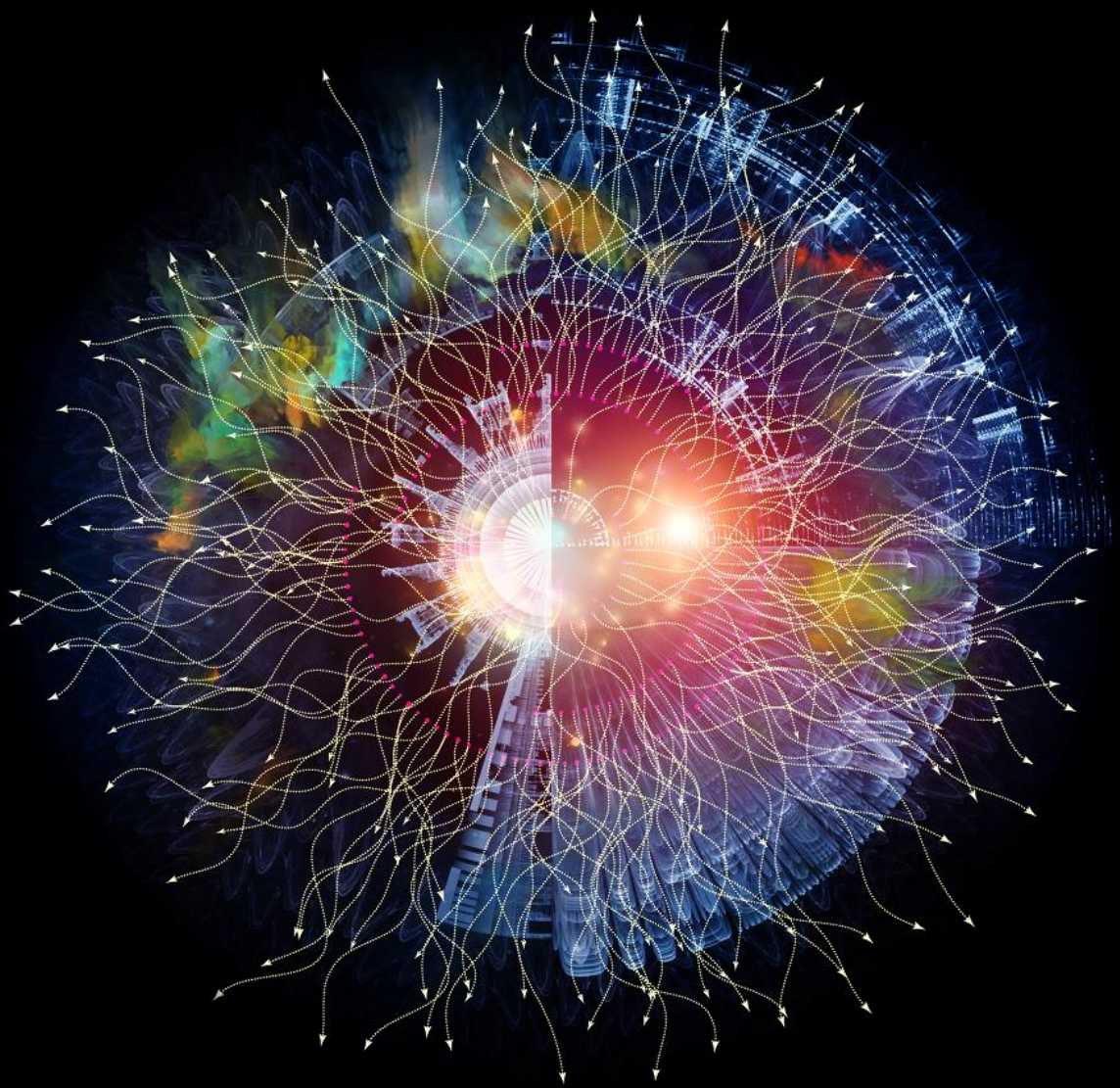
Deloitte.



Revolutionizing Product-Lifecycle-Management (PLM): A New Era of Artificial Intelligence

Securing PLM by Federated-Learning
A secure machine learning approach

March 2024

Contents

1. Preface

As organizations strive to develop their products digitally mutually, balancing the pursuit of knowledge with the imperative of safeguarding individual data has been a primary focus. Accordingly, significant technical, regulatory, and collective development complexities have become challenging for OEMs and suppliers. The emergence of Federated-Learning, a revolutionary paradigm in machine learning, offers a significant solution to this problem.

As products are Mutually developed...

In an era defined by the relentless surge of mutually managing a product's lifecycle digitally, sharing data securely and anonymously has become crucial for many OEMs and suppliers. Common Product-Lifecycle-Management (PLM) systems have encountered significant challenges concerning data privacy concerns. These systems often involve storing, sharing, and analyzing sensitive product-related information across various stages, from design to end-of-life. Additionally, Artificial-Intelligence (AI) in PLM has added another layer of complexity in correspondence to using data from multiple sources, mainly because digital products are expected to be based on platform or open source systems in >50% of cases by 2025 [4].

...sharing organizations' data has become More critical...

Handling PLM's data in a decentralized environment is a massive responsibility for the system owner, where PLM solutions frequently involve collaboration with external partners and suppliers. Therefore, managing data privacy compliance across different jurisdictions and regulatory frameworks becomes an intricate task. The inherent complexity of PLM processes makes it challenging to establish foolproof data access controls and ensure that only authorized personnel have the appropriate level of visibility. Data breaches or leaks could not only compromise proprietary product designs but also expose customer data, leading to reputational damage and legal liabilities.

...so OEMs & suppliers require to Secure their data

As a result, companies have started considering Federated-Learning (FL) to encounter such a challenge. FL, or collaborative learning, is a machine learning method that allows a group of decentralized edge devices or systems to train machine learning models without moving or storing the raw data in a central server. By adopting Federated-Learning techniques, organizations can enable collaborative model training without the need for centralizing sensitive product data. This decentralized approach allows different stakeholders to contribute their data and insights to the model-building process without actually sharing raw data.

OEM = Original-Equipment-Manufacturer | FL = Federated-Learning | AI = Artificial-Intelligence | PLM = Product-Lifecycle-Management

Trends

The average cost of a data breach in 2022 was $4.85 Million in Germany [1]

OEMs must collaborate and share available resources to evolve toward a more sustainable Manufacturing ecosystem [2]

AI will add $13 trillion to the global economy over the next decade [3]

Artificial Intelligence to develop nearly **15%** of all new applications by **2027 [4]**

Federated-Learning market is expected to reach $210 Million by 2028 [5]

"Federated-Learning is a game-changer for organizations looking to harness the power of AI while respecting user privacy"

