Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

Ontology-guided Data Sharing and Federated Quality Control with Differential Privacy in Additive Manufacturing

Tsegai O. Yhdego
Department of Industrial and Manufacturing engineering,
Florida A&M University
Florida A&M University - Florida State University College of Engineering
2525 Pottsdamer St.
Tallahassee, FL 32310, USA

Hui Wang[1]
Department of Industrial and Manufacturing engineering,
Florida A&M University
Florida A&M University - Florida State University College of Engineering
2525 Pottsdamer St.
Tallahassee, FL 32310, USA
email: hwang10@eng.famu.fsu.edu

Hongmei Chi
Computer and Information Sciences,
Florida A&M University,
1333 Wahnish Way
Tallahassee, FL 32307, USA

Zhibin Yu
Department of Industrial and Manufacturing engineering
Florida A&M University,
Florida A&M University - Florida State University College of Engineering
2525 Pottsdamer St.
Tallahassee, FL 32310, USA

The scarcity of measured data for defect identification often challenges the development and certification of additive manufacturing processes. Knowledge transfer and sharing have become emerging solutions to small-data challenges in quality control to improve machine learning with limited data, but this strategy raises concerns regarding privacy protection. Existing zero-shot learning and federated learning methods are insufficient to represent, select, and mask data to share and control privacy loss quantification. This study integrates differential privacy in cybersecurity with federated learning to investigate sharing strategies of manufacturing defect ontology. The method first proposes using multilevel attributes masked by noise in defect ontology as the sharing data structure to characterize manufacturing defects. Information leaks due to sharing ontology branches and data are estimated by epsilon differential privacy (DP). Under federated learning, the proposed method optimizes sharing defect ontology and image data strategies to improve zero-shot defect classification given privacy budget limits. The proposed framework includes (1) developing a sharing strategy based on multilevel attributes in defect ontology with controllable privacy leaks, (2) optimizing joint decisions in differential privacy, zero-shot defect classification, and federated learning, and (3) developing a two-stage algorithm to solve the joint optimization, combining stochastic gradient descent search for classification models and an evolutionary algorithm for exploring data-sharing strategies. A case study on zero-shot learning of additive manufacturing defects demonstrated the effectiveness of the proposed method in data-sharing strategies, such as ontology sharing, defect classification, and cloud information use.

Keywords: Cyber Physical Security for Factories, Cybermanufacturing, Industrial Internet of Things, Engineering Informatics, Machine Learning for Engineering Applications

1 Introduction

During the development of additive manufacturing (AM) processes, process data measurement is essential to understand printing defects for process certification and quality control. However, data measurement can be time-consuming and expensive, especially the microstructural characterization of defects, imposing labeled data scarcity challenges in the early stage of process development.

Manufacturing researchers have begun to realize the capability of zero-shot learning (ZSL) from computer vision to assist in identifying unseen faults. ZSL methods typically involve transferring knowledge from known defect classes to unknown ones by leveraging semantic relationships and feature similarities. For example, Socher et al. [1] explored ZSL for image classification using semantic embeddings to generalize to unseen classes, which can be adapted for manufacturing defect detection. Elhoseiny et al. [2] also presented ZSL approaches that utilize semantic attributes, which are relevant for identifying manufacturing defects in novel products.

These approaches rely on certain knowledge bases, such as dictionaries, to accurately embed the anomaly information as vectors to describe the characteristics of the anomalies and the associated manufacturing conditions. Inaccurate embedding of anomalies may sometimes lead to classification performance like a random guess. With the advancement of cloud technology, we envision that sharing such a knowledge base among manufacturers and researchers can be an effective strategy to improve defect embedding. However, one major challenge is that manufacturers are concerned with privacy loss, although they can benefit from data sharing.

With the advancement in cloud technology and machine learning, knowledge-sharing strategies provide new opportunities for overcoming the labeled data scarcity challenge. Cloud platforms can offer a shared space where manufacturers can disseminate and derive insights from peer data. Manufacturers can significantly accelerate process certification and improvement using advanced techniques such as federated learning and transfer learning. In particular, data shared in such environments is typically masked with noise to protect against revealing the entirety of a manufacturer's defects knowledge base.

1.1 Challenges and Privacy Concerns.

The main issue is that consistent sharing, even masked data, could inadvertently expose the complete knowledge of a manufacturer. Concerns about intellectual property protection and trade secrets are raised, impeding knowledge transfer across businesses. This possibility fosters concerns regarding protecting intellectual property and trade secrets, thus potentially restricting knowledge transfer among firms. Manufacturers are not necessarily opposed to data-sharing; in fact, they see potential advantages for their process development. Their primary reservation stems from the absence of tools to measure potential data leaks that could offer competitors an undue advantage. If manufacturers had tools to assess and set privacy exposure levels, they could strategically weigh the benefits of data-sharing against their privacy concerns. They can thereby determine a strategy to

[1]Corresponding Author.
Version 1.18, October 11, 2024

maximize the cost-effectiveness of data-sharing, i.e., achieving the best learning accuracy based on the least privacy budget.

1.2 Research Objective and Scope. This paper explores key questions central to the advancement of secure, cloud-based knowledge sharing within the manufacturing sector. The focus is to investigate sharing strategies based on appropriate data structures to optimize the efficacy of collaborative learning while simultaneously containing privacy exposures for individual manufacturers. In the long run, the study will help identify data structures of defect knowledge that facilitate knowledge sharing in the cloud.

2 Collaborative Machine Learning Considering Privacy

Federated learning is an emerging extension of distributed machine learning, where data is utilized locally on each client [3]. A central server receives the updated machine learning parameters and aggregates them to improve the model through parameter averaging [4]. With this strategy, a central server acts as the coordinator for a decentralized network of manufacturers. Manufacturers can access local training data. They compute updates to the server's global model and send only the most recent updates back for model aggregation.

Federated learning introduces various collaborative model training environments tailored to specific objectives. Federated Averaging combines server-based model averaging and local stochastic gradient descent (SGD) effectively [3]. FedProx addresses heterogeneity challenges through an innovative optimization algorithm [5]. Personalized Federated Learning tailors shared models to individual client preferences for personalized adaptability [6]. Q-Fair Federated Learning (q-FFL) promotes fairness using an objective inspired by fair resource allocation [7]. Despite its benefits, federated learning poses challenges like private information leakage, high communication costs, and device variability [5]. However, the potential for collaborative and privacy-preserving model training is promising.

Federated learning has been applied in manufacturing to improve predictive maintenance, quality control, and defect detection. McMahan et al. [3] introduced Federated Averaging, aggregating local model updates into a global model, significantly enhancing privacy preservation. Kairouz et al. [8] provided a comprehensive overview of federated learning techniques, emphasizing their applications in various industries, including manufacturing. The federated learning approaches provide a certain level of protection by sharing the model instead of raw data. However, from a cybersecurity perspective, some knowledge reflected in the data can still be partially reconstructed from the model shared over the cloud. Manufacturers may not be confident with this level of privacy protection.

Differential privacy (DP) emerged to address data security and prevent model exposure [9]. Geyer et al. [10] propose a comprehensive DP-preserving federated learning approach protecting against model exposure and safeguarding a client's entire dataset from differential attacks by other manufacturers. Other notable DP-based learning methods include local DP (LDP) [11] and distributed DP-based SGD [12]. LDP allows clients to locally perturb information before transmitting it, preserving privacy for clients and the server against data leakage. These advancements address privacy challenges in federated learning, enabling safer and more collaborative model training.

Understanding and implementing differential privacy [13] is important in federated learning settings, where data privacy is paramount [14]. Differential privacy ensures that specific individual data presence or absence does not significantly impact analysis outcomes [15]. Central to differential privacy are mechanisms such as Laplace and Gaussian noise, vital for data perturbation as they introduce calibrated noise to mask individual contributions while preserving overall analysis outcomes [16]. This controlled noise addition balances data utility and privacy protection, a cornerstone of privacy-enhancing techniques. This principle is indispensable in collaborative environments for maintaining data confidentiality and enabling valuable insights extraction [17].

Differential privacy, crucial for privacy-preserving data analysis, preserves individual privacy [18] when obtaining insights from a dataset. The Advanced Composition Theorem [19] improves the previous composition Theorem, enhancing the privacy guarantees. This development halves the anticipated privacy loss bound for $(\epsilon, 0)$-differentially private techniques. Additionally, the Composition Theorem of [20] advances differential privacy with innovative data processing inequalities and an operational interpretation that involves hypothesis testing, surpassing previous benchmarks. [21] expands this field with Composition Theorems for Interactive Differential Privacy, generalizing optimal parallel composition properties across fundamental differential privacy notions, ensuring adversaries cannot gain an advantage by combining queries.

Recent studies have significantly advanced the fields of privacy preservation and cybersecurity in AM. Yue and Kontar [22] developed a Federated Gaussian Process Regression (FGPR) framework that enhances privacy and personalization in federated learning. Sturm et al. [23] exposed cyber-physical vulnerabilities in AM, underscoring the need for robust security measures. Blockchain and camouflage encryption was introduced in [24] to protect sensor data against cyber-physical threats, while [25] demonstrated its application in protecting AM systems from cyber-physical attacks in a critical healthcare context. These advancements address key challenges in data sharing and privacy leaks in AM. However, the preservation of sharing structured knowledge, such as the ontology for defect classification via federated learning, is notably unexplored.

3 Research Gaps

Although state-of-the-art research exists addressing data privacy and sharing issues under collaborative manufacturing environments, significant research gaps have been identified concerning data-sharing strategies with controlled privacy leaks:

- *Lack of Methods for Data Sharing to Improve Defect Embedding for ZSL:* Existing ZSL approaches in manufacturing have not adequately addressed knowledge sharing to enhance defect embedding. This paper proposes a novel method to utilize knowledge sharing to overcome this limitation.
- *Insufficient Addressing of Privacy Issues During Data Sharing by Existing Federated Learning Methods:* Current federated learning approaches do not sufficiently address privacy concerns, particularly regarding joint decisions and quantitative metrics to evaluate privacy loss. This includes the following sub-gaps:
  - *Lack of Strategies for Sharing Ontology Structures to Improve the Utility of Shared Data in Defect Classification with Controlled Privacy:* Existing machine learning techniques using knowledge transfer, such as transfer learning and federated learning, lack guidelines on strategies for sharing structured manufacturing data, such as manufacturing defect ontology, with controlled privacy.
  - *Lack of Metrics to Quantify Privacy Expenditure for Data Sharing Between Manufacturers:* Accurately quantifying privacy expenditure is crucial for guiding data sharing among manufacturers to improve learning performance for defect identification. It helps determine the amount of privacy information that can be safely shared.

This paper proposes a DP-attribute learning framework under federated learning to address research gaps. proposed method integrates a differential privacy model with federated learning to

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

improve knowledge sharing with privacy protection, thereby using the knowledge-sharing strategy to improve ZSL. The research addresses three questions for each manufacturer on the cloud: (1) How to represent the information in the knowledge base to be shared to help other manufacturers improve their ZSL; (2) How to select and mask the shared knowledge while balancing the trade-off between privacy protection and ZSL performance; and (3) How to quantitatively control privacy loss during knowledge sharing. A DP-Attribute Learning framework is developed to apply to various contexts of federated learning and can also be implemented independently without federated learning.

The methodology focuses on the following three aspects:

- Utilization of multi-level attribute embeddings of defect ontology masked by noise, characterizing defects to facilitate data sharing during federated learning;
- Development of a mechanism to quantify privacy expenditure based on DP to control privacy leaks;
- Formulation of DP-attribute learning framework under the context of federated learning to determine the selective sharing strategy of ontology structure on the cloud and leverage of cloud data with controlled privacy leaks. The proposed method is not tied to federated learning since it can be implemented without federated learning

4 DP-attribute learning under the context of federated learning for zero-shot learning

Background problem: zero-shot defect classification. Zero-shot learning addresses the challenge of classifying instances from classes that are not observed during the training phase but appear only in the testing phase. Specifically, in manufacturing defect classification, ZSL is essential for identifying new defect types that emerge over time without having labeled training data for these new classes. ZSL is particularly relevant in scenarios of labeled data scarcity, where obtaining labeled data is difficult and expensive. For instance, acquiring samples and generating microscopy images in manufacturing processes can be time-consuming and costly, making it impractical to have comprehensive labeled datasets for every possible defect type. ZSL leverages shared attributes between seen and unseen classes to overcome this limitation, enabling effective classification even with limited training data. This ZSL was improved by ontology-attribute learning in our prior research [26] based on [27].

