Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 217 (2023) 423–435

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Industry 4.0 and Smart Manufacturing

Multi-level Federated Learning for Industry 4.0 - A Crowdsourcing Approach

Ihsan Ullah[a,*], Umair Ul Hassan[b], Muhammad Intizar Ali[c]

[a] *School of Computer Science, University of Galway, Galway, Ireland*
[b] *School of Business, National University of Ireland Maynooth, Maynooth, Ireland*
[c] *School of Electronic & Computer Engineering, Dublin City University, Dublin, Ireland*

Abstract

Federated learning is one of the emerging areas of research in computer science. It has shown great potential in some application areas and we are witnessing evidence of new approaches where millions or even billions of IoT devices can contribute collectively to achieve a common goal of machine learning through federation. However, existing approaches are primarily suitable for single-task learning with a single objective in a single task owner where it is assumed that the majority of devices contributing to federated learning have a similar design or device type and restrictions. We argue that the true potential of federated learning can only be realised if we have a dynamic and open ecosystem where devices, industrial units, machine manufacturers, non-governmental agencies, and governmental entities can contribute toward learning for multiple tasks and objectives in a crowdsourced manner. In this article, we propose a multi-level framework that shows how federated learning, IoT, and crowdsourcing can come hand-in-hand with each other to make a robust ecosystem of multi-level federated learning for Industry 4.0. This helps build future intelligent applications for Industry 4.0 such as predictive maintenance and fault detection for systems in smart manufacturing units. In addition, we also highlight several use-cases of multi-level federated learning where this approach can be implemented in Industry 4.0. Moreover, if the approach is implemented successfully, besides enhancement in performance it will also help towards a greater common goal e.g. UN Sustainable Goal No 13 i.e. reduction in carbon footprint.

Keywords: Federated Learning, Industry 4.0, Smart Manufacturing, Predictive Maintanance, Crowdsourcing, IoT ;

1. Introduction

Industry 4.0, including Smart Manufacturing, is commonly referred to as the next industrial revolution. It is rapidly changing processes and business models across various sectors, and it expends the use of modern technologies to truly realise smart industrial systems. Big data analytics, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), and edge computing (EC) are among the core enabling technologies of Industry 4.0. The majority of the Industry 4.0 use cases implement a data processing pipeline where IoT is used for data collection in real-time,

* Corresponding author.
E-mail address: ihsan.ullah@universityofgalway.ie **All authors contributed equally.

1877-0509
10.1016/j.procs.2022.12.238

big data and cloud technologies are used to store and analyse data, and machine learning is used to train models to incorporate intelligent services. Predictive maintenance is one of the commonly used use cases for Industry 4.0. However, most of the modern AI or ML models require large amounts of data for improved accuracy which is a significant barrier in industrial contexts. Often companies and manufacturers are concerned about sharing data which limits its utility to only internal purposes thus resulting in data silos. Furthermore, data collected from a single context is not necessarily a true representative of global contexts and AI models trained on local data are not capable of handling unknown scenarios from other contexts.

Federated learning (FL) is one of the modern ML techniques designed to train distributed models over a large number of participators, i.e., data silos, providing data for training without a need for data leaving the owner premises. FL can be a key technique in facilitating open AI models that are trained over a large number of devices and data located at various geographical locations. In some of the scenarios, a crowdsourcing-based approach was followed where each participant voluntarily provides data sometimes in return for incentives. Predictive maintenance is a common use-case of Industry 4.0 that helps industries and smart manufacturers to predict in advance possible maintenance needs of a machine which in turn leads to reduction of financial costs and better reputation, as well as in some cases fatalities. As an example, consider a predictive maintenance system for a certain type of machine (e.g. robotic arm) deployed in many manufacturing production lines. The device manufacturer or industry owner wishes to train an AI model for predictive maintenance which can be used for the maintenance of their machine. If the model is trained in a single factory (with specific humidity level, vibrations, temperature (internal in machine and external to the machine), etc.), using data collected from a single machine for the same task will very often fail whenever it receives unseen data from a situation which was not used during the training. However, if a model is trained on data from multiple machines (from the same or different manufacturer) in different industries in different localities, there is a strong likelihood of training a more powerful predictive model. However, in the majority of the cases industries do not share data for various privacy reasons e.g. IP leakage, competition, and insurance claims. Therefore, if such a mechanism or agreement is done that preserves the privacy of the contributors' data, then it can help all concerned parties e.g., smart manufacturers, machine manufacturers, governing units, and policymakers.

In this paper, we propose a novel multi-leveled crowdsource federated learning framework which combines AI, IoT, and crowdsourcing techniques to design future generations of AI models for systems in Industry 4.0 which result in three aggregated models named local, global, and supermodel. At each level, different types of models can be trained using different types of incentives provided through a crowdsourced model that will result in an enhanced model for all. Following are the key contributions of the paper:

- Proposing multi-level federated learning (MFL) architecture for industrial federated learning based on a crowdsourcing approach.
- Highlighting how incentives at various levels can motivate industries to volunteer for collecting data and allowing models to train over it.
- Highlighting use cases that can help future researchers, industrialists, and governing authorities to implement crowdsourced federated learning in a cooperative approach for the betterment of society e.g. UN Sustainable Development Goal No 13 for reducing carbon footprint.

The rest of the paper is organized as: first in section 2 we will discuss some existing work on FL, Industry 4.0, and crowdsourcing in FL. It will be followed by proposed general MFL architecture for Industry 4.0 with a crowdsourced approach in section 3. Whereas in section 4, a few use cases are given to justify the proposed architecture. In section 5, we will highlight and explain some challenges and future directions. Finally, In the end, we will conclude our work.

2. Background

Industry 4.0 is building intelligent, networked yet secured value chains through the digitization of core functional operations for various applications e.g. predictive maintenance [4, 6], anomaly detection [62, 22], machine vision (e.g. optical character recognition, object recognition or inspection) [24], robotics [23]. Following subsections will discuss state-of-the-art about role of IoT in Industry 4.0, how DL is extended to FL, and how crowdsorucing is used for FL in other domains.

2.1. Deep Learning and Federated Learning

The term *deep learning* was coined after the re-emergence of neural networks with AlexNet model [32]. Since then, various deep models e.g. DenseNet [21], FCN [54], DeepLabV3 [11], GoogleNet [60] has been adopted in

various applications (e.g. autonomous vehicles, health, robotics) that are showing promising results. Deep learning is now a new sub-branch of machine learning that is taking machine learning to its original goal of providing artificial intelligence. The core idea compare to previous neural networks was to use more layers in a network and train it over a big dataset whose processing was possible due to the use of graphical processing units and using new activation function (ReLu) that avoid vanishing gradients in deep networks [32]. Training such a deep network with millions of parameters is not possible without a large amount of labelled training data e.g. ILSVRC dataset [51] that contains 1.5 million images from 1000 categories. However, labeling or even getting such a large number of images for each domain is a big challenge. In addition, even if various organizations or industries can label and provide or collect a dataset, due to the privacy rules like EU GDPR [16], it is hard to utilize that data without getting consent. Furthermore, without anonymising the data of each client, it becomes hard to provide security of either saving it from being hacked or backtracked directly to the real owner or manufacturer. Hence a federated approach was needed that provides privacy to the data owner.

