260, 2015.
- [5] Y. L. Murphey, M. A. Masrur, Z. Chen, and B. Zhang, "Model-based fault diagnosis in electric drives using machine learning," *IEEE/ASME Trans. Mechatron.*, vol. 11, no. 3, pp. 290–303, 2006.

- [6] D. Zhang, S. Li, M. Sun, and Z. O'Neill, "An Optimal and Learning-Based Demand Response and Home Energy Management System," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1790–1801, 2016.
- [7] R. Lachmann, S. Schulze, M. Nieke, C. Seidl, and I. Schaefer, "System-Level Test Case Prioritization Using Machine Learning," in *2016 15th IEEE International Conference on Machine Learning and Applications: 18-20 December 2016, Anaheim, California : proceedings*, Anaheim, CA, USA, 2016, pp. 361–368.
- [8] S. Ji, W. Li, M. Srivatsa, and R. Beyah, "Structural Data De-anonymization," in *Proceedings of the 21st ACM Conference on Computer and Communications Security: November 3 - 7, 2014, Scottsdale, Arizona, USA*, Scottsdale, Arizona, USA, 2014, pp. 1040–1053.
- [9] S. Ji, P. Mittal, and R. Beyah, "Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 1305–1326, 2017.
- [10] B. K. Tripathy, "De-Anonymization Techniques for Social Networks," in *Social network analytics: Computational research methods and techniques*, N. Dey, A. S. Ashour, R. Babo, and S. Borah, Eds., London: Academic Press an imprint of Elsevier, 2019, pp. 71–85.
- [11] M. M. Alani and M. Alloghani, "Security Challenges in the Industry 4.0 Era," in *INDUSTRY 4.0 AND ENGINEERING FOR A SUSTAINABLE FUTURE*, M. Dastbaz and P. Cochrane, Eds., [S.l.]: SPRINGER NATURE, 2019, pp. 117–136.
- [12] V. Prabhu, J. Oyekan, S. Eng, L. E. Woei, and A. Tiwari, "Towards Data-Driven Cyber Attack Damage and Vulnerability Estimation for Manufacturing Enterprises," in *Lecture Notes in Networks and Systems, Volume 47, Smart industry & smart education: Proceedings of the 15th International Conference on Remote Engineering and Virtual Instrumentation*, M. E. Auer and R. Langmann, Eds., Cham: Springer International Publishing, 2019, pp. 333–343.
- [13] R. Anderl *et al.*, "Forschungsagenda Industrie 4.0: Aktualisierung des Forschungsbedarfs," *Ergebnispapier, Plattform Industrie 4.0*, Berlin, Oct. 2016.
- [14] F. Duscheck, R. Blameuser, and S. Gehrman, "Maschinenverfügbarkeit rauf, Wartungs- und Servicekosten runter: Chancen und Herausforderungen von Predictive Maintenance in der Industrie," *BearingPoint*, 2017.
- [15] H. Shin, J. K. Lee, J. Kim, and J. Kim, "Continual Learning with Deep Generative Replay," in *Advances in Neural Information Processing Systems 30*, I. Guyon *et al.*, Eds.: Curran Associates, Inc, 2017, pp. 2990–2999.
- [16] A. A. Rusu *et al.*, "Progressive Neural Networks," Jun. 2016. [Online] Available: <http://arxiv.org/pdf/1606.04671v3>.
- [17] P. McClure *et al.*, "Distributed Weight Consolidation: A Brain Segmentation Case Study," May. 2018. [Online] Available: <http://arxiv.org/pdf/1805.10863v9>.

- [18] J. Kirkpatrick *et al.*, "Overcoming catastrophic forgetting in neural networks," (eng), *Proceedings of the National Academy of Sciences of the United States of America*, vol. 114, no. 13, pp. 3521–3526, 2017.
- [19] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," <http://arxiv.org/pdf/1602.05629v3>.