Let X be the space of input data (e.g., microscopic images of defects), and Y^{tr} and Y^{ts} be the sets of seen and unseen class labels, respectively, such that $Y^{\text{tr}} \cap Y^{\text{ts}} = \emptyset$. During training, the model has access to pairs $(\mathbf{x}, y)$, where $\mathbf{x} \in X$ and $y \in Y^{\text{tr}}$. In the testing phase, the goal is to correctly classify instances $\mathbf{x}$ from the unseen classes Y^{ts}. This approach leverages shared attributes between seen and unseen classes, represented by an attribute space $\mathcal{A}$. Each class y (seen or unseen) is associated with an attribute vector $\boldsymbol{\phi}(y) \in \mathcal{A}$. The learning task involves mapping input data $\mathbf{x}$ to its corresponding class y through a compatibility function C_p. The methodology formulates mapping function f as:

$$f(\mathbf{x}; \mathbf{W}) = \arg\max_{y \in Y} C_p(\mathbf{x}, y; \mathbf{W}), \tag{1}$$

where $\mathbf{W}$ represents the model parameters, $\mathbf{x}$ is the input data vector, and Y is the set of class labels for manufacturing defects. The goal is to accurately map the input data to their corresponding defect classes, enhancing the classification accuracy for both seen and unseen classes. The compatibility function C_p is defined by the features of the input data $\boldsymbol{\theta}(\mathbf{x})$ and the attributes of the class $\boldsymbol{\phi}(y)$ and can be represented as:

$$C_p(\mathbf{x}, y; \mathbf{W}) = max(\boldsymbol{\theta}'(\mathbf{x})\mathbf{W}\boldsymbol{\phi}(y)) \tag{2}$$

The parameter $\boldsymbol{W}$ is defined as compatibility-based learning parameter. Its dimension depends on the extracted image dimensions and the class embedding vector dimensions. Let: $\boldsymbol{\theta}(\mathbf{x})$ represent the features extracted from images, where $\mathbf{x}$ is the image data. $\boldsymbol{\phi}(y)$ represent the attributes of the class y in the embedding vector. The dimensions of W can be described as: If $\boldsymbol{\theta}(\mathbf{x}) \in \mathbb{R}^{d_1}$ and $\boldsymbol{\phi}(y) \in \mathbb{R}^{d_2}$, then $W \in \mathbb{R}^{d_1 \times d_2}$. This way ensures that W maps the feature vectors to the class embeddings, facilitating compatibility-based classification during the testing phase.

Since image processing has been well developed to extract features from images, the key challenge in implementing the ZSL is to find an appropriate embedding vector $\boldsymbol{\phi}(y)$ to characterize the class. Our prior work developed an attribute learning framework using a structured knowledge representation, known as an ontology, to capture and organize information about various entities and their relationships within a specific domain with applications to classify manufacturing defects [26]. The proposed ontology-guided ZSL leverages rich, hierarchical knowledge about defects, including their morphology, underlying causes, and associated materials (Fig.1).

The proposed ontology-guided ZSL consists of the following steps: (1) Ontology Construction: Identify relevant concepts, relationships, and constraints associated with manufacturing defects; (2) Ontology Exploration: A walking algorithm explores the branches of the defect ontology to extract descriptive sentences; (3) Natural Language Processing (NLP): Transform the descriptive sentences obtained from ontology exploration into contextualized embedding vectors using NLP models, such as transformers; and (4) Class Embeddings: Collect the embedding vectors for all classes in a matrix with dimensions corresponding to the number of classes and the embedding vector dimension. The ontology construction is the most essential step that organizes the relationships among attributes associated with each class under a hierarchical structure. The selection of the ontology branches and depth can significantly affect ZSL performance.

In real-world scenarios, training on vector embeddings of defects through ontology ensures consistent representation, mitigating variations in data quality and heterogeneity across different manufacturing units. Federated learning and cloud-based collaboration address class imbalances by enabling manufacturers to complement each other's data, resulting in an enriched ontology structure that comprehensively covers various attributes for defects. The ontology-based data structure also supports continuous learning, allowing real-time updates with new information and ensuring that all manufacturers benefit from the latest defect detection capabilities.

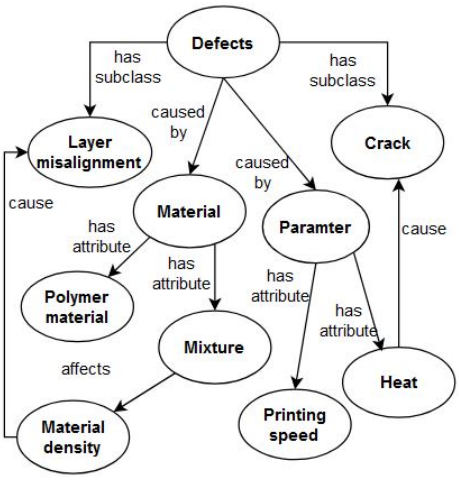

Fig. 1 Example multi-level attributes in a defect ontology characterizing two defects: layer misalignment and crack

Reivew of federated learning. In ZSL, data sharing based on diverse datasets is important in providing features and attributes

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

about manufacturing defects. However, it also raises significant concerns about data security and privacy leaks. Federated learning addresses these concerns by facilitating collaboration without sharing raw data among manufacturers. A federating strategy $\boldsymbol{F}$ should be sequentially developed to determine what parameters in the model are updated by the global model on the server. In this phase, multiple manufacturers participate by training local models and sending their parameters $\mathbf{W}_i^{(t)}$ to a central server. The server computes the global parameter as the average of this local parameters:

$$\mathbf{W} = \frac{1}{K}\sum_{i=1}^{K}\mathbf{W}_i, \tag{3}$$

which is then redistributed to each of K manufacturers for further training iterations. While federated learning can preserve raw data privacy, it does not inherently quantify the level of information leakage nor provides a mechanism to control the balance between privacy protection and information sharing. When manufacturers participate in federating learning, they are subject to unmeasured privacy concerns when benefiting from data sharing.

Reivew of differential privacy. To enhance the security framework in federated learning, this paper proposes to integrate DP with attribute learning in a federated manner. DP-attribute learning framework under federated learning becomes crucial for quantifying and controlling the level of privacy and information shared in the system. Differential privacy, as proposed by Dwork et al. [28], and extensively discussed by Dwork, Roth, and Vadhan [13], establishes a mathematical framework for protecting sensitive data. DP-attribute learning under federated learning setting, each manufacturer in the set of K manufacturers, denoted as $S = S_1, S_2, \ldots, S_K$, trains a local model using its data while ensuring privacy protection utilizing DP.

Consider D_i as a local dataset belonging to manufacturer S_i with an algorithm A_i that processes D_i to yield an output $A_i(D_i)$. The algorithm A_i satisfies ϵ_i-differential privacy if, for all datasets D_i and D_i' differing by a single record, the subsequent inequality is:

$$\Pr[A_i(D_i)] \leq e^{\epsilon_i} \cdot \Pr[A_i(D_i')] + \delta_i \tag{4}$$

This inequality is a privacy assurance that limits how much any individual data point in D_i can influence the output of A_i. Here, δ_i denotes the probability of any data point being singled out by an adversary, while ϵ_i serves as a control knob to balance the trade-off between data utility and privacy. Smaller ϵ_i values correspond to stronger privacy. It directly influences the noise characteristics in the algorithm's output, a pivotal aspect of the differential privacy mechanism.

Introducing noise, parameterized by σ_i, is fundamental in achieving (ϵ_i, δ_i)-differential privacy in a dataset. The noise level is crucial for masking individual contributions while maintaining the utility of the aggregated data. The value of σ_i is determined based on the privacy parameters ϵ_i and δ_i as follows:

$$\sigma_i = \frac{\sqrt{2\log(1/\delta_i)}}{\epsilon_i}, \tag{5}$$

where σ_i scales the Laplacian noise added to the data. This noise scaling is essential to ensure that each computational step within the algorithm maintains the prescribed differential privacy level, effectively striking a balance between privacy and utility.

To further illustrate the application of DP, consider a function $f(D_i)$ on a dataset D_i and its differentially private response $A_i(D_i)$. When employing the Laplace mechanism, the process is defined as:

$$A_i(D_i) = f_i(D_i) + \text{Laplace}(0, \sigma_i)$$

In this equation, the term σ denotes the scale of the Laplace distribution, directly influenced by the privacy parameter ϵ_i. The selection of ϵ_i is crucial as it regulates the level of privacy protection, with smaller values of ϵ_i indicating stronger privacy guarantees. A careful calibration of noise added not only safeguards individual data points but also preserves the overall utility of the data, demonstrating the intricate balancing in DP mechanisms.

In DP, Laplace noise is preferred over Gaussian noise for several reasons: it directly achieves ϵ-differential privacy by adding noise scaled to the sensitivity of the function, ensuring robust privacy without an additional delta parameter [13,29]. The heavier tails of the Laplace distribution add significant noise to outliers, enhancing privacy protection. Additionally, Laplace noise aligns with L_1-norm sensitivity, making it straightforward to implement and computationally efficient, crucial for large-scale federated learning scenarios [30]. In contrast, the Gaussian mechanism, aligned with L_2-norm sensitivity, involves more complex analysis and calibration of noise for (ϵ, δ)-differential privacy [31,32]. Extensive research has shown Laplace noise to be effective in differential privacy applications, balancing privacy and utility [9,10].

4.1 Two-stage formulation of DP-attribute learning framework under the context of federated learning. This formulation concerns the decision sharing of ontologies on the cloud instead of raw data since ontology can offer significant advantages in generating class embedding vectors to characterize manufacturing defects, thereby improving the ZSL performance for each manufacturer. Thus, a direct sharing of ontologies can best facilitate ZSL tasks for each manufacturer with limited data or knowledge base. Traditional data sharing based on information theory that focuses on optimizing the transmission and encoding of information lacks the structured representation that ontologies provide to help ZSL. Ontology-based data sharing offers several advantages: it provides enhanced interpretability with clear and structured data that both humans and machines easily understand; it ensures consistency and standardization across different datasets and systems; it supports scalability and flexibility, allowing for the easy addition of new data types and the expansion of existing datasets without disrupting the existing data structure; and it enables advanced reasoning and inference, allowing systems to infer new knowledge from existing data in ZSL, which is not typically possible with information theory-based methods.