To use privacy-preserving data, Kairouz et al. [25] first time proposed an idea of FL which is about transferring a trained model from a server to a remote edge device or organization(s) to fine-tune it over the local data of that owner. Once the network is fine-tuned, it is re-sent to the server to update the baseline model, which is further forwarded to other organizations or clients. This cycle continues and the model is regularly kept updated on the data from each organization without leaving the premises or compromising the privacy and security. This privacy and security is the main drive for adopting FL besides the reduction of communication overhead of sending raw data to the server and then processing compares to sending a small model to the clients and then receiving it to update the main model. Although, the best-explained scenario for evaluation of an FL approach is the Google's mobile keyboard [18, 25, 31, 41], however, in the majority of the cases (e.g. NVIDIA releasing Clara, and OWKIN for health sector [49]), FL is evaluated in the scenarios where the data is far more sensitive e.g. in private health-related data [55, 26, 67]. The evaluation is both qualitative and quantitative i.e security & confidentiality analysis, auditability, model performance (accuracy, loss, area under the curve), communication & computation cost, time complexity, etc. Lo et al. [39] summarised and sub-categorised components (server and clients) of an FL system. This includes compulsory components on clients (data collection, pre-processing, feature engineering, model training, and inference), on a central server (model aggregation, evaluation), and some optional components on clients (anomaly detection, model compression, auditing mechanisms, data augmentation, feature selection, security protection, privacy preservation, data provenance) and central server (advanced model aggregation, training management, incentive mechanism, resource management, communication coordination). The compulsory components mean that it performs the main FL operations. Whereas, optional components are the ones that assist or enhance the FL operations.

Despite the success and its benefits, FL is still facing various challenges both internally in its design of architecture to accommodate various infrastructures (e.g. industries), data sources (e.g. different sensors for the same task), associations or governing bodies (e.g. national & international bodies for ensuring safety (e.g. CCAM) or reducing carbon footprint e.g. UN) as well as outside in terms of attacks and the trust-building. Furthermore, challenges also exist in the form of increasing the communication efficiency between server and clients, security and reliability of both server and client from the clients and external attackers, and how to audit and scale the model, data, and the clients to increase the performance of DL network but more importantly how to bring different actors in the Industry 4.0 to a table for a common goal.

2.2. IoT for Industry 4.0

IoT is one of the core pillars of Industry 4.0 and it is playing a pivotal role in the realisation of I4.0 [43]. An amalgamation of IoT and I4.0 is also referred as Industrial Internet of Things (IIoT) [57]. IIoT is deployed for many applications of Industry 4.0, where real-time sensor data is collected from manufacturing production lines or contextual monitoring sensors in a smart factory. The collected data is then processed and analysed in real-time for monitoring and forecasting in various use cases e.g. predictive maintenance and production forecasting. A major role of IoT in the adoption of Industry 4.0 is widely advocated in both academic and industrial applied research [17, 43, 72, 7, 29]. In addition to cloud-based technologies for data storage and analytics, AI and edge computing are gaining interest in research communities to analyse IoT data at the point of action rather than storing these large datasets on the cloud infrastructure [47]. Authors in [52] demonstrated the role of big data and stream processing technologies in the realisation of IoT and Industry 4.0 usage for a predictive maintenance use case. A few techniques on the combination of AI, ML and IoT for Industry 4.0 are proposed to convert raw sensor data into smart manufacturing applications

[47, 46]. Recently, a few more advanced techniques such as the use of digital twins, distributed machine learning, and knowledge graphs have been presented [27, 8, 59, 68]. Advancements in edge analytics and FL are providing a great opportunity to apply FL over a large number of IoT devices in smart manufacturing and industry 4.0. While keeping the data at the industry level and yet building a large number of intelligent applications for federated systems. Similar to the recent advancement in the medical domain i.e. searching for a generalised model for cancer detection that can perform well on different types of input (e.g. Xrays, MRI, or CT-Scan from the device of different manufacturers), we believe that the future applications for industrial IoT will be designed in a generalised way to provide single or multi-task on-demand analytics over a large number of machines using a FL approach. Particularly, considering the dynamic nature of IoT, a loosely coupled FL with the possibility of multiple smart manufacturers volunteering to participate at the convenience of building a common learning platform will prove a big leap ahead for building intelligent IoT applications for industry 4.0 applications.

2.3. Crowdsourcing for Federated Learning

The collection of high-quality labelled data for training models is one of the fundamental requirements of ML. In general, significant human effort is required for labeling of training and testing data [42]. If done implicitly, for instance in the case of auto-correct feature in mobile phones, large amounts of labels can be gathered with minimum costs. But, if explicit attention of experts is required then it becomes challenging due to associated high costs. One solution is to use large numbers of non-experts to gather and aggregate labels – an approach known as *crowdsourcing* [20]. The main premise of crowdsourcing is that if enough answers to a question, are combined from multiple non-experts then the result can approximate an expert's answer [66]. Like crowdsourcing, FL builds a global model based on decentralized learning from data on multiple distributed devices. Existing approaches from crowdsourcing for quality control, data aggregation, and incentive mechanisms can be employed in FL to address the challenges of expensive communication, systems heterogeneity, and statistical heterogeneity [69, 35]. In traditional crowdsourcing for ML, the main objective is to aggregate labels for training data that are provided by noise labellers. By comparison, crowdsourcing for FL aggregates models from multiple devices where each device can produce low-quality models. Therefore, there are some similarities and differences in the approaches to quality control and data aggregation. However, design and algorithms for appropriate incentive mechanisms is a problem that is fundamental to both. Specifically in the context of I4.0, how to incentivise companies, industrial units, or owners of IoT devices to participate in FL is a fundamental problem.

On the other hand, [61] highlighted issues such as privacy and security, incentive mechanism, communication optimization, and quality control. In [44], these challenges were discussed in depth involving solutions like perturbation and encryption. The authors also mention the Byzantine attack and the backdoor attacks specific to the threats and vulnerabilities to the system. Beside single-point-of-failure and DDoS attacks, another security problem is losing control of the training process as described in [73]. Apart from security issues, communication bottleneck is another challenge in crowdsourced federated learning. To deal with the communication bottleneck, [34] proposed a practical solution for the excessive communication rounds in the federated networks. They used continuously running embedded speech-based models such as wake word detectors which use the federated averaging algorithm and show that the use of an adaptive averaging strategy instead of a standard weighted model reduces the number of communication rounds required to reach the target performance. The result is quite promising in terms of communication efficiency but it ignores other challenges of crowdsourced FL and thus would be as good as claimed in real-world IoT systems. To make crowdsourced FL more secure, [10, 74, 36] proposes blockchain-based implementation of FL. Cai et al. [10] elaborate on how crowdsourcing protocol enables an actor to bring a model in training and collect data from multiple sources to build a single individual model. It also provides trainers the same guarantee even when no party claims or owns the initial model. [74] used the same concept to develop a smart home system that will benefit the manufacturers in terms of feedback from the customers. A few other techniques were also proposed to enhance the security in FL such as Trusted Execution Environment (TEEs) to build assurance of participants' training executions with high confidence.