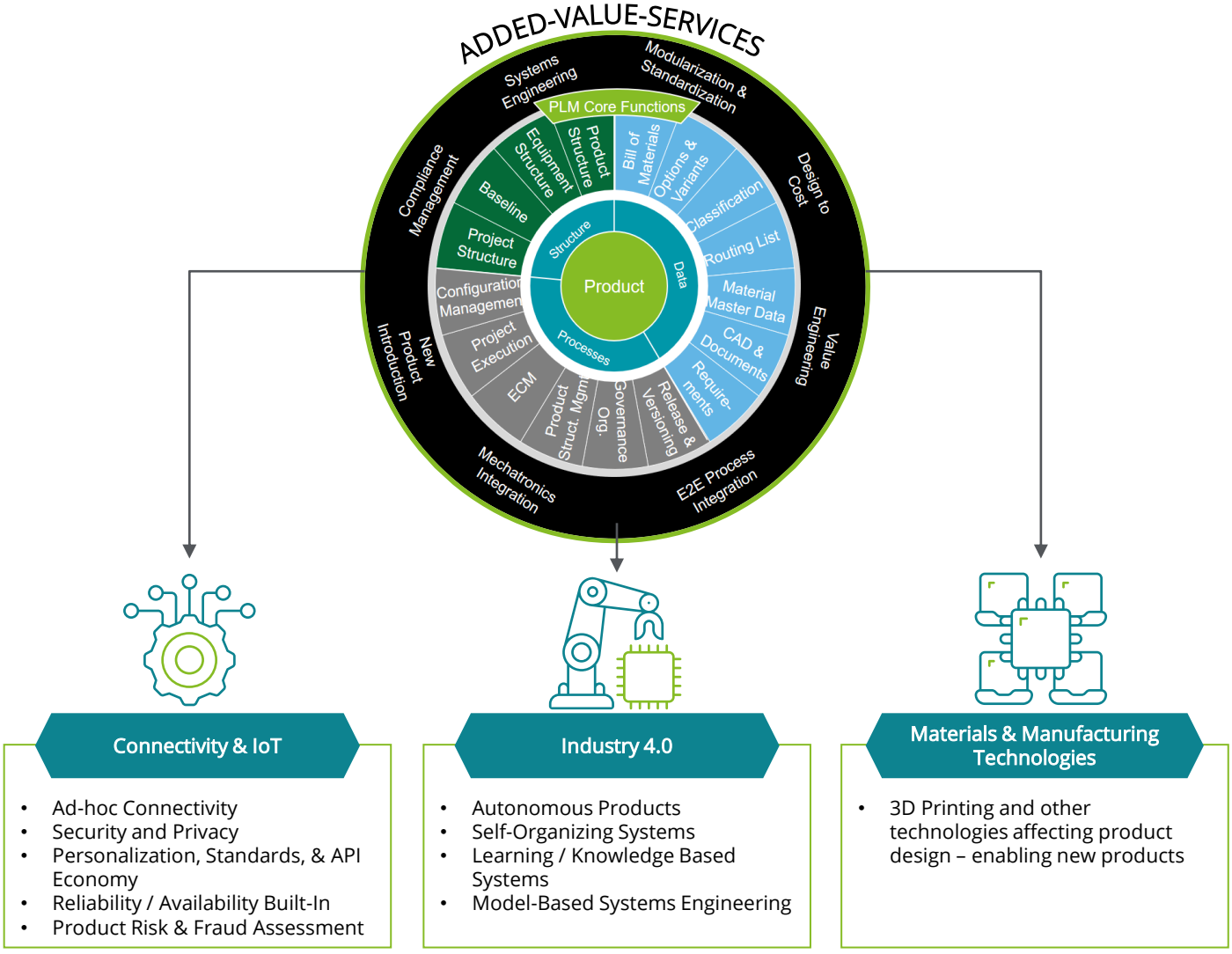
Sundar Pichai – CEO of Google

2. Understanding Product-Lifecycle-Management (PLM)

PLM is a holistic process encompassing the entire product development journey, from strategic decisions in product and portfolio management to the final stages of commercialization and operations. This framework operates within distinct architectural layers, such as requirements functional, logical, and physical models, which together define the product's evolution. These layers merge seamlessly with engineering and manufacturing bill of materials, manufacturing operations management, and service bill of materials, ultimately integrated with an IoT platform. This concise overview emphasizes PLM's role in guiding products from conception to operational excellence through intricate layers of architectural design and deployment.

2.1 Product-Lifecycle-Management at Deloitte

Although clients have the highest technological potential, they still have to approach new technologies and strategies to modernize processes, methods, and tools. Therefore, Deloitte offers integrated & comprehensive capabilities to elevate its clients to achieving their ultimate goals.



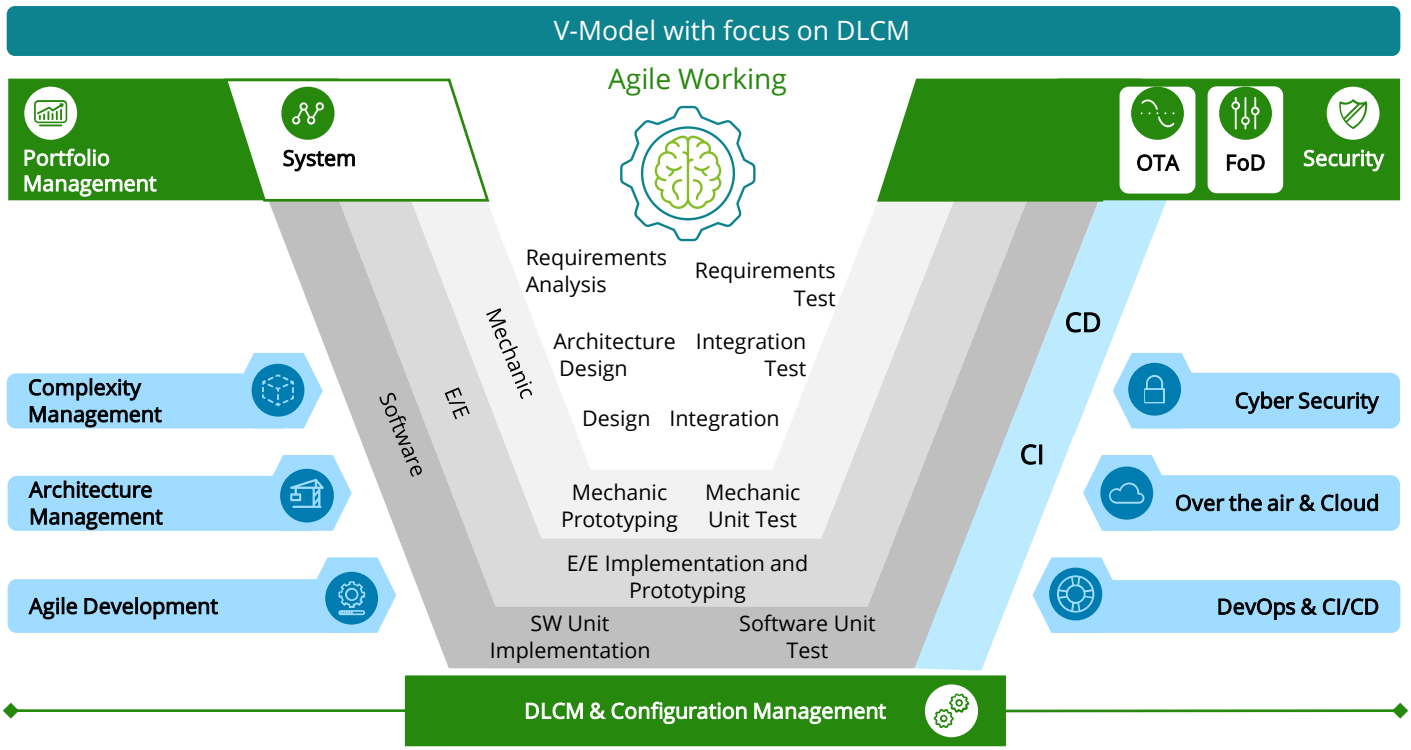
PLM intelligently connects processes, systems, and people along the product lifecycle

ECM = Engineering-Change-Management | Org. = Organization | API = Application-Programming-Interface | IoT = Internet-of-Things | CAD = Computer-Aided-Design | E2E = End-to-End | 3D = Three-Dimentional

2. Understanding Product-Lifecycle-Management (PLM)

2.2 Hardware to Software Revolution

The shift from hardware to software and the increasing functional complexity poses an enormous challenge for customer-oriented functionality and reliable compliance with legal and regulatory requirements. Deloitte's expertise in PLM is capable to guide you along the whole Digital-Lifecycle-Management (DCLM).