As illustrated in Fig. 2, the decisions involved in DP-attribute learning framework under the context of federated learning include (1) the selection of the ontology branches (red arrows on the left), represented by a class embedding vector extracted from the shared ontology $\boldsymbol{\varphi}_i$, (2) local model parameters $\mathbf{W}_i$ to classify defects with each manufacturer, and (3) whether or not to use global model on the server (red arrows on the right) to update parameters in the local model according to a sequence of federating strategies $\boldsymbol{F}_{i(n)}$ over iterations n in the (n)th round, given noises determined by (ϵ_i, δ_i) to be added by each manufacturer i to mask the class embedding as extracted from the ontology and local model parameters (See distribution additions in Fig. 2),

The overall objective in this formulation is to minimize a loss function associated with the average error in defect classification between all manufacturers while learning a mapping function f (Eq. (1)). Constraints are imposed on the optimization problem to ensure data privacy for each manufacturer by limiting the loss incurred during attribute learning and data embedding to a predefined privacy budget. The proposed formulation can be represented as

$$\min\left\{\frac{1}{\text{Number of manufacturers}}\sum_{i=1}^{\text{Number of manufacturers}}\text{Overall error}\right\}$$

S.T.

$$\text{Overall privacy loss} \leq \text{Privacy budget limit}$$

Mathematically, the formulation is to find the optimal $\mathbf{W}_i$, $\boldsymbol{\varphi}_i$, a sequence of $\boldsymbol{F}_i = \{\boldsymbol{F}_{i(1)}, \boldsymbol{F}_{i(2)} \ldots \boldsymbol{F}_{i(n)}\}$, and (ϵ_i, δ_i) that minimize the average loss L_i across K manufacturers over federating iterations (1), (2), ... (n) (Eqn. (6)). It includes two stages of decisions: learning of local model parameters given the federated ontology-sharing strategy on each manufacturer in Stage 1 and the

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

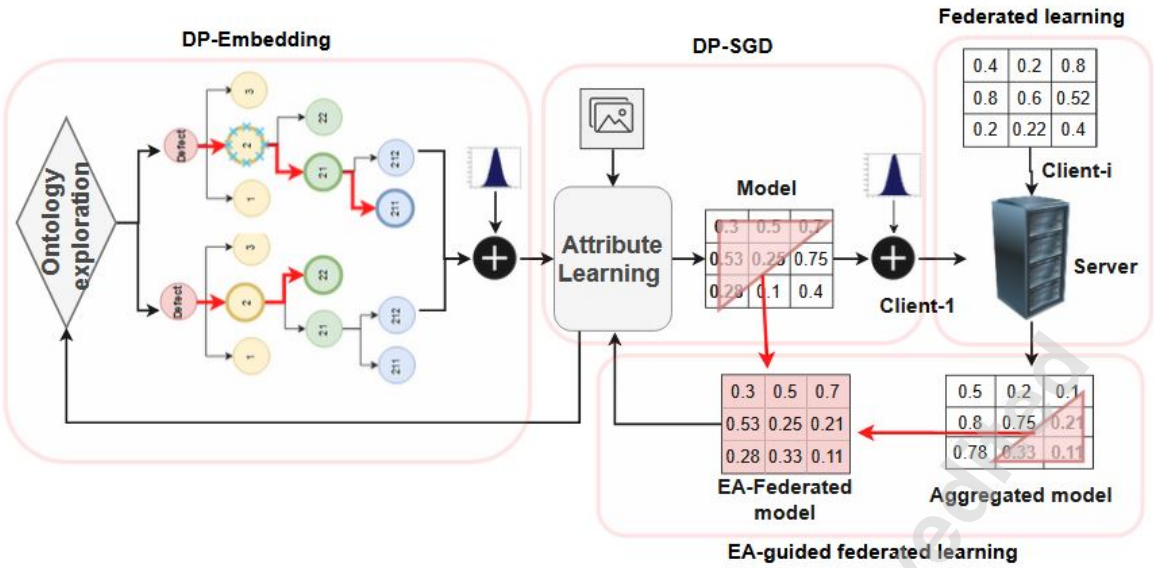

Fig. 2 Decisions involved in the proposed DP-attribute learning framework under the context of federated learning. Four decisions are outlined: selection of ontology branch depth to share (thick red arrows on the left) and federating strategy (thick red arrows on the right), local model parameter (Model matrix in the middle), and levels of noises added to ontology and models (dark distribution curves))

exploration of federated ontology-sharing strategies in Stage 2.

$$\min_{\boldsymbol{F}_i}\left\{\min_{\mathbf{W}_i,\boldsymbol{\varphi}_i|(\epsilon_i,\delta_i)}\frac{1}{K}\sum_{i=1}^{K}L_i(y_n,f_i(\mathbf{x}_n;\mathbf{W}_i,\boldsymbol{\varphi}_i)\right\} \tag{6}$$

S.T.

$$\mathrm{C}^{\mathrm{emb}}(\epsilon_i,\delta_i)+\mathrm{C}^{\mathrm{attr}}(\epsilon_i,\delta_i)\le \mathrm{B}_i,\forall i=1,2,...K \tag{7}$$

where each variable is defined as follows:(1) ϵ_i: The privacy budget parameter typically ranges from 0.01 to 10, (2) δ_i: Our formulation sets the probability of privacy loss parameter to zero, (3) Ontology privacy parameters, which measure the depth or branch of the ontology to be shared, typically ranges from 1 to 3, and (4) W_i: Local model parameters for each manufacturer, depending on the specific model architecture and learning rates.

The objective function is subject to the privacy budget constraints (Equation (7)). The federating strategy F_i in the outer loop (2nd optimization stage) is responsible for coordinating the sharing and updating of local models among the manufacturers. It determines the sequence of federating steps $F_i(n)$ that guide the selection and aggregation of local model updates. This strategy ensures effective communication and synchronization of model parameters across different manufacturers, optimizing the collaborative learning process and minimizing the overall loss. The overall privacy budget B_i is evaluated within these parameter ranges to ensure a balance between privacy preservation and model accuracy. The tested study ranges from 1000 to 10^6.

The constraints in Eqn. (7) are strictly satisfied through careful allocation of the privacy budget, the differential privacy mechanism, and iterative recalibration. Each manufacturer is assigned a specific privacy budget B_i based on data sensitivity, controlled noise is added to the embeddings to ensure cumulative privacy loss does not exceed B_i, and continuous calibration manages privacy expenditure to maintain compliance with the constraints. These constraints are critical in sharing defect ontology and attribute learning models under the federated learning framework. The advanced composition theorem [19,21] offers a way to evaluate this cumulative privacy loss, ensuring that both the class embedding and attribute learning processes privacy requirements.

- *Sharing of ontology through DP-embedding with privacy expenditure* $\mathrm{C}^{\mathrm{emb}}(\epsilon_i,\delta_i)$: This component estimates the extent to which the defect ontology can be shared during the class embedding phase. It reflects the frequency of sharing the noise-masked defect ontology and attributes extracted. By regulating the exposure of defect knowledge, this constraint minimizes the probability of external entities gaining access to privacy information. It is estimated by:

$$\mathrm{C}^{\mathrm{emb}}(\epsilon_i,\delta_i)=q_{i,j}\times\epsilon_i\sqrt{T\log\left(\frac{1}{\delta_i}\right)}, \tag{8}$$

In Equation (8), the parameter $q_{i,j}$ represents the degree to which a manufacturer i shares information j in the ontology, and T indicates the number of iterations in the learning process. This equation quantifies the privacy loss of class embedding extracted from the ontology and demonstrates how the cumulative privacy loss is calculated when applying multiple DP mechanisms.

- *Sharing of models for attribute learning with privacy expenditure* $\mathrm{C}^{\mathrm{attr}}(\epsilon_i,\delta_i)$: This measure estimates the permissible level of information sharing through attribute learning classifiers trained on local images and the extracted ontology. It effectively controls the potential privacy data leakage by masking model parameters before their distribution through federated learning. It is estimated by:

$$\mathrm{C}^{\mathrm{attr}}(\epsilon_i,\delta_i)=\epsilon_i\sqrt{T\log\left(\frac{1}{\delta_i}\right)}, \tag{9}$$

which calculates the privacy loss in proportion to the square root of the number of iterations T. This formulation is integral to the advanced composition theorem, allowing for a comprehensive assessment of cumulative privacy loss in scenarios involving multiple private mechanisms.

In the DP-attribute learning framework in the context of federated learning, both the embedded attributes of the ontology and the attribute learning models $\boldsymbol{W}_i$ are shared. The proposed constraints offer manufacturers a method to control privacy leaks caused by sharing defect ontology. By setting an upper limit B_i in the privacy budget, manufacturers can regulate how frequently the algorithm explores and shares the ontology and attribute learning models.

The privacy budget B_i is a pivotal metric for navigating the trade-off between data utility and privacy protection. Setting a privacy budget is an iterative methodology that requires continuous

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

re-assessment and re-calibration of B_i to achieve a delicate equilibrium between securing privacy and utilizing data. Central to this process are determining data sensitivity and the needed privacy safeguards, adhering to regulatory frameworks, and making timely adjustments to B_i as data utilization, legal obligations, and stakeholder demands evolve.

The privacy budget spending given the privacy parameters ϵ_i can be illustrated as follows. Consider a federated learning scenario involving two manufacturers, each starting with an initial privacy budget of 1 and other parameters held constant, the impact of varying ϵ_i values on the privacy budget is illustrated through embedding privacy loss per Equation (8). Assuming Manufacturer A has a significantly higher ϵ_i value of 0.7, leading to an embedding privacy loss (C^{emb}) of 0.08, and Manufacturer B has a much lower ϵ_i value of 0.1, with an embedding privacy loss (C^{emb}) of 0.02, the adjustments to their privacy budgets post one federation round are notable. Manufacturer A's budget decreases to 0.92, demonstrating a greater reduction due to the higher ϵ_i, while Manufacturer B's budget is reduced to 0.98, indicating less impact from a smaller ϵ_i.

4.2 DP-Embedding of Ontology. In DP-based class embedding, the process begins by generating vector embeddings for sentences describing defects with each the manufacturer's knowledge base. This step uses the natural language processing model, such as Bidirectional Encoder Representations from Transformers (BERT). Each sentence is denoted as $s_{i,j}$, implying the jth sentence in the dataset of the ith manufacturer. Controlled noise is added to these embeddings $E()$, as shown in Eq. (10).

$$E_{dp}(s_{i,j}) = E(s_{i,j}) + \Delta_{i,j} \tag{10}$$

where $\Delta_{i,j}$ is a random noise drawn from the Laplace distribution with mean 0 and scale parameter $\sigma = \frac{\sqrt{2\log(1/\delta_i)}}{\epsilon_i}$, i.e., $\Delta_{i,j} \sim \text{Lap}(0, \sigma q_{i,j})$, where $q_{i,j}$ is ontology privacy parameters, measuring the depth or branch of ontology to be shared. To generate each embedding $E(s_{i,j})$, the algorithm selects $q_{i,j}$ (Fig. 3). Figure 3 illustrates the process of ontology exploration and DP-embedding for attribute learning. The figure shows two potential paths for ontology exploration (Path A and B). Each path involves hierarchical levels of attributes related to defects. Path A follows ontology exploration with a hierarchical depth of $q_{i,j} = 2$, while Path B follows ontology exploration with a hierarchical depth of $q_{i,j} = 3$. For each path, the algorithm selects $q_{i,j}$ values corresponding to the depth of the ontology branches. These selections determine the amount of controlled noise $\Delta_{i,j}$ added to the class embeddings $E(s_{i,j})$, ensuring differential privacy. The embeddings are then used for attribute learning in defect classification. In other words, when a specific part of hierarchical branches is selected from the ontology, the algorithm responds by scaling the noise to prevent privacy leaks. Deeper branches are rich in information, which costs more in terms of the privacy budget.. The calculated DP-embedding vector $E_{dp}(s_{i,j})$ is then incorporated into the class embedding matrix $\boldsymbol{\phi}_i(y)$. To guarantee (ϵ_i, δ_i)-DP, an advanced composition theorem is implemented (Equation (8)) to quantify and control the embedding privacy loss ($C^{emb}(\epsilon_i, \delta_i)$) within the set overall privacy budget B_i.

The loss incurred in each embedding is subtracted from the privacy budget to calculate the remaining privacy budget. Then, Eq. (11) updates the privacy budget as follows:

$$B_i \leftarrow B_i - C^{emb}(\epsilon_i, \delta_i) \tag{11}$$

If the remaining privacy budget is non-positive, training terminates and discards the last calculated embedding to guarantee differential privacy. Otherwise, the computed embedding $E_{dp}(s_{i,j})$ is used for training the classifier.