Leveraging the previously mentioned solutions, [36] proposed a combined model of blockchain with FL to build a crowdsourcing platform named CrowdSF using new encryption methods to ensure user privacy. The authors have claimed that the model works with surprisingly superior overhead than the other conventional methods and is also more accurate. Crowdsourced FL shows promising results in various applications, specifically for edge computing. However, CSFL in Industry 4.0 is not explored. Moreover, a general multilayer architecture is not proposed that can

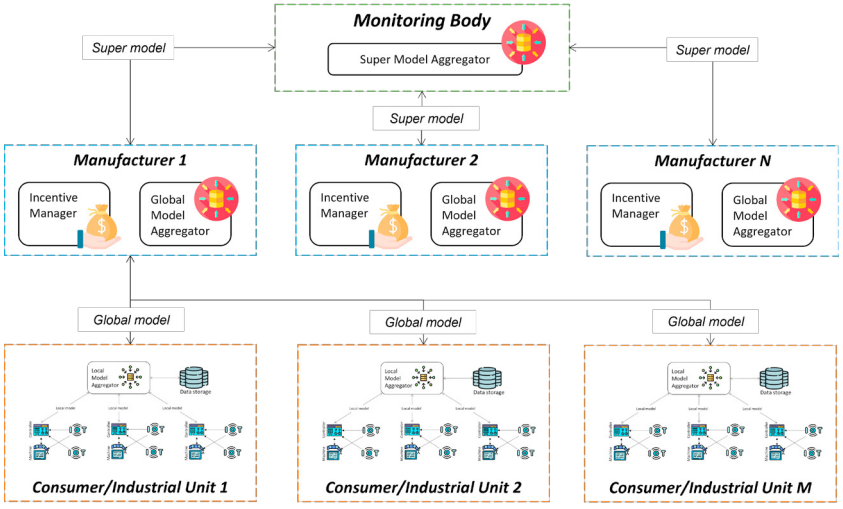

Fig. 1. Overview of the multi-level federated learning (MFL) for Industry 4.0

share incentives from government or monitory bodies level to machine manufacturers to smart manufacturers. In the following section, we will propose a multilevel FL architecture with crowdsourcing approach that can be adopted for various applications in Industry 4.0.

3. Multi-level Federated Learning

The proposed architecture is divided in three main levels based on the aggregator or user role in MFL i.e. a monitory organisation, government, or association, Machine manufacturer, and Industry or Consumer Unit. The proposed approach is designed in a way that helps each member in the federation with out losing privacy or intellectual property of a company, user, or manufacturer. Yet collaborating to achieve performance, enhance safety, and reduce usage of non-green materials. Figrue. 1 shows an overview of the MFL architecture.

Architecture: Our proposed model is an extension of the Industrial Federated Learning model (IFL) discussed in [19] which is an approach for individual industry unit. It provides industry specific collection of requirements and workflows covered in an IFL architecture. The basic implementation at Industrial unit level will be same as the IFL. However, considering that our model contain crowdsource approach where each unit volunteers therefore, the basic notation of MFL systems are updated. It consists of IoT Node in industrial units (e.g. sensor), incentive manager (at global level in MM), MFL server (a global at MM level and a local at industry unit in LMA), MFL task (Machine Learning task), MFL population (Volunteers that are industrial units) and MFL plan. Now we will discuss major modules individually from bottom (client) level towards the top (monitory).

3.1. Industrial or Consumer Unit

The Industrial Unit is the consumer or client who will have the actual data and who will utilise a trained model for various applications. These are the smart manufacturer who are the user of a machine developed by another company (i.e. manufacturer). They can have one or multiple machines from same or different manufacturer. An industrial unit is the base layer that will contain the actual data and local training and aggregation. Each industrial unit will consist of a machine, its IoT nodes, and a controller to control that machine. In addition, it will have a local model aggregator (LMA) which will be managing one or more machines (from same or different manufacturer) who are under observation through multiple IoT nodes.

As depicted in the fig. 2, consider a scenario (e.g. predictive maintenance of machines) where an industrial owner or consumer wishes to share certain type of data produced by their IoT nodes (e.g. thermometer) for specific machines (e.g. engine, a cutting tool called spindle related data in a computerised numerical control (CNC) machine) with its manufacturer. CNC machining controls a range of complex machinery, such as grinders, lathes, and turning mills, all of which are used to cut, shape, and create different parts and prototypes e.g. take a sheet of metal and turn it into a critical airplane or automobile part. The spindle is highly sensitive device and needs to be finely balanced. Its process and performance can easily be affected by spindle imbalance, temperature (e.g. thermal growth), operator

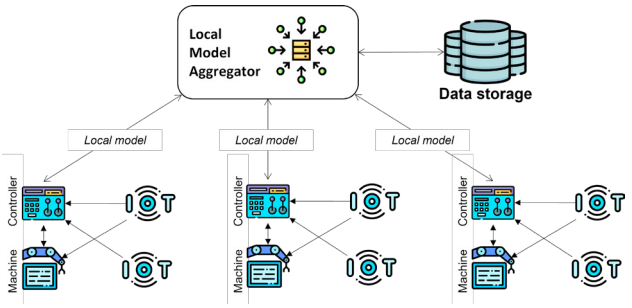

Fig. 2. Overview of the local learning in industrial units for Industry 4.0

error, sustained vibration through poor tool holders, poor programming or machining strategies. It is an expensive device to replace for smart manufacturers as well as it takes time to be replaced. The quality varies over time with the usage. Considering the influencing factors and the cost and time on maintenance, predictive maintenance can play a vital role for Industrial unit.

3.1.1. IoT Nodes, Machines, and Controllers

IoT nodes are devices connected to a controller with processing power. Each nodes contains sensors that sense the environment of a machine and produce an enormous amount of data as live streams. Our approach is to provide an opportunity to enable FL through crowdsourcing over such large number of IoT nodes. The *machines*, in this case, are the actual physical systems that are used for the purpose of smart manufacturing e.g,. a computerised numerical control machine. The predictive maintenance system will be continuously monitoring complete or part of such machine through IoT nodes e.g., a CNC spindle. The *controller* is an IoT Node with processing power. It can also be added to the integrated control system (ICS) of a machine. it can support an ICS to manage the usage of a machine, generation of alarms, and processing of data in real-time. In addition, it will also transfer data to the LMA for storage and future usage in the MFL. In MFL, the industrial unit LMA will be able to announce its availability together with a certain set of parameters (e.g. which predictive model is used in the controller, type of IoT nodes (sensors), sensor data type, & make of machine) in terms of device configuration and data quality. Once the availability is announced that industrial unit or controller (at the local level) is registered as a volunteer on the MFL platform.