In the environment of new product development and product enhancement beyond the SOP (e.g., over-the-air updates), Systems Engineering is often positioned as the clear antipode to agility in the automotive industry, which is supposedly challenging to reconcile. However, the erroneous assumption that Systems Engineering only follows a purely phased waterfall approach is incorrect, where progress is measured and controlled against a set of specific, one-off milestones, with no continuous and iterative verification and validation.

Challenge: During joint software and hardware testing, particular challenges arise regarding complexity and coordination between the various organizational units.

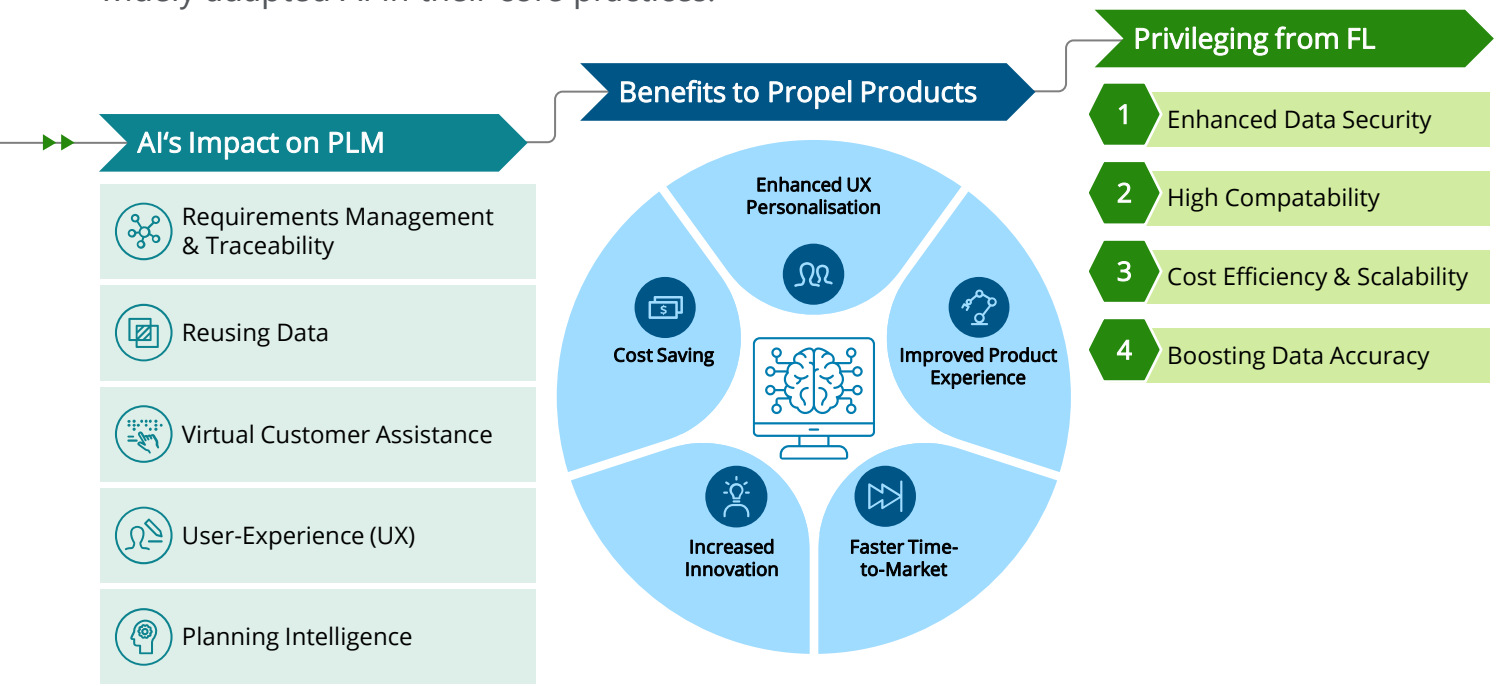
Solution: Simplifying the complexity of the overall system by breaking it down, where the system is demonstrating the portfolio and overall system requirements are met. Testing as early as possible and regularly at different test levels makes it possible to uncover errors and reduce costs and development times. Innovation and update cycles simplify coordination and communication.

Following the E2E Deloitte's approach enables efficient testing & quality assurance of the product lifecycle and overall systems, while considering portfolio management, requirements-based engineering, organizational communication & collaboration.

DLCM = Digital-Lifecycle-Management | E/E = Electrical/Electronic | CI/CD = Continuous-Integration-and-Continuous-Delivery/Continous-Deployment | FoD = Function-on-Demand | OTA = Over-The-Air | SOP = Standard-Operating-Procedure

3. Empowering Product-Lifecycle-Management (PLM) by AI: Encouraging Enterprises to Boost AI Adaptation

Even though enterprises advocate using AI in their PLM and data handling, only 8% have widely adapted AI in their core practices.



Gathering and analyzing the needs of products' end-users to create large sets of models for better PLM decision-making

Reducing duplicate efforts by analyzing the vast amount of data from multiple sources (e.g., Bill-of-Material)

Optimizing predefined patterns to improve PLM's aspects (e.g., Change Management)

Simplifying tools by various mechanisms (e.g., enabling speech recognition)

Simplifying tools by various mechanisms (e.g., enabling speech recognition)

Artificial intelligence (AI) transforms product development by increasing productivity, fostering better decision-making, and opening new possibilities. Businesses can streamline many phases of product development, from conception to design, testing, and validation, up to launching the product and its services projection. By utilizing AI technologies, companies can enhance their decision-making processes and process optimization, improve customer service cost savings, and speed up development processes. It is crucial to remember that.

Federated-Learning (FL) presents a collaborative approach to modern Product-Lifecycle-Management (PLM), treating individual IoT devices as distinct clients for model training while safeguarding data privacy. In this process, devices collect task-specific data, transmitting only model updates to a central server, thus ensuring security and operational integrity. FL's distribution of datasets across multiple locations and concurrent model training accelerates AI and IoT deployment, enhancing scalability. Its versatility allows knowledge transfer between domains, optimizing efficiency, reducing costs, and expediting processes. Unlike centralized data training, FL leverages decentralized data sources for enriched model generalization and bias reduction, making it a transformative solution for PLM and beyond.

Effective AI deployment in PLM necessitates careful consideration of ethical & privacy issues, as well as the requirements for human monitoring & intervention.

OEM = Original-Equipment-Manufacturer | FL = Federated-Learning | AI = Artificial-Intelligence | PLM = Product-Lifecycle-Management

4. Understanding Federated-Learning

Federated-Learning Overview

Federated-Learning (also known as collaborative learning) is a machine learning technique that enables collaborative training of shared models while preserving decentralized data. Federated-Learning (FL) is a decentralized approach to training machine learning models that gives advantages of privacy protection, data security, and access to heterogeneous data over the usual centralized machine learning approaches. FL differs from traditional centralized machine learning techniques in its capabilities to merge local datasets into one training session, where FL distributes local data samples identically. FL can handle the devices' trustworthiness and malicious actors' impact on the learned model.