4.3 Stage 1 Optimization: DP-Attribute Learning. Once the DP-embedding $E_{dp}(s_{i,j})$ is calculated and stacked into class embedding matrix $\boldsymbol{\phi}_i^{(t)}(y)$, multiple manufacturers participate in the attribute learning process over iterations indexed by (t). Each

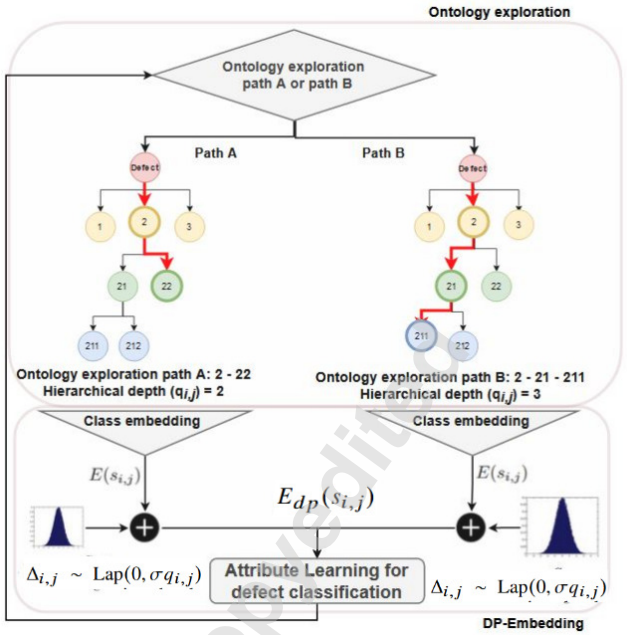

Fig. 3 DP-Embedding for attribute learning

manufacturer S_i has access to its dataset D_i (image features $\boldsymbol{\theta}_i(\mathbf{x})$ and DP attribute embeddings $\boldsymbol{\phi}_i^{(t)}(y)$). Manufacturers train an attribute learning classifier locally to obtain the feature-to-attribute mapping matrix $\mathbf{W}_i^{(t)}$ that minimizes the local loss function. As such, Equation (2) for the attribute learning objective becomes $C_{pi}^{(t)}(\mathbf{x}, y; \mathbf{W}_i^{(t)}) = max(\boldsymbol{\theta}'(\mathbf{x})\mathbf{W}_i^{(t)}\boldsymbol{\phi}_i^{(t)}(y))$. Each manufacturer needs to solve the constrained two-stage optimization problem (6) and (7). Stage 1 learns $\mathbf{W}_i^{(t)}$ given attribute stacking matrix $\boldsymbol{\varphi}_i^{(t)}$ and Stage 2 sequentially searches for ontology to be shared with federated learning by an evolutionary algorithm (EA). This section focuses on the DP formulation of the optimization for stage 1. Its objective function is

$$\min_{\boldsymbol{\varphi}_i} \min_{\mathbf{W}_i|\boldsymbol{\varphi}_i} \frac{1}{K_i} \sum_{i=1}^{K} L_i^{(t)}(y_n, f_i^{(t)}(\mathbf{x}_n; \mathbf{W}_i^{(t)}, \boldsymbol{\varphi}_i^{(t)})) \tag{12}$$

where $L_i^{(t)}$ is the loss function that defines a ranking-based loss function $L_i^{(t)}$ as in Equation (13):

$$L_i^{(t)} = \sum_{y \in Y^{tr}} max\left\{0, \Delta(y_n, y) + C_{p,i}^{(t)}(\mathbf{x}_n, y; \mathbf{W}_i^{(t)}) - C_{p,i}^{(t)}(\mathbf{x}_n, y_n; \mathbf{W}_i^{(t)})\right\} \tag{13}$$

where $\Delta(y_n, y) = 1$ if $y \neq y_n$ and 0 otherwise. This loss function forces the model to produce higher compatibility between the defect image and the true label than between the image and the incorrect labels.

This problem consists of inner and outer optimizations. In the inner optimization, DP is integrated into the solution algorithm for optimization in (12), such as SGD. This step utilizes the Laplace mechanism to add noise to the gradient at each iteration (Fig. 4 upper left panel). Noise $\mathbf{N}$ sampled from a Laplace distribution ($\mathbf{N}_i^{(t)} \sim \text{Laplace}(0, \sigma)$) with scale $\sigma = \frac{\sqrt{2\log(1/\delta_i)}}{\epsilon_i}$ is added to the gradient $\tilde{\nabla}_{\boldsymbol{W}} L_i^{(t)}$ (Eq. (14)).

$$\tilde{\nabla}_{\mathbf{W}} L_i^{(t)} = \nabla_{\mathbf{W}} L_i^{(t)} + \mathbf{N}_i^{(t)} \tag{14}$$

DP-SGD (Eq. (15)) then updates the weights of the model using

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

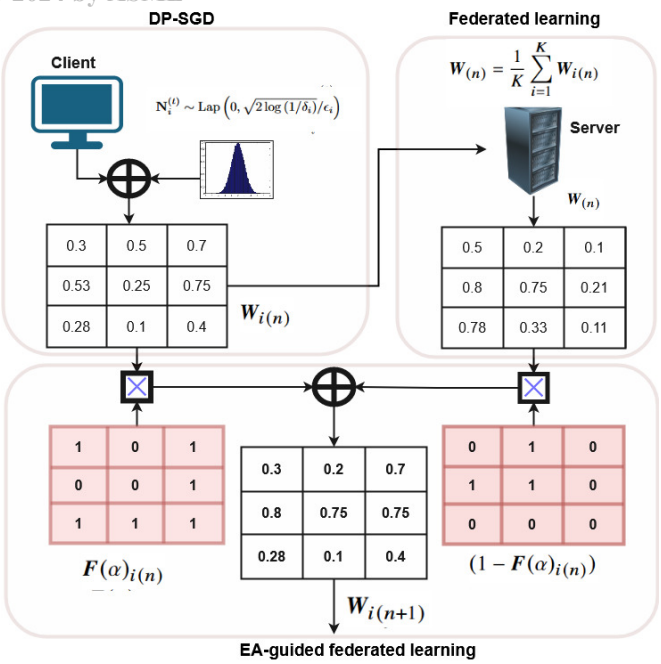

Fig. 4 Federated DP-SGD for attribute learning

the noisy gradient:

$$\mathbf{W}_i^{(t)} \leftarrow \mathbf{W}_i^{(t-1)} - \eta \tilde{\nabla}_{\mathbf{W}} L_i^{(t)} \tag{15}$$

where η is the learning rate, a hyperparameter.

The outer optimization follows our prior research [26], which minimizes the ZSL loss function in (12) and finds the optimal ontology structure $\boldsymbol{\varphi}_i$ through stochastic exploration and exploitation in an evolutionary algorithm. This layer of optimization searches for ontology structure $\boldsymbol{\varphi}_i$, given mapping $\mathbf{W}$ in the compatibility function and privacy parameters (ϵ, δ) which restricts the amount of information to be shared with other manufacturers.

During the testing phase, manufacturer S_i computes classification accuracy $(\alpha_i^{(t)})$ in finding the label k for manufacturing defects. The label is identified as one that maximizes the compatibility between the input features $\boldsymbol{\theta}_i(x_t)$ and the kth class embedding $\boldsymbol{\phi}_i^{(t)}(y_k)$ as formulated in Eq. (16).

$$\hat{k} = argmax\{\boldsymbol{\theta}_i'(x_t)\hat{\mathbf{W}}_i^{(t)}\boldsymbol{\phi}_i^{(t)}(y_k)\} \tag{16}$$

The advanced composition theorem (Eq. (9)) is used to calculate the loss of attribute learning privacy $\mathrm{C}^{\mathrm{attr}}(\epsilon_i, \delta_i)$. Finally, the privacy budget (B_i) is updated (Eq. (17)) to ensure that the total privacy loss stays within the desired bound:

$$B_i \leftarrow B_i - \mathrm{C}^{\mathrm{attr}}(\epsilon_i, \delta_i) \tag{17}$$

If the privacy budget is exhausted (i.e., $B_i \leq 0$), training stops and return the final weight matrix $\mathbf{W}_i^{(t-1)}$.

4.4 Stage 2 Optimization: DP-attribute learning framework under the context of federated learning. This section focuses on the Stage 2 solution algorithm. Considering the combinatorial nature of ontology exploration in this stage, this paper proposes to solve it by integrating the evolutionary algorithm (EA) with federated learning based on manufacturer collaboration. After completing the iterations of attribute learning in Stage 1, the algorithm enters into the $(n)th$ federating round, each manufacturer S_i sends the noise-masked model parameters $\boldsymbol{W}_{i(n)}$ from local clients to the central server. The central server computes the average of the received parameters (Eq. (18)):

$$\boldsymbol{W}_{(n)} = \frac{1}{K}\sum_{i=1}^{K} \boldsymbol{W}_{i(n)} \tag{18}$$

Subsequently, the server sends the updated global parameter $\boldsymbol{W}_{(n)}$ back to each manufacturer.

Each manufacturer needs to decide on whether or not to incorporate the model results from the server at each federating round. The decision can be driven by the learning accuracy α_i of each manufacturer. If the accuracy is insufficient, the manufacturer will leverage the model parameters from the server. Otherwise, the manufacturer can rely on its local model for optimization without sharing their ontology and image data. This decision is captured by a binary federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$, which is affected by accuracy α_i and has the same dimension as the attribute learning model $\boldsymbol{W}_i$. This matrix determines what parameters in the model should be updated by the global model on the server.

An evolutionary strategy is developed to direct the search for federating matrices $\boldsymbol{F}(\alpha)_{i(n)}$. This method leverages a fitness function based on α_i to fine-tune the trade-off between local knowledge and aggregated global information. The fitness function serves as a dynamic guide, iteratively refining the search for optimal solutions by evaluating and minimizing the objective function across successive iterations. Although not optimal in initial iterations, it drives the EA progressively towards better solutions, reducing the objective function over time. The search strategy should balance exploration and exploitation by adjusting the contribution of local and global information within the federated learning framework.

4.4.1 Federating Crossover. The exploration phase of federated learning is dominated by the crossover operation. This paper proposes to govern this process by a federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$ based on the local model accuracy α_i. The federating matrix is defined as follows:

$$\boldsymbol{F}(\alpha)_{i(n)} = \begin{cases} 1, & \text{with probability of the same value as } \alpha_i \\ 0, & \text{with probability } (1-\alpha_i) \end{cases} \tag{19}$$

During crossover, a random subset of genes (parameters) from the local parameter matrix $\boldsymbol{W}_{i(n)}$ is selected, proportional in size to the local accuracy α_i. These genes are then merged with complementary genes from the global parameter matrix $\boldsymbol{W}_{i(n)}$, under the direction of the federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$. This process can be depicted as:

$$\boldsymbol{W}_{i(n+1)} = \text{Fed-Crossover}(\boldsymbol{W}_{i(n)}, \boldsymbol{W}_{(n)}, \boldsymbol{F}(\alpha)_{i(n)}) \tag{20}$$

This crossover operation under the federating context (Fed-Crossover) encourages the exploration of new configurations in the parameter matrix, thereby enhancing the adaptability and potential for improved performance in the learning model.

4.4.2 Federating Mutation. In the exploitation phase, particularly when the local model accuracy α_i is high, the federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$ undergoes local adjustments. This adjustment process originates from the previous iteration of the matrix, $\boldsymbol{F}(\alpha)_{i(n-1)}$. The updated matrix $\boldsymbol{F}(\alpha)_{i(n)}$ is formed through a probabilistic modification based on the current local accuracy α_i:

$$\boldsymbol{F}(\alpha)_{i(n)} = \text{Adjust}(\boldsymbol{F}(\alpha)_{i(n-1)}, \alpha_i) \tag{21}$$

In this adjustment, each entry in $\boldsymbol{F}(\alpha)_{i(n)}$ is changed from the original value with a probability proportional to α_i. This probabilistic approach ensures that the matrix accurately reflects the latest state of local model accuracy. This adjusted matrix then guides the mutation process for the local parameter matrix $\boldsymbol{W}_{i(n)}$. This step involves row swapping in $\boldsymbol{W}_{i(n)}$ to enhance the local model. The mutation operation is represented as follows:

$$\boldsymbol{W}_{i(n+1)} = \text{Fed-Mutation}(\boldsymbol{W}_{i(n)}, \boldsymbol{F}(\alpha)_{i(n)}), \tag{22}$$

where mutation under the federating context (Fed-Mutation) applies specific alterations to $\boldsymbol{W}_{i(n)}$ based on the directives of $\boldsymbol{F}(\alpha)_{i(n)}$. This mutation allows for fine-tuning of the local model in response to its performance.