3.1.2. Local Model Aggregation

LMA is server at certain level in the MFL that share a trained model with its clients (IoT nodes) and gather a model after its finetuning on the edge. The role of LMA can be both internal and external. For example, an industrial unit who has multiple machines from different MM and different IoT nodes for vibration calculation are able to gather different type of sensor data for vibration of a spindle or robotic arm. However, varying data can play a vital role if collected from multiple machines with in the unit as well as from other units in same industry. Hence, even if the industrial unit does not federate with external units or their MM in higher level, still they can combine or federate from multiple sub-units using same or different machines and IoT nodes. Hence locally enhancing a specific model for a specific machine trained over its own past data with in the unit. The LMA can also act as a client for the server in MM level. In this case, a model is shared by global model aggregator (GMA) with LMA to use and train on local data. Whenever a request to perform FL over a large corpus of clients is launched, the incentive manager at global level within the platform will identify and select the appropriate LMA.

3.2. Machine Manufacturer

Machine manufacturers (MM) are the companies who provide machines to industrial units. Their main business is to sell, rent, or lease machines to different consumers or industrial units. In this level of MFL, each manufacturer will have two modules i.e. Incentive manager and global model aggregator (GMA). This level set a platform to collect models from all the consumers of that manufacturer to provide them with an enhanced model as a new version e.g. an enhanced predictive maintenance model for the spindle. An example of such a scenario could be CNC spindle predictive maintenance system provided by MM to its consumers. Other examples can be engine manufacturers (e.g. Rolls Royce) for airbuses who rather than ask for data from the consumer may send a model to train on the consumer side and do predictive maintenance. In addition to GMA, the incentive manager will give incentives to industrial units

that cooperate in providing locally trained models. These incentives can be in any form e.g. enhanced performance, free after-sale services, or free gadgets.

3.2.1. Global Model Aggregator

MM does not perform training rather it collects the locally aggregated models from each of LMAs, aggregates them, and then shares it again with the industrial units. This helps the manufacturer to improve the overall performance of the machines and find any defects in advance, eventually saving lives and cleaning society. The aggregation in this case will be always homogeneous or horizontal due to the reason that each MM will have the same machine and input data for training the models locally. A common federation approach is averaging e.g. federatedAveraging [41] approach was a generalization that takes into account unbalanced and non-IID data. Others in crowdsourced FL have looked at a number privacy-preserving approaches e.g. [56]. Both of these works offer a foundation for the distributed training of deep networks, with emphasis on privacy and communication costs.

3.2.2. Incentive Manager

The general focus of crowdsourcing-based FL is to utilize a large number of participating industrial units with smart machines, IoT nodes, and their respective data towards a shared learning goal, where the broker distributes learning tasks to LMA or IoT nodes based on their availability, resources, and reliability. The computational nature of learning tasks and the spatiotemporal diversity of IoT nodes differentiate FL from traditional learning systems. One of the main challenges of crowdsourcing-based FL is the heterogeneity of learning tasks and IoT nodes. On one hand, learning tasks are associated with different requirements which may necessitate certain types of resources and data in IoT nodes. On the other hand, IoT nodes can be mobile as well as unreliable which means that they might be able to not complete an assigned task. Therefore, matching the requirements of FL tasks with a dynamic pool of industrial units or IoT nodes and designing appropriate incentive mechanisms to ensure participation are fundamental challenges. These challenges are particularly faced in situations where FL tasks can consume significant computation resources, network bandwidth, or battery life; and the participating nodes can independently determine when to accept or reject FL tasks.

Existing research work have proposed different formulations of the task assignment and incentive mechanisms in FL. For instance, [37] formulated the problem of task assignment, in synchronous DL, as a makespan minimization problem to minimize the execution time. Kang et al. formulated the task assignment as a reputation management problem using smart contracts where a blockchain is used to maintain training records and reputation data [28]; however, they do not consider incentives and assume that the utility of workers is to minimize the execution time on their edge devices. In comparison to the above, some recent works have considered the problem of incentive design in FL. For instance, Zou et al. [75] proposed a market design approach to FL and modeling pricing strategies as a differential game. Zhan et al. [71] designed a reinforcement mechanism for task assignment in FL to address the time-cost trade-off.

In our proposed framework, we assume that the MFL clients (i.e., industrial units or IoT nodes) voluntarily agree to participate in the FL process in expectation of rewards. Therefore, the MFL broker must decide which clients are given a MFL learning task (i.e. task assignment) and what is the associated reward (e.g. after sale service or other rewards). At the time of registration a client provides details of its capabilities including its computing resources and data. The MFL broker uses this information to find a pool of requisite clients that are capable of performing the learning task. Among the pool of capable MFL clients, the broker prices the learning task while considering the estimated reliability of each client. We propose to design the incentive mechanism that involves online learning and optimization while assuming probabilistic knowledge about reliability of clients. In our proposed approach, each FL task is associated with a using *smart contract* and the information about a client's reliability is maintained in a *blockchain* that ensures execution of smart contracts between MFL broker and clients. For each MFL assigned task to a client, besides supporting the execution of a learning task, the blockchain maintains an immutable history of events such as assignment, start, completion and payment.

Many of the MMs make it compulsory for the customers to provide machine usage data to the manufacturer. For example, Rolls-Royce makes and provides engines to many airlines and helicopter manufacturers, and it collects data from them to enhance the engine designs and perform predictive maintenance [4, 6]. In the proposed model, we give an option to the customers to provide data that will help them and others. For example, instead of labeling millions of data points, if they work in federation, each of the customer might save computational and financial resources by labeling or collecting only small amount of data that is used locally on their premises to train a federated model. In

addition, it can also help the manufacturers who do not want to share their own data. Hence, it is in customers' interest to support the aggregated model and share is benefits with consumers.

3.3. Monitory Bodies

The monitory bodies can be any governmental or non-governmental monitory association or organisation that collects the trained model and aggregate them to re-send the models to each manufacturer for enhancing the performance of a device critical to health & safety of humans and society. The monitory bodies can be national or international actors who are working for the betterment and safety of the society e.g. UN working for reducing carbon footprint. The role of these bodies is to collect global models from the manufacturers and aggregate them at super model aggregator (SMA) to provide the super model to the MM. Although this is a challenging scenario as many companies will not share their models for various reasons e.g. information leakage in FL models [14, 48], however, their is a possibility that for the betterment of a society any association that has many members might persuade companies to provide their model for aggregation of critical products e.g. Connected Cooperative & Automated Mobility (CCAM) can work on it for betterment of society similar to the work proposed in a recent project by Eureka for a federated platform for industrial technologies [2]. Similarly, Intel collaborated with another company to fight financial fraud [1] where they used data from different organisations and jurisdictions. Furthermore, the proposed model will be a good future route for projects like Machining 4.0 that have 6800 SMEs working on Machining (turning, drilling, milling) in a manufacturing process. Its has a voucher scheme to transform their production systems (50 transformation vouchers of €12.000) which can act as a kind of reward for agreeing in the MFL approach.