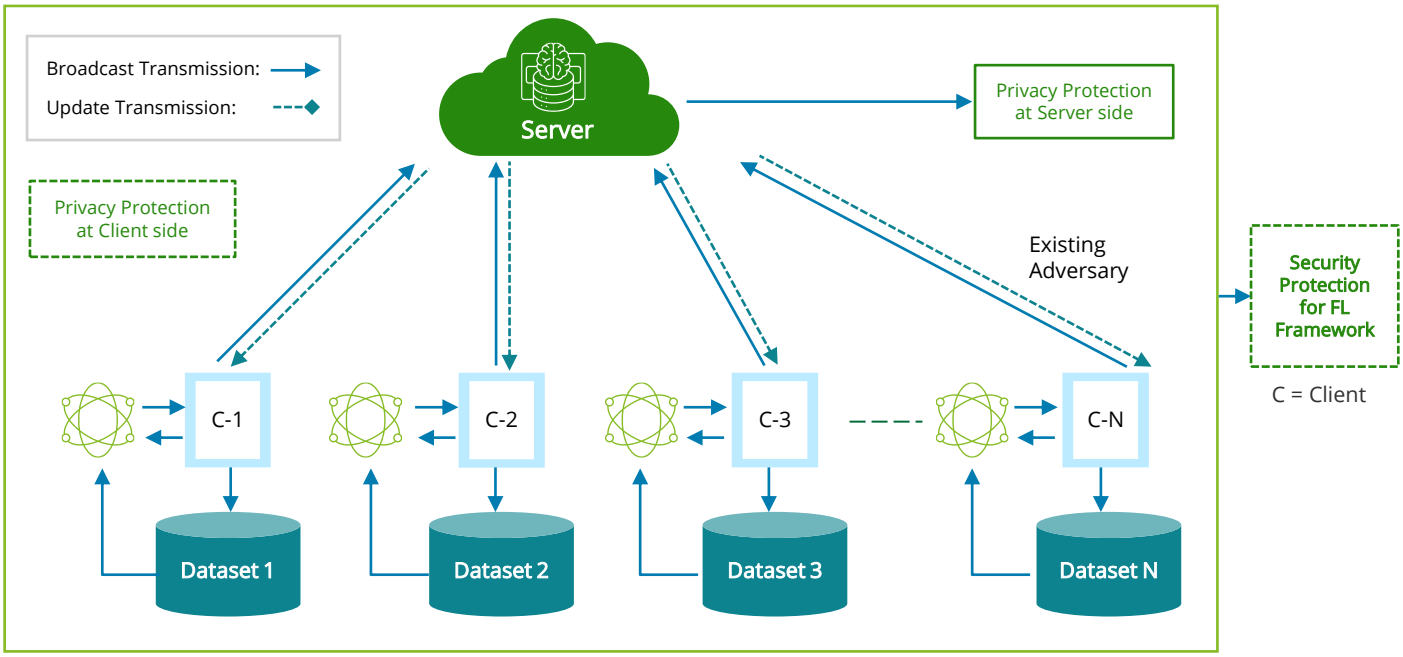


Figure (1): Federated-Learning Architectural View

4.1 Federated-Learning Approach

The Aggregation Server model consists of a single and central aggregator surrounded by nodes. The Federation of training nodes receives the global model from the aggregation server, and then each node independently starts the training model with its data. Afterward, they resubmit their partially trained models to a central server for aggregation and then continue training after receiving the consensus from the central aggregator. This type of architecture is proper when an entity needs to train its Machine Learning model on various non-communicating nodes (e.g., clients of other institutions) acting as trainers.

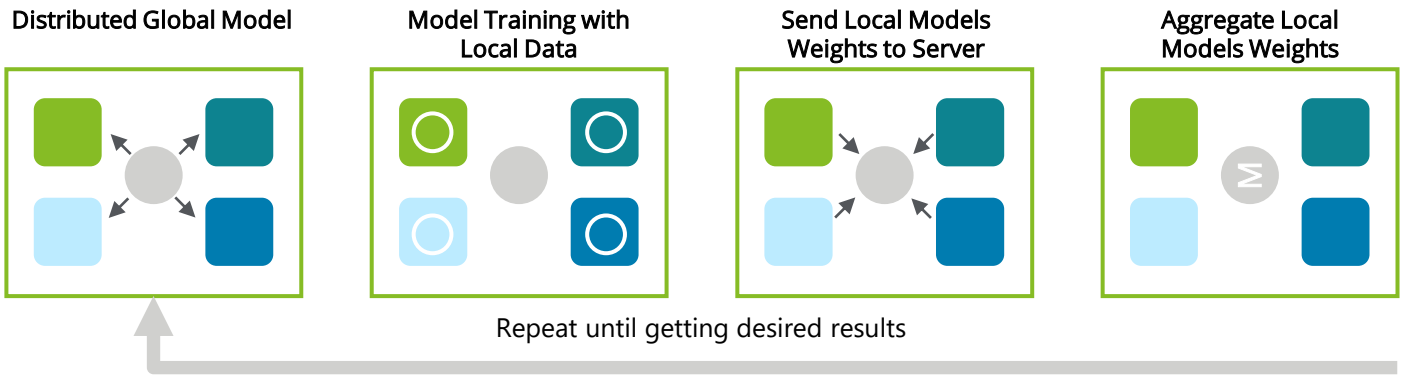


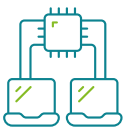
Figure (2): Federated-Learning Workflow Cycle – Aggregation Local Models Weights

4. Understanding Federated-Learning

Development starts by defining the problem and selecting participants who will contribute their local data. Design a model architecture that accommodates participant constraints and partition the data among them. Each participant trains a local model, and their updates are aggregated using techniques like federated averaging. Evaluate the aggregated model, deploy it for inference, and continuously monitor and refine it over time while ensuring ongoing privacy and collaboration with participants.

4.2 Federated-Learning Development Steps






Problem FL Data Formulation	Data Privacy, Security Measures & Data Partitioning	Model Aggregation	Analyse Results & Model Effectiveness
Defining the problem that FL intends to solve.	Defining the security measures to protect the private information stored on client devices.	Combining local model updates from many clients into a global model.	Providing an overview of the datasets used in our tests and their corresponding properties.
Defining the goal of our study the activities involved in the learning process.	Defining the capability to preserve raw data on the client side and only share model changes with the central server is essential.	Model updates while reducing information loss and maintaining the correctness of the overall model.	Full description of the utilized experimental setup, including the hardware, software, and network setups.
Defining Architecture based on the problem formulation.	Examine several privacy-preserving techniques that are protecting individual data while improving the overall models, such as: 1. Differential privacy, secure multi-party computation (SMPC). 2. Homomorphic encryption.	Identifying aggregation techniques like weighted averaging, federated averaging, or federated stochastic gradient descent (FSGD).	Creating relevant assessment measures and giving the findings from our experiments to evaluate the performance of the model.
Defining main components: 1. Central server (aggregator). 2. Participating nodes (Clients).		Examine the justification for selecting a specific aggregation technique based on communication effectiveness, convergence speed, and model stability.	Examining the justification for selecting a specific aggregation technique based on elements including communication effectiveness, convergence speed, and model stability.
High Level diagram including the data updates and communication among the architecture.	Identifying partitioning and distribution of the dataset among the participating client devices, including stratified partitioning and random partitioning, Non-IID (non-independent and identically distributed) data handling.	Identifying difficulties posed by client heterogeneity, such as different computing power and data quality.	Evaluating the efficiency of our federated process learning model.