In both the crossover and mutation phases, the federating matrices $\boldsymbol{F}(\alpha)_{i(n)}$ play a vital role in balancing local and global-scale searches during the learning process. The local parameter update can be expressed as:

$$\boldsymbol{W}_{i(n+1)} = \boldsymbol{F}(\alpha)_{i(n)} \odot \boldsymbol{W}_{i(n)} + (1 - \boldsymbol{F}(\alpha)_{i(n)}) \odot \boldsymbol{W}_{(n)} \tag{23}$$

Algorithm 1 DP-Federated Attribute Learning Algorithm

Initialize the global model parameter vector $\boldsymbol{W}^{(0)}$
for each iteration $t = 1, 2, \ldots T$ **do**
  for each device $S_i \in S$ **do** — Initialize
    for each sentence $s_{i,j}$ in D_i **do**
      Compute the BERT embedding $E(s_{i,j})$
      Perform DP-embedding: $E_{dp}(s_{i,j}) = E(s_{i,j}) + \Delta_{i,j}$

$$\text{where, } \Delta_{i,j} \sim \text{Lap}\left(0, q_{i,j}\sqrt{2\log(1/\delta_i)}/\epsilon_i\right)$$

      Update overall privacy: $B_i \leftarrow B_i - q_{i,j}\epsilon_i\sqrt{T\log(1/\delta_i)}$
    end for
    S_i trains $\mathbf{W}_i^{(t)}$ using dataset D_i to minimizes the objective function: — DP-Attribute Learning

$$\min_{\boldsymbol{\varphi}_i} \min_{\mathbf{W}_i|\boldsymbol{\varphi}_i} \frac{1}{K_i}\sum_{i=1}^{K} L_i^{(t)}(y_n, f_i^{(t)}(\mathbf{x}_n; \mathbf{W}_i^{(t)}, \boldsymbol{\varphi}_i^{(t)}))$$

    DP-attribute learning: $\mathbf{W}_i^{(t)} \leftarrow \mathbf{W}_i^{(t-1)} - \eta\tilde{\nabla}_{\mathbf{W}} L_i^{(t)}$ where,

$$\tilde{\nabla}_{\mathbf{W}} L_i^{(t)} = \nabla \mathbf{W} L_i^{(t)} + \mathbf{N}_i^{(t)} \quad \text{and,} \quad \mathbf{N}_i^{(t)} \sim \text{Lap}\left(0, \sqrt{2\log(1/\delta_i)}/\epsilon_i\right)$$

    Update overall privacy: $B_i \leftarrow B_i - \epsilon_i\sqrt{T\log(1/\delta_i^{all})}$
    S_i Computes accuracy α_i and sends $\boldsymbol{W}_{i(n)}$ to the central server
    Server computes: $\boldsymbol{W}_{(n)} = \frac{1}{K}\sum_{i=1}^{K} \boldsymbol{W}_{i(n)}$ and sends $\boldsymbol{W}_{(n)}$ back — DP-Federated Learning
    if α_i is very low **then**
      Compute the federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$:

$$\boldsymbol{F}(\alpha)_{i(n)} = \begin{cases} 1, & \text{with probability of the same value as } \alpha_i \\ 0, & \text{with probability } (1-\alpha_i) \end{cases}$$

      Do Crossover: $\boldsymbol{W}_{i(n+1)} = \text{Fed-Crossover}(\boldsymbol{W}_{i(n)}, \boldsymbol{W}_{(n)}, \boldsymbol{F}(\alpha)_{i(n)})$
    else
      Compute the adjusted federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$:

$$\boldsymbol{F}(\alpha)_{i(n)} = \text{Adjust}(\boldsymbol{F}(\alpha)_{i(n-1)}, \alpha_i)$$

      Do Mutation: $\boldsymbol{W}_{i(n+1)} = \text{Fed-Mutation}(\boldsymbol{W}_{i(n)}, \boldsymbol{F}(\alpha)_{i(n)})$
    end if
    Update the local parameter matrix $\boldsymbol{W}_{i(n+1)}$:

$$\boldsymbol{W}_{i(n+1)} = \boldsymbol{F}(\alpha)_{i(n)} \odot \boldsymbol{W}_{i(n)} + (1 - \boldsymbol{F}(\alpha)_{i(n)}) \odot \boldsymbol{W}_{(n)}$$

  end for
end for

The operation $\boldsymbol{F}(\alpha)_{i(n)} \odot \boldsymbol{W}_{i(n)}$ multiplies each element of the federating matrix $\boldsymbol{F}(\alpha)_{i(n)}$ with the corresponding element of the local parameter matrix $\boldsymbol{W}_{i(n)}$. Similarly, $(1-\boldsymbol{F}(\alpha)_{i(n)}) \odot \boldsymbol{W}_{(n)}$ involves element-wise multiplication of the global parameter matrix $\boldsymbol{W}_{(n)}$ with the result of 1 minus each element in the federating matrix. This equation encapsulates the essence of the adaptive learning process, highlighting the importance of local model accuracy α_i in guiding the learning direction, whether through crossover or mutation. The entire methodology is summarized in Algorithm 1.

The DP-attribute learning framework under the context of a federated learning algorithm operates under two stopping criteria: (1)*Federating Rounds*: The algorithm is regulated by a predetermined number of federating rounds (N), which dictate the duration of the collaborative learning process, and (2) *Privacy Budget*: The participation of each manufacturer in updating the model parameters is limited by its allocated privacy budget. Once depleted, the manufacturer ceases to contribute new data. All genes generated at each generation are inspected to ensure a feasible solution.

Overall, the proposed DP-attribute learning framework under federated learning provides solutions to joint decision-making problems while balancing accuracy and privacy. Given noise added to mask shared information, decisions involve the selection of the depth of the ontology branch for sharing and whether to integrate the global model shared in the cloud. Furthermore, the framework develops a two-stage solution algorithm. The first stage refines the solutions using SGD for better accuracy, while the second stage employs metaheuristics (EA) to explore the solution space efficiently. This dual-stage optimization effectively balances computational demands with the need for accurate model training.

Remark: Although it is not common in the early stage of developing new manufacturing processes if a larger dataset is available, the proposed algorithm may encounter challenges in the combinatorial search for appropriate mapping $\boldsymbol{W}$ between the images and attributes extracted from the ontology and selection of ontology branches to be shared to the cloud.

5 Case study

This case study considers a scenario where two manufacturers leverage information from each other to improve defect identification accuracies in their direct-ink-writing processes. Each manufacturer possesses defect image data along with the ontology characterizing the defects and attempts to perform zero-shot learning of unseen classes measured in each process. Information sharing can benefit each other; however, manufacturers want to limit information disclosure. This study makes decisions for each manufacturer regarding which parts of the defect ontology and defect images to be shared through attribute learning models. Since existing federated learning and ZSL cannot address the decision-making outlined in Section 3, there is a lack of benchmark methods for comparison.

5.1 Manufacturers data and privacy budget.

5.1.1 Data source and pre-processing. The case study focuses on a printing process for creating a new nanowire-polymer composite structure as photoactive coatings that detect visible light [33]. This research addresses ten defect types captured by microscopic images, including cracks and pores in different morphologies. Figure 5 illustrates examples of these defects.

The dataset includes various cracks and pores, each with a unique shape, texture, or color properties. The dataset is divided into seen and unseen classes for zero-shot learning (ZSL). The ZSL classifier in Figure 5 is trained on 70% (7 seen classes) and tested on 30% (3 unseen classes). Some examples of shared features between seen and unseen classes are Irregular pore-1, which shares the attribute "grey colored surface" with Large pore-2, and "irregularly shaped pores" with Irregular pore-2. Large pore-1 shares the attribute "reddish surface with small red dots" with Tiny crack-1 and "large circular pores" with Large pore-2.

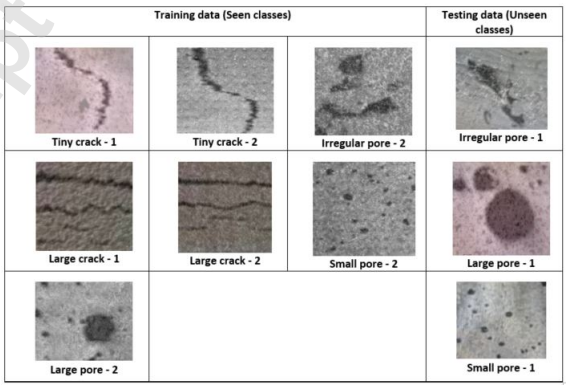

Fig. 5 Examples of training data (seen classes) and testing data (unseen classes) in the dataset

This study addresses the challenge of recognizing and classifying novel defect types of a new manufacturing process without extensive labeled training data. The case study focuses on utilizing ontology sharing among manufacturers to enhance zero-shot learning of printing defects in a direct ink writing process. As this is a new process, the dataset has a sample size of 50. There is a lack of historical samples, and generating microscopy images is time-consuming and expensive. Consequently, this case study targets machine learning in resource-limited settings, with each manufacturer having limited samples. To mitigate the limitations of a small test dataset, we implemented cross-validation by swapping the roles of training and testing data. For example, classes initially used for training as seen classes are subsequently used for testing as unseen classes, and vice versa. This approach effectively increases the testing scenarios. The performance of ontology-based ZSL in improving embeddings to compensate for data shortages with several scenarios has been demonstrated s in our prior work [26]. Additionally, prior research [27] has thoroughly tested larger

Defect	Manufacturer-1 available image samples for training	Manufacturer-2 available image samples for training
Tiny crack-1	1,2,3,4,5	1,2,3,4,5
Tiny crack-2	6,7,8,9,10	6,7,8,9,10
Irregular pore-1	11,12,13,14,15	
Irregular pore-2	16,17,18,19,20	16,17,18,19,20
Large crack-1		21,22,23,24,25
Large crack-2		26,27,28,29,30
Large pore-1	31,32,33,34,35	
Large pore-2		36,37,38,39,40
Small pore-1	41,42,43,44,45	41,42,43,44,45
Small pore-2	46,47,48,49,50	

Fig. 6 Availability of image samples for training provided by Manufacturer 1 and Manufacturer 2. Defects for which manufacturers did not provide morphology data were used as testing data.

testing datasets as long as the class embedding is accurate. This study focuses on collaborative efforts to improve class embedding for manufacturing defects, given data shortages on each manufacturer while ensuring privacy guarantees. This study focuses on collaborative efforts to mitigate data shortages while ensuring privacy guarantees.

Following [26], feature extraction involved obtaining $\boldsymbol{\theta}(\mathbf{x})$ from defect images, where the Img2Vec Python library was employed for image embedding. This method leveraged a ResNet50 model with pre-trained weights sourced from the ImageNet dataset [34]. This study incorporated an ontology exploration strategy and natural language processing to convert the ontology into class embeddings represented as vectors for ZSL. A customized "walk" algorithm facilitated the process of ontology parsing. Furthermore, the "BERT BASE Uncased" variant of the BERT model was applied for converting sentences derived from multiple "walks" into contextualized embedding vectors, denoted as ($\boldsymbol{\phi}$) of size 768.

5.1.2 Manufacturer's data. In this example, both manufacturers provided ontology with ten different defect types and morphology data for seven. Defect images were provided by Manufacturer 1 and Manufacturer 2 for seven types of defects. As shown in Fig. 6, there were differences between the manufacturers in the availability of image samples. Manufacturer-1's image data represented Tiny crack-1, Tiny crack-2, Irregular pore-1, Irregular pore-2, Large pore-1, Small pore-1, and Small pore-2, but did not include image data for Large crack-1, Large crack-2, and Large pore-2. In contrast, Manufacturer-2's image data included Tiny crack-1, Tiny crack-2, Irregular pore-2, Large crack-1, Large crack-2, Large pore-2, and Small pore-1 but did not include images for Irregular pore-1, Large pore-1, and Small pore-2.