Bringing multiple companies is challenging, however, based on some evidence that such work is possible, the existence of opportunities for each organization, the criticality of applications towards human lives, and the reason that it will not do any training other than aggregating the models to achieve an aggregated supermodel, there is a chance that this proposed MFL is possible to implement. The FL will be somewhat similar to vertical FL i.e. the input and the models might not be the same from all the manufacturers, however, such a model will be proposed that will enhance all the respective models. Industrial control systems (ICS) in I4.0 also face a severe threat from cyber attacks. As a result, standards and best practices to handle such attacks on ICS are proposed by the European cyber security organisation (ECSO) and European network and information security agency (ENISA) [12]. Such organisation can play the role of monitory bodies for anomaly detection techniques i.e. they can create an association where manufacturers and industrial units can cooperate to provide their anomaly detection models. Hence make industrial units resilient to cyber-attack by getting an enhanced and secure anomaly detection model against attack e.g. DDoS on industrial unit.

4. Multi-level Federated Learning Use-cases

Predictive Maintenance: Predictive maintenance involves creation of a machine learning model that generates is a probabilistic estimate i.e., when a machine is going to fail. It helps in precaution, pre-order, or avoiding any accident that can cause substantial cost and depreciation in the state of the machine e.g. in CNC machine spindle, jet engines, welding machines in smart manufacturing industries. A model for predictive maintenance, when trained in MFL, can learn from the data of the same industrial unit as well as others who volunteered for a maintenance of a specific machine e.g. spindle, welding machines, jet engines, calculating and compensating for distortions in multitasking machine with the inbuilt probing system. This helps in a preventive maintenance system that eliminates fatal errors. Based on an estimate in [15], an efficient preventive system can help in saving 12-40% of the maintenance cost. In addition, it can also help in the reduction of carbon footprint. For example, a good engine will have a low carbon footprint but a defective, old, or due to some other reasons (temperature, usage, etc), the carbon footprint might increase. The benefit to the local level is maintaining a uniform usage or early prediction of problems. The benefit to the manufacturer level is overall knowledge of predictive maintenance, maintenance cost, and prediction of carbon footprint. Finally, for monitory bodies, it is having a model that is shared with all MM and their respective industrial units to reduce the carbon footprint.

Prediction of Black Carbon Emissions: A predictive model for the prediction of black carbon emissions from industrial furnaces in Industry 4.0 is presented in [50]. It not only helps the industrial units but also facilitates monitory authorities in estimating and reducing the carbon footprint in a region without targeting a specific company. For example, a good engine will have a low carbon footprint; however, due to defects or some other reasons (temperature, usage, etc), the carbon footprint of an old engine might increase. Collecting data from various smart manufacturers for training a model at the industrial level will help in enhancing the prediction model for carbon footprint at a local level, manufacturer level, and monitory bodies level. The benefit to the local level is maintaining a uniform usage or

early prediction of problems. The benefit to the manufacturer level is overall knowledge of predictive maintenance, maintenance cost, and prediction of carbon footprint. Finally, the benefit to monitory bodies is having a model that is shared with all manufacturer and their respective industrial units to reduce the carbon footprint, hence supporting the environment, society, and resources.

Fault Detection in Industrial Control Systems: Industry 4.0 uses intelligent and interconnected cyber-physical systems to automate various industrial operations ranging from design and manufacturing to supply chain and service maintenance. A fault detection system for ICS is a fundamental part of today's smart manufacturing industrial units. It helps in avoiding life-threatening situations and costly maintenance. Similarly, with advancements in IoT technologies and cloud computing, ICS has a potential threat from cyber attacks. Hence, an intrusion detection system is another important factor for I4.0. Many organizations such as the European Cyber Security Organization and the European Network and Information Security Agency have developed cybersecurity standards and gathered best practices to address this issue for the industrial control systems [12]. Therefore, it is crucial to use anomaly detection-based techniques to maintain a close eye on these systems against attacks. FL is used in [62] for anomaly detection in time-series data of an ICS. It has a lightweight anomaly detection architecture that showed fast and accurate detection in the ICS context. In [38], convolutional neural network approaches based on attention mechanism is proposed that uses long short-term memory model to allow decentralized edge devices to cooperate in training for anomaly detection. Similarly, [22] proposed an explainable FL system for anomaly detection in ICS using Shap – an explainable technique to differentiate between features of a normal and anomalous signal. These are cases where FL was used locally in an industrial unit or at a small scale across multiple units. Hence, there is an opportunity to expand this with the help of our MFL.

Smart Mobility: A MFL model can be easily adapted for today's emerging new auto industry that is becoming more electric and autonomous. This industry can ask for voluntarily but secure data from the advanced vehicles to improve their various on-board models. This data can be from on-board sensors, environment, route, speed, etc. In this case, the vehicle can considered an IoT node that will collect the data and share it with the manufacturer to enhance the performance. As a return, each IoT node will have either a free model update or any other specific reward provided by the manufacturer. This will help both the manufacturer (in enhancing their vehicle systems, learning about the faults or limitations in the system) and the owner who has an up-to-date vehicle or other upgrades. The privacy-preserving aspects of MFL will help in hiding the information, such as speed or route, that might be private to the user. The way one drives might lead to further issues for a driver e.g., not following speed limit might result in increased premiums with an insurer. An association like CCAM can play a vital in this scenario as the core objective is to have connected and safe mobility. However, one thing to highlight is that this form of federation is limited due to variation in the systems each vehicle use. If devices in autonomous vehicles have shared software or operating system then there could be the possibility of global models; otherwise, each manufacturer might have their models. If many cars manufacturer use Blackberry QNX OS then the global model can be trained on potentially more data.

Smart Agriculture: In the context of smart agriculture, the use of low-cost IoT devices for sensing and actuation is becoming common to automate and optimize the life cycle of crops at various stages. Such IoT devices, capture a significant amount of data that in turn is used for a plethora of ML-based application scenarios including but not limited to crop yield prediction, weather forecasting, and precision farming [53]. Similar to previously discussed use-cases, creating large-scale ML models based on distributed data faces challenges of data security and protection in smart agriculture and farming. This creates a potential areas for application of the proposed MFL approach.

5. Challenges and Future Research Directions

Model Sizes: A key challenge for the MFL deep network is common in FL i.e. a large number of parameters in an architecture that results in a heavy model to be transferred from SMA to GMA, GMA to LMA, LMA to edge devices, and vice versa. In addition, it also results in slow learning, information leakage, corruption during transfer, and communication overhead. Small and optimised models are needed in MFL that will be easy to transfer without loosing information or model performance. Techniques like lightweight models [62], compression [70], or specific models e.g. pyramidal models [63, 64, 65] can be used to avoid any issues.

Smart Contracts: Blockchain-based approaches have recently emerged which can address the issue of having a single central aggregator that creates a single point of failure. Authors in [40] highlighted the intrinsic advantages of using blockchain, namely that it is tamper-proof. It provides anonymity and traceability, and creates an immutable audit trail of ML models that can guarantee knowledge of provenance. Blockchain approaches also have the distinct advantage

of typically having the capability for Smart Contracts (SC) to be built into the blockchain, which sets out rules for negotiating, verifying the fulfillment of rules, and executing the agreement using formal code. The use of SCs can alleviate the problem of a malicious clients, where they can be detected and punished [13]. A commercial example can be seen in RavenProtocol [5], which is a blockchain-based FL training protocol that has been integrated with OceanProtocol [3] to act as a Compute Provider. This blockchain approach can be easily adopted for managing our proposed MFL model both at local, global, and super level aggregation of the models to enforce authenticity.