5. Core Challenges in Federated-Learning

Since FL is a technology approaching a relative maturity stage, it has yet to be widely used compared to other technologies. So far, many FL-concerned enterprises prefer to use FL in training their Machine-Learning models in a distributed manner while preserving the original locations of their sensitive raw data. Slower convergence and poorer model performance might occur due to the communication overhead associated with sharing data between various devices or systems during the training related to multiple vulnerabilities. More importantly, systems & data heterogeneity and privacy concerns are perhaps the most anticipated challenges in FL [6].

5.1 Systems- & Data-Heterogeneity

It is difficult to effectively compare and combine different Federated-Learning systems because protocols, algorithms, and assessment measures are not standardized. Solving those issues enables us to fully realize the benefits of Federated-Learning across various applications and domains. Data heterogeneity is a significant issue since generalizable models cannot be successfully trained using decentralized data from numerous sources due to variances in data distributions. In FL, two sets of data heterogeneity exist;

1. Structured Data:
Structured data is data that adheres to a specific format or schema, which is often available in relational databases and spreadsheets. It is typically quantitative data, highly organized and easily decipherable by machine learning algorithms. A significant challenge in the FL of Structured Data is Data Normalization, where each entity may have its own data format or standard.

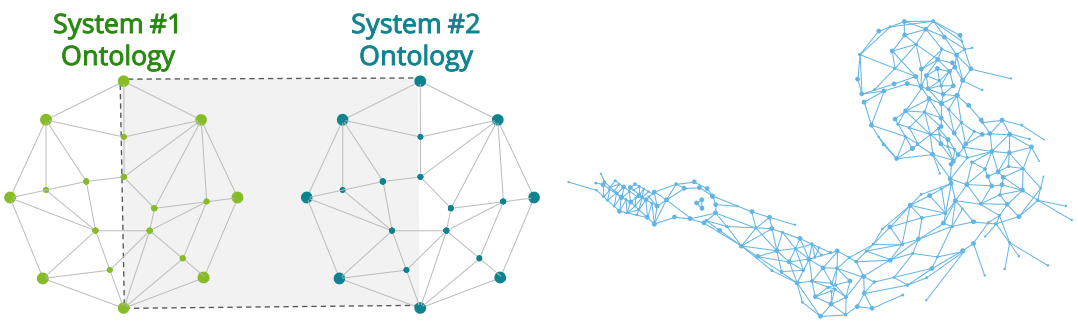
A practical example in product development is the Requirements-Interchange-Format (ReqIF), where the formats from different systems & tools are standardized for representing requirements data, making it easier to share and manage structured data across various stages of product development. ReqIF can be complemented by Standard-for-the-Exchange-of-Product-Model-Data (STEP), an ISO-10303 international standard for facilitating the exchange of computer-readable product data across multiple systems and software applications. Using ReqIF and STEP, structured data can be well-harmonized for collaborative learning.

2. Unstructured Data:
Unstructured data does not have a predefined data model and is typically qualitative data, such as text documents, images, audio, and videos. Therefore, it cannot be processed and analyzed via conventional data tools and methods. One major challenge is the FL computational limitations in data size and processing the data before feeding it to the FL model.

In product development, there are two types of unstructured data: Non-Synthetic and Synthetic Data. Non-Synthetic Data (real data) results from real-world observations, such as experiment measurements and physical prototypes, where the data is used to simulate various product scenarios. Synthetic Data, on the other hand, refers to artificially generated data that emulates real-world data but is not collected from actual observations (e.g., Finite-Element-Analysis). Both unstructured non-synthetic & synthetic data need to be systematically processed, harmonized, and mapped before feeding it to the FL model.

Dealing with Data Heterogeneity

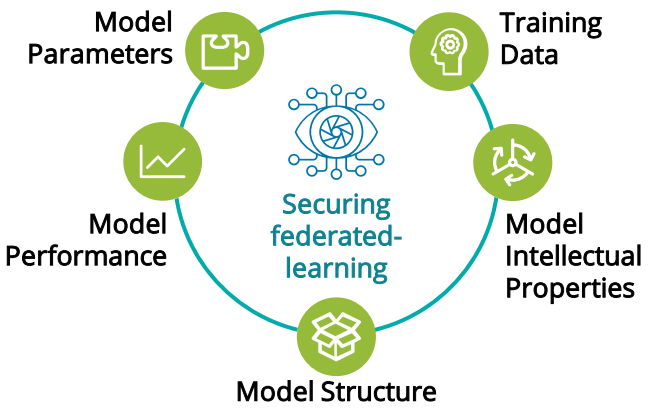
Deloitte offers an engineered Knowledge-Graph Ontology that plots multiple data into it. It establishes End-to-End (E2E) traceable relationships between data structures and prepares them as predictable objects. E2E traceability enriches data modeling to make it machine-interpretable with a thematic context. Additionally, queries-based powered-AI human interaction is possible, where users can have a human Natural-Language dialogue with the system.



ReqIF = Requirements-Interchange-Format | STEP = Standard-for-the-Exchange-of-Product-Model-Data

5.2 Privacy Concerns

Another difficult task that requires complex strategies to secure sensitive data is guaranteeing data privacy and security when training on decentralized data, primarily that enterprises shall protect their intellectual properties. Therefore, it is recommended to look at the security aspects from 5 different perspectives [7].



Model Parameters & Training Data
Model inversion attacks have been a central research area of Federated-Learning. It is a reversed engineered AI attack by analyzing its outputs and reconstructing its parameters. Providing security protocols keeps private datasets safe by preventing raw datasets from being stolen or manipulated.

Model Intellectual Property (IP)
Preserving IP rights in the model assets is crucial in a collaborative learning environment among different entities.

Model Structure
If the FL global model structure is pre-defined and shared among each participant, this might expose the model to vulnerabilities.

Model Performance
The trade-off between model performance and security is another challenge. In case a malicious user attacks one of the model contributors, the attacker can impose manipulation on the model data that impacts the model training and degrades the performance.

Preserving Privacy Techniques

In general, privacy preservation techniques for a distributed learning system target two main objectives: exchanging the privacy of the training set and the local model parameters with other nodes and/or a centralized server. Regarding this topic, there are notable privacy-preserving techniques in Machine Learning, such as Data Anonymization, Differential Privacy, Multi-Party-Computation (MPC), and Homomorphic Encryption.

Data Anonymization
Data anonymization or de-identification constitutes a method for concealing or eliminating personal information and sensitive data, such as Personally-Identifiable- Information (PII), from data to make a person unidentifiable in the changed dataset. As a result, the data anonymization process must strike a delicate balance between ensuring privacy and maintaining usability, given that concealing or eliminating data might diminish the distinguishing capacity of the dataset. Moreover, when coupled with supplementary details derived from other unidentified datasets, an individual within the data could be re-identified, exposing them to a privacy breach known as a linkage attack.

Differential Privacy
An advanced version of the perturbation privacy method involves adding random noise to actual data outputs. Those noises make it statistically challenging to differentiate between the original dataset and one with differentially added noise. Thus, individual identities remain hidden, as statistical queries on the initial dataset yield nearly identical results regardless of an individual's presence.