The ontology available to Manufacturer-1 and Manufacturer-2 is illustrated schematically in Fig. 7. This ontology exhibits a combination of complementary and overlap in certain attributes, while instances of entirely missing data in other attributes. The ontology of Manufacturer-1 included the morphology of Tiny crack-1, Tiny crack-2, Irregular pore-1, Irregular pore-2, Large pore-1, Small pore-1, and Small pore-2. However, this ontology does not include information about the Large crack-1, Large crack-2, and Large pore-2 morphology. In contrast, Manufacturer-2's ontology includes morphology for Tiny crack-1, Tiny crack-2, Irregular pore-2, Large crack-1, Large crack-2, Large pore-2, and Small pore-1. It lacks morphology for Irregular pore-1, Large pore-1, and Small pore-2. A summary of ontology information regarding morphology, materials, and causes for each defect in both manufacturers is presented in Fig. 7.

5.1.3 Privacy budget. This study focuses on evaluating the impact of the privacy budget on the accuracy of the model. It involves training the proposed algorithm with various privacy parameters

Table 1 Ranges and increments of the factors evaluated in the proposed algorithm.

Factor	Range of Values	Increment
Federating Round (N)	5 – 30	5
Upper Bound Budget	10^3 – 10^6	10^2
Epsilon	0.1–10	×100

for each manufacturer. The accuracy was evaluated at various levels of the privacy budget to assess the privacy-accuracy trade-off. The objective is to determine an appropriate privacy budget by fine-tuning the parameters. Table 1 shows the range of privacy parameters in the case study. We conducted experiments with different combinations of federating rounds N, upper bound budget B_i, and ϵ_i for manufacturer i=1 or 2. Forty-two (42) numerical experiments on the proposed method were conducted, each with a different combination of the above-mentioned factors. Each experiment was repeated five times.

5.2 Results and discussion.

5.2.1 Results of ontology sharing in DP-attribute learning framework under the context of federated learning. This section discusses how each manufacturer benefits from ontology sharing based on the proposed DP-attribute learning framework under federated learning. Each manufacturer may miss some data in the ontology, as shown in Fig. 7, but they can leverage the complementary information from another manufacturer to improve the learning. The ontology of manufacturing defects always exhibits a root-branches-subbranches structure, with branches in each class containing information about materials, causes, or morphology. However, the composition of these branches can differ between manufacturers, such as the attribute information in each branch and the depth of the branch. This variability in the ontology composition can impact the performance of the proposed algorithm. In this study, changing the privacy budget can affect the depth of each ontology branch to be shared, resulting in different ZSL performances.

Figure 8 (dark grey cells) illustrates the actual ontology data shared during training, in which manufacturers complement each other to supplement the missing ontology data of their respective unseen classes. For instance, considering Manufacturer-1, the unseen class Large crack-1 lacked morphology information in the ontology, images, and shared model trained on "cause." Through DP federated training, Manufacturer-2 shared a model trained on images and morphology of Large crack-1 to supplement information for Manufacturer-1. Similarly, for identifying Large crack-2, Manufacturer-1 selected ontology containing "material" and "cause" data, supplemented by morphology information in ontology and images of Large crack-1 from Manufacturer 2. Another defect, Large pore-2, missed morphology information in the ontology and images in Manufacturer-1, which was complemented by the data from Manufacturer-2. Similarly, the DP attribute learning framework in federated learning was also beneficial for Manufacturer-2, as missing morphology information on three types of defects was supplemented from Manufacturer-1. As illustrated in Figure 8, in Manufacturer-2's unseen classes, image data and morphology were absent for "Irregular pore-1", "Large pore-1", and "Small pore-2". Despite this absence, DP federated training facilitated the integration of these missing attributes from the partner manufacturer, effectively supplementing information on the missing data.

Although both manufacturers lacked image and morphology data for their respective unseen classes, the proposed algorithm demonstrated the ability to correctly classify these unseen classes for both manufacturers through collaboration. Given the available ontology structure in Fig. 7 and the optimal ontology structure

Defect	Manufacturer-1 ontology data			Manufacturer-2 ontology data		
Tiny crack-1	Morphology		Cause	Morphology	Material	
Tiny crack-2	Morphology	Cause	Material	Morphology	Material	Cause
Irregular pore-1	Morphology		Cause		Material	Cause
Irregular pore-2	Morphology			Morphology		Cause
Large crack-1		Cause		Morphology		Cause
Large crack-2		Material	Cause	Morphology		
Large pore-1	Morphology	Material	Cause		Material	Cause
Large pore-2		Material	Cause	Morphology		Material
Small pore-1	Morphology			Morphology	Material	Cause
Small pore-2	Morphology	Material	Cause		Material	Cause

Fig. 7 Available ontology for Manufacturer 1 and Manufacturer 2

Defect	Manufacturer-1 ontology data			Manufacturer-2 ontology data		
Tiny crack-1	Morphology		Cause	Morphology	Material	
Tiny crack-2	Morphology	Cause	Material	Morphology	Material	Cause
Irregular pore-1	Morphology		Cause		Material	Cause
Irregular pore-2	Morphology			Morphology		Cause
Large crack-1		Cause		Morphology		Cause
Large crack-2		Material	Cause	Morphology		
Large pore-1	Morphology	Material	Cause		Material	Cause
Large pore-2		Material	Cause	Morphology		Material
Small pore-1	Morphology			Morphology	Material	Cause
Small pore-2	Morphology	Material	Cause		Material	Cause

Fig. 8 Selected optimal ontology (dark grey cells) for Manufacturer-1 and Manufacturer-2

selected in Fig. 8, Manufacturer-1 achieved 100% accuracy in correctly classifying all samples in a three unseen class scenario (Fig. 9). This result demonstrates how different ontology structures can be harmonized to improve the effectiveness of the proposed algorithm in real-world manufacturing scenarios. Given the actual ontology shared, Manufacturer-1 and 2 spent a similar amount of privacy budget, which regulates the frequency of its defect ontology and images shared. The results underscore the potential of the proposed method to effectively leverage shared information from both manufacturers, even in scenarios of missing or fragmented data.

This study also computed additional performance such as Recall, precision, and F1-Score for both manufacturers. The metrics in Table 2 provide a detailed comparison of the performance of both manufacturers. Manufacturer 1 shows perfect performance across all tests with Precision, Recall, and F1-Score consistently at 1.0, indicating an excellent classification. Manufacturer 2, while demonstrating strong performance, shows variability, particularly in Test-4 and Test-5. In Test-4, Manufacturer 2 has a Precision of 0.83 but maintains a Recall of 1.0, leading to an F1-Score of 0.91. Test-5 reveals a trade-off, with a Precision of 1.0 but a lower Recall of 0.8, resulting in an F1-Score of 0.89. These variations highlight the impact of imbalanced datasets and the effectiveness of the federated learning approach in improving classification performance despite these challenges. The consistent performance of Manufacturer 1 suggests that the ontology-based ZSL method effectively captures the necessary semantic information, while the slight variations for Manufacturer 2 indicate areas for further refinement and adjustment in handling diverse datasets.

To illustrate the performance of the proposed method on seen classes, as an example, figure 10 presents the confusion matrix

Table 2 Precision, Recall, and F1-Score for Manufacturer 1 and 2

Manufacturer	Sample	Precision	Recall	F1-Score
Manufacturer 1	Test-1	1.0	1.0	1.0
Manufacturer 1	Test-2	1.0	1.0	1.0
Manufacturer 1	Test-3	1.0	1.0	1.0
Manufacturer 2	Test-4	0.83	1.0	0.91
Manufacturer 2	Test-5	1.0	0.8	0.89
Manufacturer 2	Test-6	1.0	1.0	1.0

for Manufacturer 1. These experiments were based on separate test results, which expanded the number of testing classes to ten, and it was conducted based on training with three training samples and two testing samples for each class; the testing data contained a mixture of seen and unseen classes. Specifically, Test-5, Test-6, and Test-8 were unseen classes, while the rest were seen classes. Manufacturer 1 achieved a test accuracy of 0.55 overall, with an accuracy of 0.70 for seen classes. Testing a mixture of seen and unseen classes is particularly challenging because the model must recognize the classes it has been trained on and generalize to identify and classify entirely new defect types. This complexity can lead to lower accuracy for unseen classes as the model has no prior exposure to these defects during training but is still much better than random guesses. The confusion matrix in Figure 10 further illustrates the model's performance in these test scenarios.

Remark: This study only considers two manufacturers but the conclusions can apply to more than two. If manufacturers have ontologies that complement each other, the results will improve regardless of the number of manufacturers involved. The conclusions are similar to those of the two manufacturers.

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

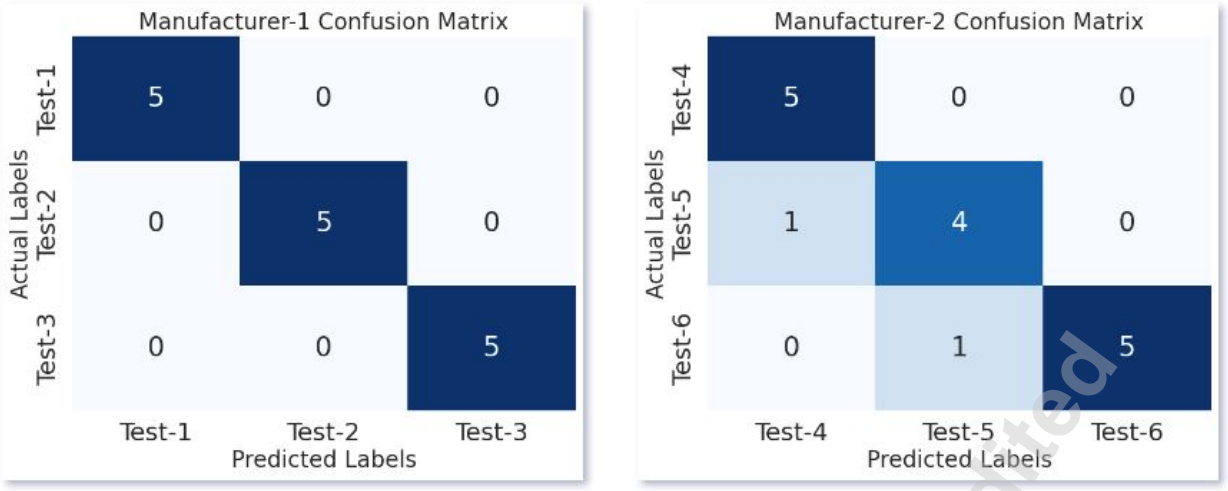

Fig. 9 The confusion matrix for Manufacturer 1 and Manufacturer 2 based on the ontology structure of Fig. 8

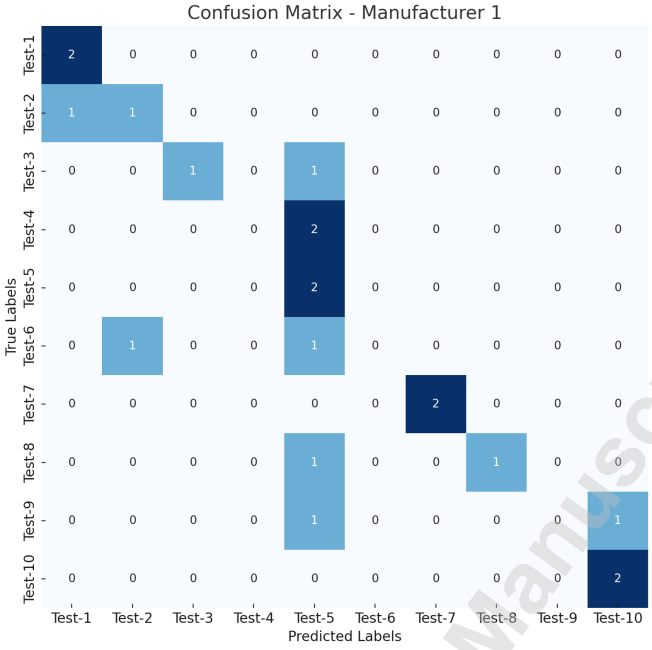

Fig. 10 The confusion matrix for Manufacturer 1 based on the expanded test results with ten testing classes, include a mixture of seen and unseen classes. Test-5, Test-6, and Test-8 are unseen classes

5.2.2 Learning performance for classification with different numbers of unseen classes. This section tests the performance of the proposed algorithm dealing with different complexities of zero-shot classification problems. The complexity is evaluated by the number of unseen classes, including two, three, four, and five unseen classes, from a pool of ten total classes. There are five samples in each class. Each experiment was run five times.