Participation and Incentive Design: The participation and incentive design in crowdsourcing can be done using dynamic procurement or posted pricing. Dynamic procurement involves repeated buying of products or services in a market [58, 9]. In our context, the MFL broker will decide prices for learning tasks to be completed by clients. This entails sequential decision making where during each interaction between broker and IoT nodes, the MFL broker decides prices for FL tasks and the client nodes can choose to accept or reject the associated contracts. In case of posted pricing mechanism, three main features make it an attractive approach for incentive design for MFL. First, the pricing algorithm is agnostic to the learning algorithm and data used for training. Therefore, the same mechanism can be used in systems that deal with multiple and heterogeneous learning models. Second, in this "take it or leave it" mechanism, the IoT nodes do not have to reveals their private costs and they do not have to bid for tasks. Third, the pricing algorithm can incorporate the contextual information about nodes, for example their reputation, reliability, performance and resources, in the deciding the prices.

IoT related challenges: IoT systems are dynamic by their nature and designed with limited or no central control. For FL algorithms to work properly, there is an expectation that IoT devices are capable of returning the calculated weights of the model with minimal delay. Stragglers devices is a known phenomenon for FL, and any FL model deployed over IoT infrastructure is expected to suffer with such issues. However, with the latest advancements there are techniques available to handle straggler devices for FL [33, 45]. Another important challenges for IoT and crowdsourced system is the provenance of data. As there is a limited control on devices, there are chances of data corruption and there is limited guarantee that FL algorithm is trained on devices with the data generated by the devices at the exact time and location as expected. However, in I4.0, there are limited chances of data corruption since there is a strong possibility of a reasonable oversight and control over participating devices within a smart factory environment.

Aggregating Heterogeneous Models to form Super modal: This novel proposed MLF model is considered for same models at each level (local, global, and super). However, the scenario where the parameters or models are not the same, in such scenario the concept of building a super model which is bigger, deeper, and more accurate can be used as the base or parent model that can be used by all the clients in the FL. Clients can adapt approaches like knowledge distillation [30] to get an optimal and customised model for their target that is based on different data. On the other hand regarding how different models can be aggregated, a model consists of kernels which are automatically learned filters (similar to Sobel, Laplacian, etc. which were designed after careful consideration and research), these new kernels can be stored in a model bank that can be later used by clients in transfer learning or knowledge distillation (child network is designed from a parent network by selecting only few layers & kernels of the whole network) approach to design a small and accurate model for the specific target/s.

6. Conclusion

The proposed framework is a novel multi-level design for crowdsourced FL in Industry 4.0. It helps various actors in Industry 4.0 from individual smart manufacturer to machine manufacturer up to local and international monitory bodies. It provides a mechanism to ensure training over highly distributed sensor data from various machines in one or more industrial units. Appropriate incentive mechanisms are suggested for persuading industrial units and machine manufacturers to volunteer for federation. To the best of our knowledge, MFL is a new platform that provides a foundational design for machine learning in a more connected future in Industry 4.0 that can lead to a better, clean, green, and safe society. Several use-cases with background justification are given which provide a path for successful deployment of MFL in the near future. In addition, several challenges are highlighted that will help future researchers to work in exploring, designing, and implementation. In future, we intend to implement and deploy MFL pilots in Industry 4.0 for some of the common problems that require large amount of complex sensor data. In addition, it is worth mentioning that multilayered federated learning can also leverage different machine learning techniques and should be agnostic to the used techniques.

Acknowledgement This publication has emanated from research supported in part by a Grant from Science Foundation Ireland under Grant number [SFI 20/SPP/3705].

References

[1] Intel Consilient Join Forces to Use Federated Learning to Fight Financial Fraudl, . URL https://www.unite.ai/intel-consilient-join-forces-to-use-federated-learning-to-fight-financial-fraud/.

[2] Federated ai platform for industrial technologies, . URL https://www.celticnext.eu/project-f4itech/.

[3] Data is a new asset class. — Ocean Protocol. URL https://oceanprotocol.com/.

[4] How Rolls-Royce Maintains Jet Engines With the IoT. URL https://www.rtinsights.com/rolls-royce-jet-engine-maintenance-iot/.

[5] Artificial Intelligence — Raven Protocol. URL https://www.ravenprotocol.com/.

[6] The Rolls-Royce IntelligentEngine – Driven by data. URL https://www.rolls-royce.com/media/press-releases/2018/06-02-2018-rr-intelligentengine-driven-by-data.aspx.

[7] Shohin Aheleroff, Xun Xu, Yuqian Lu, Mauricio Aristizabal, Juan Pablo Velásquez, Benjamin Joa, and Yesid Valencia. Iot-enabled smart appliances under industry 4.0: A case study. *Advanced engineering informatics*, 43:101043, 2020.

[8] Muhammad Intizar Ali, Pankesh Patel, John G Breslin, Ramy Harik, and Amit Sheth. Cognitive digital twins for smart manufacturing. *IEEE Intelligent Systems*, 36(2):96–100, 2021.

[9] Ashwinkumar Badanidiyuru, Robert Kleinberg, and Yaron Singer. Learning on a budget: Posted price mechanisms for online procurement. In *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, page 128–145, New York, NY, USA, 2012. Association for Computing Machinery. ISBN 9781450314152. doi: 10.1145/2229012.2229026.

[10] Harry Cai, Daniel Rueckert, and Jonathan Passerat-Palmbach. 2cp: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments, 11 2021. URL https://arxiv.org/pdf/2011.07516.pdf.

[11] Liang-Chieh Chen, Yukun Zhu, George Papandreou, Florian Schroff, and Hartwig Adam. Encoder-decoder with atrous separable convolution for semantic image segmentation. In *ECCV (7)*, volume 11211 of *Lecture Notes in Computer Science*, pages 833–851. Springer, 2018.

[12] Angelo Corallo, Mariangela Lazoi, and Marianna Lezzi. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114:103165, 2020. ISSN 0166-3615. doi: https://doi.org/10.1016/j.compind.2019.103165. URL https://www.sciencedirect.com/science/article/pii/S0166361519304427.

[13] Harsh Bimal Desai, Mustafa Safa Ozdayi, and Murat Kantarcioglu. BlockFLA. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, pages 101–112, New York, NY, USA, 4 2021. ACM. ISBN 9781450381437. doi: 10.1145/3422337.3447837. URL https://dl.acm.org/doi/10.1145/3422337.3447837.

[14] Jiahui Geng, Yongli Mou, Feifei Li, Qing Li, Oya Beyan, Stefan Decker, and Chunming Rong. Towards general deep leakage in federated learning. 10 2021. URL http://arxiv.org/abs/2110.09074.

[15] Morteza Ghobakhloo. The future of manufacturing industry: a strategic roadmap toward industry 4.0. *Journal of Manufacturing Technology Management*, 2018.