However, there's a balance between privacy and utility, as excessive noise can reduce dataset reliability. Differential privacy is widely used in Machine Learning algorithms like Logistic Regression, Support Vector Machine (SVM), and Deep Learning.

Multi-Party-Computation (MPC)
MPC, often called privacy-preserving computation, is an advanced technique enabling multiple parties to compute over a shared dataset collaboratively. Each participant contributes their input data, and the computation yields results without divulging individual data specifics, except for the final outputs. This approach is precious for upholding data privacy during distributed learning scenarios, where computations are performed across various entities' data holdings without directly sharing raw data. MPC ensures that sensitive information remains confidential while still allowing meaningful collective computations to take place.

Homomorphic Encryption
An alternative strategy for safeguarding data privacy, particularly tailored for Aggregation Server architecture, involves a distinct methodology. This technique empowers the execution of computations on encrypted data, eliminating the necessity for the secret decryption key. The computation's outcomes are presented in an encrypted format, only susceptible to encryption by the entity that requested the computation.

IP = Intellectual-Property | MPC = Multi-Party-Computation | SVM = Support-Vector-Machine

6. Federated-Learning Applications

Data privacy is paramount in extensive data collection from mobile devices and edge servers. Federated-Learning (FL) has emerged as a vital solution with notable applications while ensuring data privacy & security in sectors such as:

Improving the accuracy of object detection, lane detection, and traffic prediction in autonomous vehicles. It enables organizations to train AI models on decentralized data.

Enabling secure, collaborative analytics that enhances patient care by training models on patient data without centralizing or sharing that data.

Can be used to build models on user behavior from a data pool of mobile communication without leaking personal data, such as for next-word prediction, face detection, etc.

Can be used to improve fraud detection, credit scoring, and customer segmentation in financial services. It enables organizations to train AI models on decentralized data.

Federated-Learning makes it easier to perform a time-series analysis of the industrial environment factors obtained using multiple sensors and companies.

6.1 Autonomous Driving

Industries dealing with sensitive data, such as autonomous driving (AD), face significant privacy concerns. The drawbacks of centralized training are that it needs to adjust to the ever-changing environment of each device. Challenges include rapid real-world response requirements, potential communication bottlenecks, and the necessity to effectively enhance safety by minimizing latency. Additionally, the unequal contribution of data by various devices potentially leads the model to exhibit biased tendencies towards the devices contributing the most data, especially in Vehicle-to-Everything (V2X), where communication encompasses between vehicles and environmental elements [8]. A few FL advantages in AD are:

Data Privacy & Security
Model training without transferring raw data to the centralized server.

Latency Communication
Learns from local data and adapts models to dynamic conditions.

Scalability
Capability to update models on each vehicle without requiring a massive centralized computational infrastructure.

Resilience to Communication Loss
Vehicles possessing a locally trained model continue to make decisions in case of temporary disconnection from the network.

97% of cars are projected to become connected by 2026

V2X = Vehicle-to-Everything

6.2 Healthcare

In the healthcare field, patient information confidentiality is a primary concern, and the sharing of such data between different medical institutions is restricted. FL offers a fitting solution for safeguarding sensitive medical information. When implementing FL in healthcare contexts, individual hospitals can be considered distinct clients, while a central server could function as a data hub under a government agency's supervision. In this approach, each hospital obtains an initial shared model from the server, conducts training using its local data, encrypts the model after training, and then uploads the encrypted model back to the server. The global model is subsequently updated through a federated algorithm. As a result of this process, the data hub acquires an enhanced disease detection model. The integration of FL into intelligent medical applications is thereby facilitated.

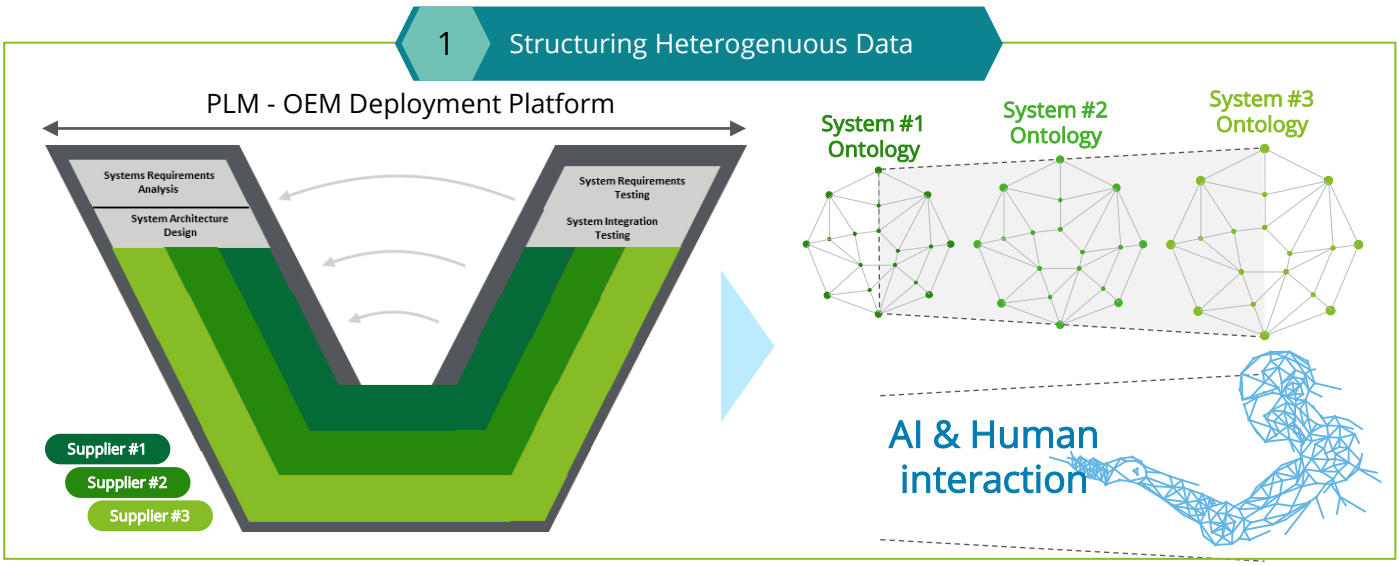
The practicality and efficacy of FL technology offer viable recommendations for implementing intelligent services within the medical sector. Integrating FL with the medical industry enables the creation of a high-performing disease detection model while upholding patient privacy. This synergy contributes to advancing intelligence within the medical field [9].

Studies have demonstrated the feasibility of implementing FL for multi-institutional collaboration among clinicians in Neurosurgery [10]

7. Use-Case (1): Product-Lifecycle-Management in Software-Defined-Vehicles (SDVs)

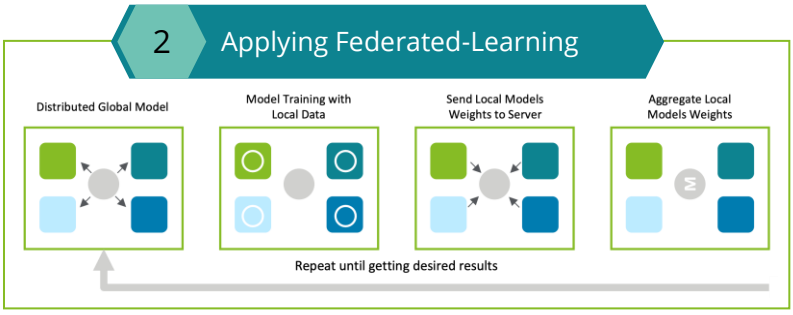
As software complexity in vehicles continues to rise, the software and underlying architecture are becoming the key differentiator for automotive Original-Equipment-Manufacturers (OEMs). SDV is experiencing a shift from the integrated domains state-of-the-art towards the futuristic software-guided architecture, which raises significant technical and regulatory complexities that OEMs and suppliers are obligated to handle, especially when sharing sensitive data.