Figure 11 illustrates the box plots of accuracy for Manufacturer-1 and Manufacturer-2 across various unseen class scenarios. Notably, Manufacturer-1 demonstrated an accuracy of 100% during the experiment with the two unseen classes. As the number of unseen classes increased from two to five, a gradual decline in accuracy was observed. In the scenario involving five unseen classes out of ten, the accuracy lowers to about 43%. This result is superior to random coin toss classification, underlining the framework's efficacy. Manufacturer-2's performance showed a similar pattern. For two unseen classes, the accuracy was 100%; for three unseen classes, the median accuracy was around 80%; for four unseen classes, it was about 60%; and for five unseen classes, it was about 40%.

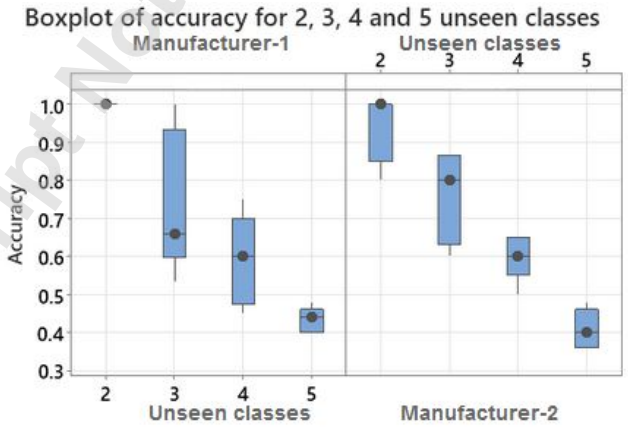

Fig. 11 Zero-shot defect classification accuracy

5.2.3 Privacy Expenditure in Zero-Shot Learning. This section discusses the privacy costs incurred by Manufacturer-1 and Manufacturer-2. Figure 12 uses a box plot to illustrate the relationship between privacy spending and the number of unseen classes in zero-shot learning scenarios. This graphical representation offers insights into the privacy spent under scenarios containing two, three, four, and five unseen classes.

The results show a pattern that reducing the number of unseen classes is associated with decreased privacy costs. For Manufacturer-1, as the number of unseen classes rises from two to five, the overall privacy loss significantly decreases, with the privacy cost reduction observed at approximately a 25% decrease when moving to five unseen classes from two. Similarly, Manufacturer-2's overall privacy expenditure follows this trajectory, where the transition from scenarios with two unseen classes to those with five unseen classes results in a privacy loss reduction of close to 25%. The overall privacy loss for both manufacturers decreases as the number of unseen classes increases. This trend is consistent with the notion that less information sharing results from having many unseen classes since not much information

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

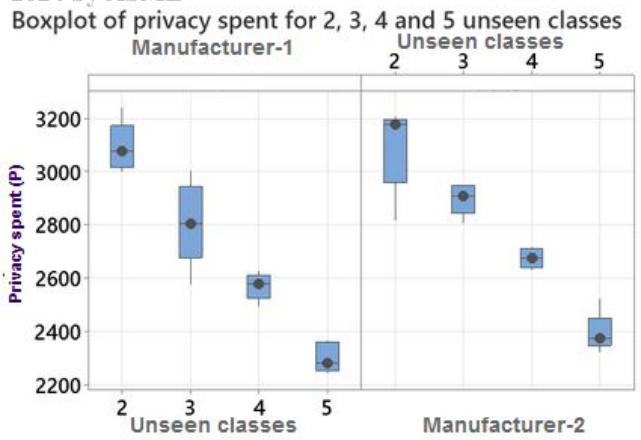

Fig. 12 Privacy expenditure and the number of unseen classes in zero-shot learning

is shared about unseen classes, which minimizes information loss. In other words, more morphology data is missing in the ontology if there are many unseen classes.

5.2.4 The trade-off between privacy budget and accuracy. This section presents the results of experiments to evaluate the impact of three factors on the privacy and accuracy of the proposed algorithm. The factors evaluated were federating round, upper bound budget, and epsilon. The experiment involved two manufacturers, and the accuracy was recorded for each manufacturer and the total amount of privacy budget spent. The number of federating rounds was varied from 5 to 30 in increments of 5 to study the effect of iterative learning on model accuracy and privacy. The upper bound budget for privacy was set between 10^3 and 10^6, with increments of 10^2, controlling the total allowable privacy expenditure.

Impacts on accuracy: The experiments were designed to evaluate the impact of these parameters on the model's accuracy (Table 3). Federating Rounds (N) indicate the number of iterations the federated learning process undergoes. The values tested were 5, 10, 15, 20, 25, and 30 rounds. Epsilon (ϵ) represents the privacy budget in the differential privacy mechanism, controlling the amount of noise added to the data. Two epsilon values were tested: 0.1 and 10.

(1) Manufacturer 1: With an epsilon value of 0.1, the accuracy improves steadily with increasing federating rounds, starting from 0.5 at N=5 and reaching 0.68 at N=30. Higher initial accuracy is observed for an epsilon value of 10, starting at 0.65 for N=5 and achieving 0.75 by N=30, indicating better model performance with decreased privacy restrictions.
(2) Manufacturer 2: For an epsilon value of 0.1, similar to Manufacturer 1, accuracy increases from 0.5 at N=5 to 0.7 at N=30, showing a positive trend with more federating rounds. For an epsilon value of 10, the accuracy starts at 0.62 for N=5 and reaches 0.73 at N=30, indicating an improvement, although slightly less variation compared to Manufacturer 1.

These results highlight that both manufacturers benefit from increased federating rounds and higher epsilon values, which improve model performance and accuracy. The trends are consistent across both manufacturers, suggesting robustness and reliability in the proposed method.

Impacts on privacy spent ($P(\epsilon_i, N)$): The following analysis explores how epsilon affects overall privacy expenditure $P(\epsilon_i, N)$ affected by federating rounds and noises controlled by ϵ_i. Notably, the epsilon choice substantially impacts privacy spending. For instance, when $\epsilon = 0.1$, privacy spending is considerably lower compared to $\epsilon = 10$. Figures 13 and 14 illustrated the median of privacy spent against N and upper bound budget B_i for Manufacturer-1 and Manufacturer-2. When $\epsilon = 0.1$, the observations include

(1) Effect of Federating Rounds N: Generally, as the number of federating rounds increases from $N = 5$ to $N = 30$, privacy spending increases approximately 2.5-fold (i.e., more chance of exposing the data and ontology), underlining growing privacy concerns as federating rounds increase.
(2) Effect of upper bound budget limit B_i: For a given federating round, when ϵ=0.1, the upper bound budgets do not impact the overall privacy expenditure because it is considerably lower than the set upper bound limit. As a result, all upper-bound limits lead to the same privacy spent for each federating round.

When $\epsilon = 10$, the observations are:

(1) Effect of Federating Rounds N: For high upper bound limits (10^4 and 10^6), the privacy spent increases as the number of federating rounds increases ($N = 5$ to $N = 30$). For Manufacturer 1, privacy spending nearly triples when N increases from 5 to 30 at an upper budget limit of 10^4, indicating a vast privacy loss increase as federating rounds increase.
(2) Effect of upper bound budget limit B_i: For relatively lower privacy budget limit of 10^3, the privacy spent is reduced accordingly. A small upper bound privacy limit effectively restricted privacy spending despite increasing federating rounds.

Cost-effective data sharing: Numerical results from optimization (Eq. (6) - Eq. (7)) sheds light on the accuracy achieved per unit privacy cost spent by the proposed algorithm. This section discusses the optimal trade-off between privacy and accuracy in a federated learning scenario by tuning the privacy parameter (ϵ) and the number of federating rounds (N). The optimization problem is stated as:

$$\min_{\epsilon_i, N} \left\{ \frac{P(\epsilon_i, N)}{A} \right\} \tag{24}$$

Subject to $0.1 \leq \epsilon \leq 10$ (Privacy Constraint)

$0 \leq A \leq 1$ (Accuracy Constraint)

$N \in \{5, 10, 15, 20, 25, 30\}$ (Federating Constraint)

The results of this optimization suggest that the most cost-effective way of sharing for Manufacturer-1 is 30 federating rounds with a privacy parameter ϵ_1 of 0.1, achieving an accuracy of 0.68.

6 Conclusions

For manufacturing quality control, data sharing among multiple manufacturers has emerged as a promising solution to scarcity in labeled data. Knowledge transfer and sharing have emerged as solutions to small-data challenges in quality control, enhancing machine learning with limited data. However, this approach raises significant privacy concerns. Current zero-shot learning and federated learning methods do not adequately address the complexities of representing, selecting, masking, and quantifying the privacy loss of shared data. This study introduces a differential privacy (DP)-enhanced federated attribute learning framework, guided by a defect ontology, to preserve privacy when exchanging data to identify manufacturing defects amidst limited measurement data. The defect ontology based on multi-level attributes to characterize manufacturing defects offers a structured approach to facilitate data sharing. Federated attribute learning enables the zero-shot detection of defects by collectively refining local attribute models, thereby circumventing the need to share original data directly. Differential privacy is integrated into this federated learning framework, safeguarding individual data during sharing processes and providing a quantifiable measure to assess privacy breaches.

Table 3 Comparison of Accuracy Data for Manufacturer 1 and Manufacturer 2 at Different Federating Rounds and Epsilon Values

Fed. Rnds (N)	Manufacturer 1 ($\epsilon = 0.1$)	Manufacturer 1 ($\epsilon = 10$)	Manufacturer 2 ($\epsilon = 0.1$)	Manufacturer 2 ($\epsilon = 10$)
5	0.5	0.65	0.5	0.62
10	0.55	0.68	0.55	0.68
15	0.6	0.7	0.6	0.65
20	0.65	0.7	0.63	0.7
25	0.58	0.72	0.65	0.72
30	0.68	0.75	0.7	0.73

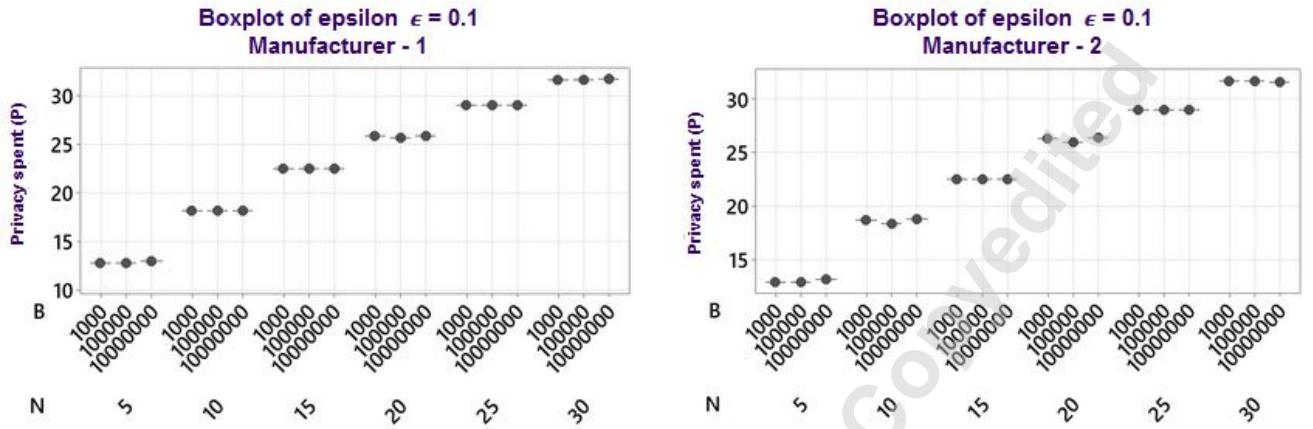

Fig. 13 The median plot of privacy spent against the number of federating rounds *N* and upper bound budget for Manufacturer-1 and Manufacturer-2. The privacy spent generally increases as the number of federating rounds increases (*N* = 5 to *N* = 30). Within each federating round, epsilon 0.1 yields similar privacy spend for all upper-bound budget limits.