[16] Bryce Goodman and Seth Flaxman. European union regulations on algorithmic decision making and a "right to explanation". *AI Magazine*, 38(3):50–57, 2017. ISSN 07384602. doi: 10.1609/aimag.v38i3.2741.

[17] Francis Griffiths and Melanie Ooi. The fourth industrial revolution-industry 4.0 and iot [trends in future i&m]. *IEEE Instrumentation & Measurement Magazine*, 21(6):29–43, 2018.

[18] Andrew Hard, Chloé M Kiddon, Daniel Ramage, Francoise Beaufays, Hubert Eichner, Kanishka Rao, Rajiv Mathews, and Sean Augenstein. Federated learning for mobile keyboard prediction, 2018. URL https://arxiv.org/abs/1811.03604.

[19] Thomas Hiessl, Daniel Schall, Jana Kemnitz, and Stefan Schulte. Industrial federated learning – requirements and system design. *Communications in Computer and Information Science*, 1233 CCIS:42–53, 2020. ISSN 18650937. doi: 10.1007/978-3-030-51999-5_4.

[20] Jeff Howe. The rise of crowdsourcing. *Wired magazine*, 14(6):1–4, 2006.

[21] Gao Huang, Zhuang Liu, Laurens Van Der Maaten, and Kilian Q Weinberger. Densely connected convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 4700–4708. IEEE Computer Society, 2017.

[22] Truong Thu Huong, Ta Phuong Bac, Kieu Ngan Ha, Nguyen Viet Hoang, Nguyen Xuan Hoang, Nguyen Tai Hung, and Kim Phuc Tran. Federated learning-based explainable anomaly detection for industrial control systems. *IEEE Access*, 10:53854–53872, 2022. ISSN 2169-3536. doi: 10.1109/ACCESS.2022.3173288. URL https://ieeexplore.ieee.org/document/9770834/.

[23] Unai Izagirre, Imanol Andonegui, Itziar Landa-Torres, and Urko Zurutuza. A practical and synchronized data acquisition network architecture for industrial robot predictive maintenance in manufacturing assembly lines. *Robotics and Computer-Integrated Manufacturing*, 74:102287, 2022.

[24] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, and Rajiv Suman. Exploring impact and features of machine vision for progressive industry 4.0 culture. *Sensors International*, 3:100132, 2022. ISSN 2666-3511. doi: https://doi.org/10.1016/j.sintl.2021.100132. URL https://www.sciencedirect.com/science/article/pii/S266635112100053X.

[25] Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, Rafael G. L. D'Oliveira, Hubert Eichner, Salim El Rouayheb, David Evans, Josh Gardner, Zachary Garrett, Adrià Gascón, Badih Ghazi, Phillip B. Gibbons, Marco Gruteser, Zaid Harchaoui, Chaoyang He, Lie He, Zhouyuan Huo, Ben Hutchinson, Justin Hsu, Martin Jaggi, Tara Javidi, Gauri Joshi, Mikhail Khodak, Jakub Konečný, Aleksandra Korolova, Farinaz Koushanfar, Sanmi Koyejo, Tancrède Lepoint, Yang Liu, Prateek Mittal, Mehryar Mohri, Richard Nock, Ayfer Özgür, Rasmus Pagh, Mariana Raykova, Hang Qi, Daniel Ramage, Ramesh Raskar, Dawn Song, Weikang Song, Sebastian U. Stich, Ziteng Sun, Ananda Theertha Suresh, Florian Tramèr, Praneeth Vepakomma, Jianyu Wang, Li Xiong, Zheng Xu, Qiang Yang, Felix X. Yu, Han Yu, and Sen Zhao. Advances and open problems in federated learning, 2019. URL https://arxiv.org/abs/1912.04977.

[26] Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert, and Rickmer F. Braren. Secure, privacy-preserving and federated machine learning

in medical imaging. *Nature Machine Intelligence*, 2(6):305–311, 2020. ISSN 2522-5839. doi: 10.1038/s42256-020-0186-1. URL http://dx.doi.org/10.1038/s42256-020-0186-1.

[27] Vignesh Kamath, Jeff Morgan, and Muhammad Intizar Ali. Industrial iot and digital twins for a smart factory: An open source toolkit for application design and benchmarking. In *2020 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2020.

[28] Jiawen Kang, Zehui Xiong, Xuandi Li, Yang Zhang, Dusit Niyato, Cyril Leung, and Chunyan Miao. Optimizing task assignment for reliable blockchain-empowered federated edge learning. *IEEE Transactions on Vehicular Technology*, 70(2):1910–1923, 2021. doi: 10.1109/TVT.2021.3055767.

[29] Ibrahim Haleem Khan and Mohd Javaid. Role of internet of things (iot) in adoption of industry 4.0. *Journal of Industrial Integration and Management*, page 2150006, 2021.

[30] Youmin Kim, Jinbae Park, YounHo Jang, Muhammad Ali, Tae-Hyun Oh, and Sung-Ho Bae. Distilling global and local logits with densely connected relations. In *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 6270–6280, 2021. doi: 10.1109/ICCV48922.2021.00623.

[31] Jakub Konečný, H. Brendan McMahan, Felix X. Yu, Peter Richtarik, Ananda Theertha Suresh, and Dave Bacon. Federated learning: Strategies for improving communication efficiency. In *NIPS Workshop on Private Multi-Party Machine Learning*, 2016. URL https://arxiv.org/abs/1610.05492.

[32] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. ImageNet Classification with Deep Convolutional Neural Networks. In *Advances in NIPS*, pages 1097–1105, 2012.

[33] Siddhartha Kumar, Reent Schlegel, Eirik Rosnes, et al. Coding for straggler mitigation in federated learning. *arXiv preprint arXiv:2109.15226*, 2021.

[34] David Leroy, Alice Coucke, Thibaut Lavril, Thibault Gisselbrecht, and Joseph Dureau. Federated learning for keyword spotting. *arXiv:1810.05512 [cs, eess, stat]*, 02 2019. URL https://arxiv.org/abs/1810.05512.

[35] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3):50–60, 5 2020. ISSN 15580792. doi: 10.1109/MSP.2020.2975749.

[36] Ziyuan Li, Jian Liu, Jialu Hao, Huimei Wang, and Ming Xian. CrowdSFL: A secure crowd computing framework based on blockchain and federated learning. *Electronics (Switzerland)*, 9(5):773, 5 2020. ISSN 20799292. doi: 10.3390/electronics9050773.

[37] Laércio Lima Pilla. Optimal task assignment for heterogeneous federated learning devices. In *2021 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pages 661–670, 2021. doi: 10.1109/IPDPS49936.2021.00074.

[38] Yi Liu, Sahil Garg, Jiangtian Nie, Yang Zhang, Zehui Xiong, Jiawen Kang, and M Shamim Hossain. Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal*, 8(8):6348–6358, 2020.

[39] Sin Kit Lo, Qinghua Lu, Chen Wang, Hye-Young Paik, and Liming Zhu. A Systematic Literature Review on Federated Machine Learning: From A Software Engineering Perspective. 37(4), 2020. URL http://arxiv.org/abs/2007.11354.