Scenario: Multiple Suppliers Mutually Developing Software Products for an OEM



Deloitte's expertise in PLM offers a framework that operates within distinct architectural layers. For instance, requirements, functional, logical, and physical models define the product's evolution from concept to operations, as shown in the V-Model based on ISO/IEC 15288. As a result, Systems Ontology establishes End-to-End (E2E) traceable relationships between data structures and prepares them as predictable objects, where Natural-Language-Processing (NLP) tool can be applied for human interaction.

Federated-Learning can analyze data from human drivers to predict how they respond when faced with sudden lane changes by other vehicles. This knowledge can help train autonomous vehicles to anticipate and safely navigate similar scenarios.



Deloitte's Ontology establishes End-to-End (E2E) traceable relationships between data structures and prepares them as predictable objects.

Federated-Learning can mitigate privacy concerns among mutual development platforms, whereas utilizing other machine learning techniques such as Natural-Language-Processing (NLP) can predict the users' behavior, where recommended design changes for autonomously driven SDVs are provided.

8. Use-Case (2): Federated-Learning in Large-Language-Models (LLMs)

Large-Scale-Language-Models (LLMs) have garnered substantial interest and have been applied across various fields. However, their practical implementation faces hurdles in real-world situations. These obstacles stem from the limited accessibility of publicly available data and the imperative to safeguard the privacy of proprietary data. In response to these challenges, Federated-Learning (FL) has arisen as a promising solution, allowing for collaborative training of shared models while upholding the decentralized nature of data [11].

Large-Language-Models (LLMs)

LLMs are a type of AI that is capable of emulating human intelligence. They employ statistical models to scrutinize immense datasets, acquiring an understanding of the relationships and associations among words and phrases. Such employment enables them to produce fresh content, like essays or articles, that closely aligns with the stylistic characteristics of a particular author or genre. LLMs have demonstrated exceptional capabilities in handling complex tasks, as evidenced by their capacity to participate in conversational interactions that closely resemble human conversations, as illustrated by ChatGPT. The efficiency of the LLMs is significantly dependent on the scale of their model sizes and the extent of their training datasets [12-13].

Tackling LLMs Challenges by Using Federated-Learning

Consider a situation: three hospitals train Software-as-a-Medical-Device (SaMD) LLMs for a medical device purpose. They use large patient data to analyze their cardiovascular clinical studies. On an individual basis, each of these entities possesses datasets that are insufficient for training a robust model. However, if these organizations were to work together and pool their datasets, the resulting combined dataset would be substantial. Unfortunately, real-world data privacy regulations often constrain direct data sharing among separate entities, exacerbating concerns about data scarcity and privacy protection.

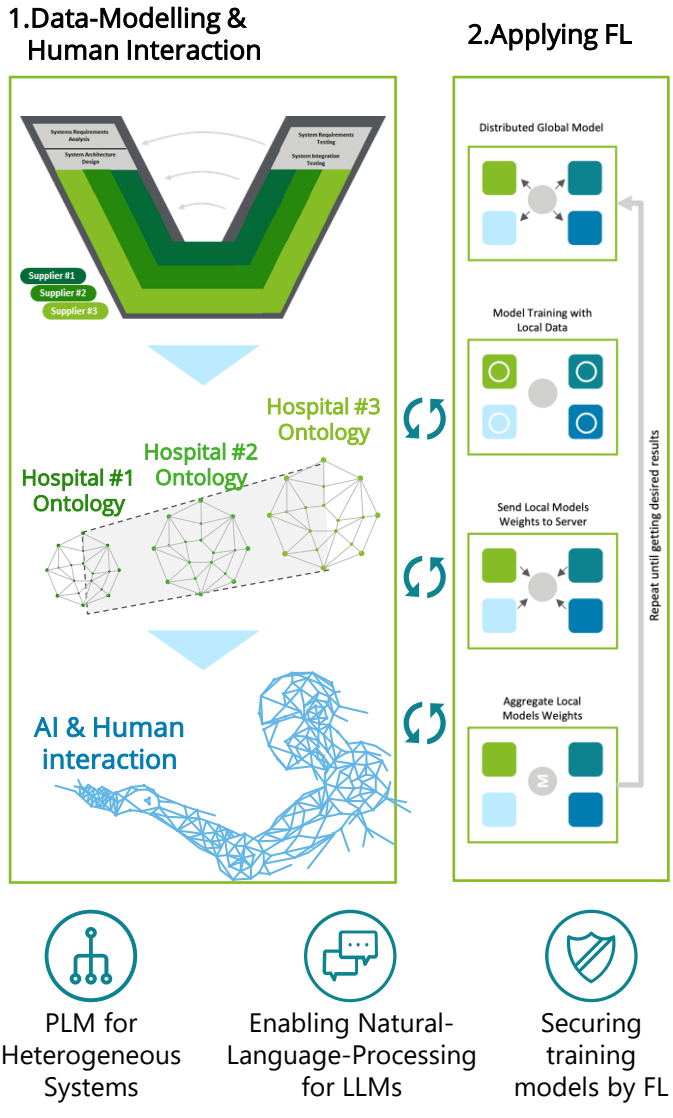
Addressing the challenge of using private domain data for modeling purposes while maintaining data privacy is paramount. One primary approach to privacy-preserving computation is Federated-Learning (FL), which incorporates privacy-preserving mechanisms into collaborative modeling efforts.

Product-Lifecycle-Management Role

As mentioned in the preceding chapters, PLM can complement the FL approach by contributing to structuring the heterogeneous data from multiple hospital models.

Consolidated PLM, LLM, & FL Framework

As illustrated below, valuable benefits can be gained by combining PLM, FL, and LLM.



LLM = Large-Language-Model | PLM = Product-Lifecycle-Management | FL = Federated-Learning

9. Why Deloitte is the Perfect Partner

Deloitte company profile

Deloitte's deep expertise in Product-Strategy-and-Lifecycle-Management, complemented with Deloitte's AI-Institute, offers a multidisciplinary framework to elevate its clients' competitive advantages in the market. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 457,000 people worldwide make an impact that matters at www.deloitte.com/de.

Multidisciplinary
Multidisciplinary solutions to complex business issues

Technology
Innovative and technology-based solutions

Industry/Sector expertise

Cross-border collaboration and expert knowledge

Industry/Sector expertise

Multidisciplinary team

Product-Strategy-and-Lifecycle-Management (PSLM): Product Strategy & Lifecycle Management uses a 360-degree approach to transformation projects concerning integrated, systems-based product development and data management across the product lifecycle. Using our end-to-end approach, we can assist you with whatever challenges you face, whether in Product-Lifecycle-Management strategy, systems & software engineering, product compliance, or the digital thread.