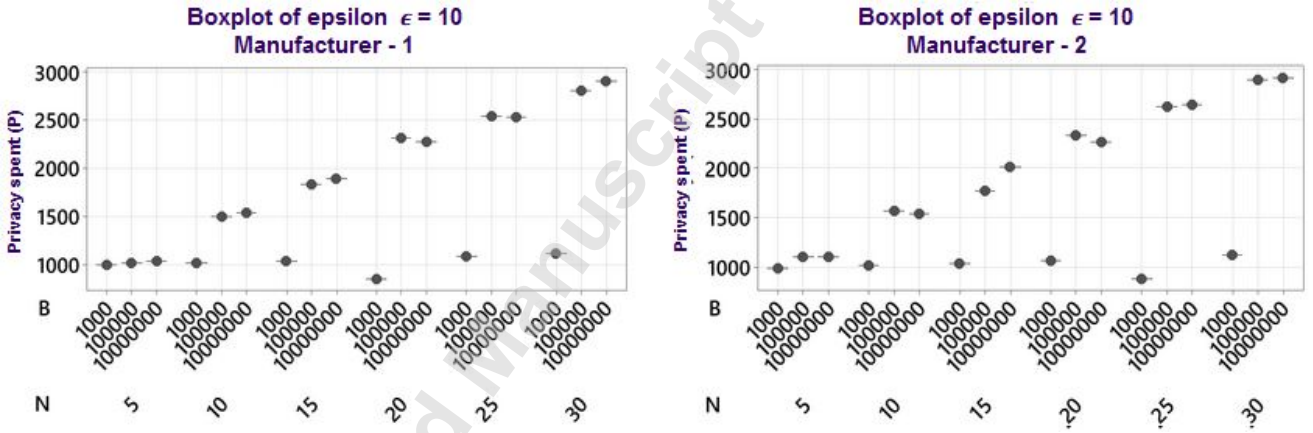

Fig. 14 The median of privacy spent against the number of federating rounds *N* and upper bound budget for Manufacturer 1 and Manufacturer 2. For high upper bound limits, the privacy spent increases as the number of federating rounds increases. On the other hand, the privacy spent is limited at a specified level for a very low privacy budget limit.

Given noises added to conceal shared data, the paper formulates a joint optimization problem to refine data exchange strategies, taking into account (1) selection of ontology and image data for sharing, (2) collaboration through federated learning, and (3) zero-shot classification of defects. To reduce computation, a two-stage solution algorithm is proposed: a zero-shot classifier is trained using stochastic gradient descent in Stage 1, given certain shared ontology/data. Strategies for federated sharing of ontology/data are optimized using an evolutionary algorithm in Stage 2. Two stages iterate till stopping criteria are met. This framework strikes a balance between the enhancement of shared data utility and the management of differential privacy.

Case studies demonstrated the effectiveness of the proposed algorithm in discerning unseen defect classes while preserving privacy. The results show that although each manufacturer may miss some data in the ontology, they can leverage complementary information from other manufacturers to improve the defect identification accuracy. The study highlights the importance of shared attributes in boosting ZSL performance. The study also evaluates the performance of the proposed algorithm in tackling different complexities of zero-shot classification problems. As the number of unseen classes increases, the classification accuracy gradually declines, but the privacy expenditure decreases.

The study also discusses the trade-off between privacy and accuracy. Experimental results reveal that increasing the number of federating rounds boosts accuracy for both participating manufac-

turers. However, opting for a larger privacy parameter ϵ improves accuracy at the expense of increased privacy risk. Furthermore, increasing the number of federating rounds increases privacy costs for both manufacturers, particularly with higher values of ϵ. This observation underscores the privacy sensitivity to the choice of ϵ. Finally, this paper demonstrates that this framework can help estimate the most cost-effective data sharing with the best defect identification accuracy achieved per unit privacy budget spent. In the long run, this research can enable essential data sharing based on text and image data from the literature for zero-shot or few-shot identification of printing defects, given very limited measurements from real processes.

Future research will address the following limitations of this work, including:

- Ontology Based on Text Data Only: The proposed approach utilized the text-based ontology for defect classification as presented in our prior work [26]. This type of input limits the scope of available data for ontology generation. Extending the ontology to include image and sensor data would greatly expand the dataset, improving the comprehensiveness of the defect detection models.
- Qualitative Nature of Output: The output of the proposed method is primarily qualitative, focusing on the classification and identification of defects. Integrating quantitative measures and performance metrics could provide a more detailed and actionable insight into the manufacturing processes. Future research should incorporate quantitative analysis to complement the qualitative findings.

7 Acknowledgement

This material is based upon work supported by the National Science Foundation under award number CMMI-1901109 and the Air Force Office of Scientific Research under award number FA9550-23-1-0739. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation and the United States Air Force.

References

[1] Socher, R., Ganjoo, M., Manning, C. D., and Ng, A., 2013, "Zero-shot learning through cross-modal transfer," Advances in neural information processing systems, **26**.

[2] Elhoseiny, M., Saleh, B., and Elgammal, A., 2013, "Write a classifier: Zero-shot learning using purely textual descriptions," *Proceedings of the IEEE International Conference on Computer Vision*, pp. 2584–2591.

[3] McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A., 2017, "Communication-efficient learning of deep networks from decentralized data," *Artificial intelligence and statistics*, PMLR, pp. 1273–1282.

[4] Mohammad, U. and Sorour, S., 2019, "Adaptive task allocation for asynchronous federated mobile edge learning," arXiv preprint arXiv:1905.01656.

[5] Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., and Smith, V., 2020, "Federated optimization in heterogeneous networks," Proceedings of Machine learning and systems, **2**, pp. 429–450.

[6] Fallah, A., Mokhtari, A., and Ozdaglar, A., 2020, "Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach," Advances in Neural Information Processing Systems, **33**, pp. 3557–3568.

[7] Li, T., Sanjabi, M., Beirami, A., and Smith, V., 2019, "Fair resource allocation in federated learning," arXiv preprint arXiv:1905.10497.

[8] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., et al., 2021, "Advances and open problems in federated learning," Foundations and trends® in machine learning, **14**(1–2), pp. 1–210.

[9] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., and Zhang, L., 2016, "Deep learning with differential privacy," *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 308–318.

[10] Geyer, R. C., Klein, T., and Nabi, M., 2017, "Differentially private federated learning: A client level perspective," arXiv preprint arXiv:1712.07557.

[11] Wang, S., Tuor, T., Salonidis, T., Leung, K. K., Makaya, C., He, T., and Chan, K., 2019, "Adaptive federated learning in resource constrained edge computing systems," IEEE journal on selected areas in communications, **37**(6), pp. 1205–1221.

[12] Wang, Z., Song, M., Zhang, Z., Song, Y., Wang, Q., and Qi, H., 2019, "Beyond inferring class representatives: User-level privacy leakage from federated learning," *IEEE INFOCOM 2019-IEEE conference on computer communications*, IEEE, pp. 2512–2520.

[13] Dwork, C., Roth, A., et al., 2014, "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, **9**(3–4), pp. 211–407.

[14] Wei, K., Li, J., Ding, M., Ma, C., Yang, H. H., Farokhi, F., Jin, S., Quek, T. Q., and Poor, H. V., 2020, "Federated learning with differential privacy: Algorithms and performance analysis," IEEE Transactions on Information Forensics and Security, **15**, pp. 3454–3469.

[15] Dankar, F. K. and El Emam, K., 2013, "Practicing differential privacy in health care: A review." Trans. Data Priv., **6**(1), pp. 35–67.

[16] Canonne, C. L., Kamath, G., and Steinke, T., 2020, "The discrete gaussian for differential privacy," Advances in Neural Information Processing Systems, **33**, pp. 15676–15688.

[17] Ma, C., Li, J., Ding, M., Yang, H. H., Shu, F., Quek, T. Q., and Poor, H. V., 2020, "On safeguarding privacy and security in the framework of federated learning," IEEE network, **34**(4), pp. 242–248.

[18] Dwork, C., 2011, "A firm foundation for private data analysis," Communications of the ACM, **54**(1), pp. 86–95.

[19] Dwork, C., Rothblum, G. N., and Vadhan, S., 2010, "Boosting and differential privacy," *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, IEEE, pp. 51–60.

[20] Kairouz, P., Oh, S., and Viswanath, P., 2015, "The composition theorem for differential privacy," *International conference on machine learning*, PMLR, pp. 1376–1385.

[21] Lyu, X., 2022, "Composition theorems for interactive differential privacy," Advances in Neural Information Processing Systems, **35**, pp. 9700–9712.

[22] Yue, X. and Kontar, R., 2024, "Federated Gaussian Process: Convergence, Automatic Personalization and Multi-fidelity Modeling," IEEE Transactions on Pattern Analysis and Machine Intelligence.

[23] Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., and Parker, R., 2017, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects," Journal of Manufacturing Systems, **44**, pp. 154–164.

[24] Shi, Z., Oskolkov, B., Tian, W., Kan, C., and Liu, C., 2024, "Sensor Data Protection through Integration of Blockchain and Camouflaged Encryption in Cyber-physical Manufacturing Systems," Journal of Computing and Information Science in Engineering, **24**(7).

[25] Shi, Z., Kan, C., Tian, W., and Liu, C., 2021, "A Blockchain-based G-code protection approach for cyber-physical security in additive manufacturing," Journal of Computing and Information Science in Engineering, **21**(4), p. 041007.

[26] Yhdego, T. O., Wang, H., Yu, Z., and Chi, H., 2023, "Ontology-guided attribute learning to accelerate certification for developing new printing processes," IISE Transactions, pp. 1–14.

[27] Xian, Y., Schiele, B., and Akata, Z., 2017, "Zero-shot learning-the good, the bad and the ugly," *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 4582–4591.

[28] Halevi, S., 2006, *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006: Proceedings*, Vol. 3876, Springer Science & Business Media.

[29] Dwork, C., McSherry, F., Nissim, K., and Smith, A., 2006, "Calibrating noise to sensitivity in private data analysis," *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*, Springer, pp. 265–284.

[30] Mironov, I., 2017, "Rényi differential privacy," *2017 IEEE 30th computer security foundations symposium (CSF)*, IEEE, pp. 263–275.

[31] Balle, B. and Wang, Y.-X., 2018, "Improving the gaussian mechanism for differential privacy: Analytical calibration and optimal denoising," *International Conference on Machine Learning*, PMLR, pp. 394–403.

[32] Papernot, N. and McDaniel, P., 2018, "Deep k-nearest neighbors: Towards confident, interpretable and robust deep learning," arXiv preprint arXiv:1803.04765.

[33] Shan, X., Mao, P., Li, H., Geske, T., Bahadur, D., Xin, Y., Ramakrishnan, S., and Yu, Z., 2019, "3D-Printed Photoactive Semiconducting Nanowire–Polymer Composites for Light Sensors," ACS Applied Nano Materials, **3**(2), pp. 969–976.

[34] Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., and Fei-Fei, L., 2009, "Imagenet: A large-scale hierarchical image database," *2009 IEEE conference on computer vision and pattern recognition*, Ieee, pp. 248–255.

Journal of Computing and Information Science in Engineering. Received February 25, 2024;
Accepted manuscript posted October 26, 2024. doi:10.1115/1.4067086

List of Figures

List of Tables