Deloitte PSLM Offering

Product-Lifecycle-Management
Planning, building and running the engineering systems of the future for PLM & ALM

Systems Engineering
Currently the top-focus within product development

Software Defined Vehicle
Software-led ecosystem continues to adapt and evolve post-sale

Embedded Systems & SW Dev.
Shift from hardware to software and solving functional complexity

Product & Regulatory Compliance
Capability to perform assessments and fulfill product liability & warranty

Digital Thread
Connected value chain from engineering over production to service

Other Deloitte Offerings

AI Institute:
The AI Institute is at the center of an international ecosystem through which we and our clients gain access to the most innovative startups, leading research and development teams, and companies and innovators. The focus is on developing and advancing the latest AI technologies.

Human Capital:
Making humans better at work and working better for humans. Unlocking human potential creates productive, adaptable organizations that are resilient to risk, fit for the future, and grounded in purpose.

Technology Strategy & Transformation:
Deloitte's specialists help organizations reset their IT strategy and implement the systems and solutions, including cutting-edge cloud services, to re-energize performance across the enterprise.

Deloitte's Starter-Kit

Incubation Workshops → Business- & Use-Cases Evaluation → Proof-of-Concept

10. Conclusion

In conclusion, this paper delves into Federated-Learning in Product-Lifecycle-Management (PLM), highlighting its significance in addressing the challenges posed by the need for collaborative product development while safeguarding data privacy. It begins by emphasizing the critical role of PLM as a holistic process guiding products from conception to operational excellence through intricate layers of architectural design and deployment.

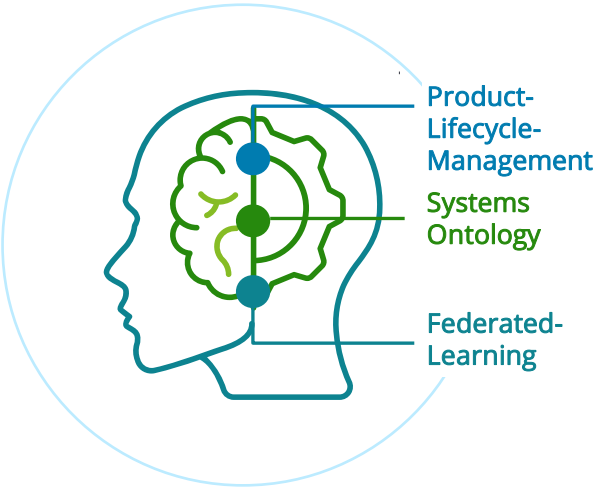
The paper underscores the potential of AI to empower PLM, encouraging enterprises to embrace AI adaptation while being mindful of ethical, privacy, and monitoring considerations. It then provides a comprehensive understanding of Federated-Learning, a decentralized machine learning technique that preserves data privacy and security, distinguishing it from traditional centralized approaches.

Challenges associated with Federated-Learning include communication overhead, model performance, data heterogeneity, and privacy concerns. Innovative solutions, such as Knowledge-Graph Ontology and end-to-end traceability, are proposed to address these challenges effectively.

The paper explores diverse Federated-Learning applications, demonstrating their relevance in autonomous driving, healthcare, mobile communication, financial services, and industrial environmental monitoring. Two compelling use cases were presented: one in Software-Defined Vehicles (SDVs) and another in Large-Language Models (LLMs), showcasing how Federated-Learning can mitigate privacy concerns and enhance data security in these domains.

Deloitte Product Strategy and Lifecycle Management (PSLM) asserts its position as the ideal partner for organizations embarking on Product Strategy and Lifecycle Management (PSLM) transformations.

With a 360-degree approach to integrated, systems-based product development and data management, it offers a comprehensive suite of services, including incubation workshops, business case evaluation, and proof-of-concept support. By combining PLM, Federated-Learning, and Large-Language Models, this paper outlines a path toward unlocking valuable benefits for heterogeneous systems, enabling Natural-Language Processing for LLMs, and securing training models through Federated-Learning.



Contacts

Ulrich Schoof
Director
Product Strategy & Lifecycle Management
uschoof@deloitte.de

Christian Ewertz
Director
Product Strategy & Lifecycle Management
cewertz@deloitte.de

Authors

Mohammad Haifawi
Senior Consultant
Product Strategy & Lifecycle Management

Gaurav Makwana
Junior Staff
Product Strategy & Lifecycle Management

Contributors

Sandro Urban
Manager
Product Strategy & Lifecycle Management

Felix Wunner
Manager
Product Strategy & Lifecycle Management

11. References

[1] https://www.morganlewis.com/blogs/sourcingatmorganlewis/2023/01/study-finds-average-cost-of-data-breaches-reaches-all-time-high-in-2022#:~:text=The%20other%20top%20five%20countries,and%20Germany%20at%20%244.85%20million.

[2] Artificial intelligence in Product-Lifecycle-Management, The International Journal of Advanced Manufacturing Technology · March 2021

[3] https://hbr.org/2019/07/building-the-ai-powered-organization

[4] https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending

[5] https://www.marketsandmarkets.com/Market-Reports/federated-learning-solutions-market-151896843.html

[6] https://www.theodi.org/article/federated-learning-an-introduction-report/#:~:text=Privacy%20enhancing%20technologies%20(PETs)%20could,of%20awareness%20and%20practical%20application.

[7] Federated-Learning with privacy-preserving and model IP-right-protection. Machine Intelligence Research, vol.20, no.1, pp.19–37, 2023.

[8] https://medium.com/@ys2223/a-study-of-federated-learning-in-autonomous-vehicle-system-ca9be70291fc

[9] International Journal of Machine Learning and Cybernetics (2023) 14:513–535 , https://doi.org/10.1007/s13042-022-01647-y

[10] Cheung, Alexander T. M. MBHL*; Nasir-Moin, Mustafa AB*; (Fred) Kwon, Young Joon PhD*; Guan, Jiahui PhD‡; Liu, Chris BS*; Jiang, Lavender BS*,§; Raimondo, Christian BS*; Chotai, Silky MD‖; Chambless, Lola MD‖; Ahmad, Hasan S. BS¶; Chauhan, Daksh BS¶; Yoon, Jang W. MD, MSc¶; Hollon, Todd MD#; Buch, Vivek MD**; Kondziolka, Douglas MD*; Chen, Dinah MD††; Al-Aswad, Lama A. MD, MPH††; Aphinyanaphongs, Yindalon MD, PhD‡‡; Oermann, Eric Karl MD*,§,§§. Methods and Impact for Using Federated-Learning to Collaborate on Clinical Research. Neurosurgery 92(2):p 431-438, February 2023. | DOI: 10.1227/neu.0000000000002198

[11] Federated Large Language Model : A Position Paper Chaochao Chen, Xiaohua Feng, Jun Zhou, Jianwei Yin, Xiaolin Zheng Zhejiang University, Hangzhou, China

[12] Kaplan, J., McCandlish, S., Henighan, T., Brown, T. B., Chess, B., Child, R., Gray, S., Radford, A., Wu, J., and Amodei, D., "Scaling laws for neural language models," arXiv preprint arXiv:2001.08361, 2020.

[13] Hoffmann, J., Borgeaud, S., Mensch, A., Buchatskaya, E., Cai, T., Rutherford, E., Casas, D. d. L., Hendricks, L. A., Welbl, J., Clark, A., et al., "Training compute-optimal large language models," arXiv preprint arXiv:2203.15556, 2022

Deloitte.

Created by CoRe Creative Services. RITM1688127