[40] Chuan Ma, Jun Li, Ming Ding, Long Shi, Taotao Wang, Zhu Han, and H. Vincent Poor. When Federated Learning Meets Blockchain: A New Distributed Learning Paradigm. 9 2020. URL http://arxiv.org/abs/2009.09338.

[41] H. McMahan, Eider Moore, D. Ramage, and Blaise Agüera y Arcas. Federated learning of deep networks using model averaging. *ArXiv*, abs/1602.05629, 2016.

[42] Cade Metz. A.I. Is Learning From Humans. Many Humans. (Published 2019). *The New York Times*, August 2019. ISSN 0362-4331. URL https://www.nytimes.com/2019/08/16/technology/ai-humans.html.

[43] Marcelo T Okano. Iot and industry 4.0: the industrial new revolution. In *International Conference on Management and Information Systems*, volume 25, page 26, 2017.

[44] Shashi Raj Pandey, Nguyen H. Tran, Mehdi Bennis, Yan Kyaw Tun, Aunas Manzoor, and Choong Seon Hong. A crowdsourcing framework for on-device federated learning. *IEEE Transactions on Wireless Communications*, 19(5):3241–3256, 5 2020. ISSN 1536-1276. doi: 10.1109/TWC.2020.2971981. URL https://ieeexplore.ieee.org/document/8995775/.

[45] Jungwuk Park, Dong-Jun Han, Minseok Choi, and Jaekyun Moon. Sself: Robust federated learning against stragglers and adversaries. 2020.

[46] Pankesh Patel, Muhammad Intizar Ali, and Amit Sheth. On using the intelligent edge for iot analytics. *IEEE Intelligent Systems*, 32(5):64–69, 2017.

[47] Pankesh Patel, Muhammad Intizar Ali, and Amit Sheth. From raw data to smart manufacturing: Ai and semantic web of things for industry 4.0. *IEEE Intelligent Systems*, 33(4):79–86, 2018.

[48] Anastassiya Pustozerova and Rudolf Mayer. Information leaks in federated learning. Internet Society, 8 2021. doi: 10.14722/diss.2020.23004.

[49] Nicola Rieke, Jonny Hancox, Wenqi Li, Fausto Milletarì, Holger R. Roth, Shadi Albarqouni, Spyridon Bakas, Mathieu N. Galtier, Bennett A. Landman, Klaus Maier-Hein, Sébastien Ourselin, Micah Sheller, Ronald M. Summers, Andrew Trask, Daguang Xu, Maximilian Baust, and M. Jorge Cardoso. The future of digital health with federated learning. *npj Digital Medicine*, 3(1):1–7, 2020. ISSN 23986352. doi: 10.1038/s41746-020-00323-1. URL http://dx.doi.org/10.1038/s41746-020-00323-1.

[50] Javier Rubio-Loyola and Wolph Ronald Shwagger Paul-Fils. Applied machine learning in industry 4.0: Case-study research in predictive models for black carbon emissions. *Sensors*, 22(10):3947, 2022.

[51] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision (IJCV)*, 115(3):211–252, 2015. doi: 10.1007/s11263-015-0816-y.

[52] Radhya Sahal, John G Breslin, and Muhammad Intizar Ali. Big data and stream processing platforms for industry 4.0 requirements mapping for a predictive maintenance use case. *Journal of Manufacturing Systems*, 54:138–151, 2020.

[53] Faisal Karim Shaikh, Mohsin Ali Memon, Naeem Ahmed Mahoto, Sherali Zeadally, and Jamel Nebhen. Artificial intelligence best practices in smart agriculture. *IEEE Micro*, 42(1):17–24, 2021.

[54] Evan Shelhamer, Jonathan Long, and Trevor Darrell. Fully convolutional networks for semantic segmentation. *IEEE Trans. Pattern Anal. Mach. Intell.*, 39(4):640–651, April 2017. ISSN 0162-8828.

[55] Micah J Sheller, Brandon Edwards, G Anthony Reina, Jason Martin, Sarthak Pati, Aikaterini Kotrotsou, Mikhail Milchenko, Weilin Xu, Daniel Marcus, Rivka R Colen, and Spyridon Bakas. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data. *Scientific Reports*, 10(1):12598, 2020. ISSN 2045-2322. doi: 10.1038/s41598-020-69250-1. URL https://doi.org/10.1038/s41598-020-69250-1.

[56] Reza Shokri and Vitaly Shmatikov. Privacy-Preserving Deep Learning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, volume 2015-October, pages 1310–1321, New York, NY, USA, 10 2015. ACM. ISBN 9781450338325. doi: 10.1145/2810103.2813687. URL https://dl.acm.org/doi/10.1145/2810103.2813687.

[57] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. Industrial internet of things: Challenges, opportunities, and directions. *IEEE transactions on industrial informatics*, 14(11):4724–4734, 2018.

[58] Aleksandrs Slivkins and Jennifer Wortman Vaughan. Online decision making in crowdsourcing markets: Theoretical challenges. *SIGecom Exch.*, 12(2):4–23, November 2014. doi: 10.1145/2692359.2692364. URL https://doi.org/10.1145/2692359.2692364.

[59] Bharath Sudharsan, Pankesh Patel, John Breslin, Muhammad Intizar Ali, Karan Mitra, Schahram Dustdar, Omer Rana, Prem Prakash Jayaraman, and Rajiv Ranjan. Toward distributed, global, deep learning using iot devices. *IEEE Internet Computing*, 25(03):6–12, 2021.

[60] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. Going deeper with convolutions. In *Computer Vision and Pattern Recognition (CVPR)*, 2015.

[61] Yongxin Tong, Yansheng Wang, and Dingyuan Shi. Federated learning in the lens of crowdsourcing. URL http://sites.computer.org/debull/A20sept/p26.pdf.

[62] Huong Thu Truong, Bac Phuong Ta, Quang Anh Le, Dan Minh Nguyen, Cong Thanh Le, Hoang Xuan Nguyen, Ha Thu Do, Hung Tai Nguyen, and Kim Phuc Tran. Light-weight federated learning-based anomaly detection for time-series data in industrial control systems. *Computers in Industry*, 140:103692, 9 2022. ISSN 0166-3615. doi: https://doi.org/10.1016/j.compind.2022.103692. URL https://www.sciencedirect.com/science/article/pii/S0166361522000896.

[63] Ihsan Ullah and Alfredo Petrosino. A strict pyramidal deep neural network for action recognition. In Vittorio Murino and Enrico Puppo, editors, *Image Analysis and Processing — ICIAP 2015*, pages 236–245, Cham, 2015. Springer International Publishing. ISBN 978-3-319-23231-7.

[64] Ihsan Ullah and Alfredo Petrosino. About pyramid structure in convolutional neural networks. In *2016 International Joint Conference on Neural Networks (IJCNN)*, pages 1318–1324. IEEE, 2016.

[65] Ihsan Ullah, Sean Reilly, and Michael G Madden. Enhancing semantic segmentation of aerial images with inhibitory neurons. In *2020 25th International Conference on Pattern Recognition (ICPR)*, pages 5451–5458. IEEE, 2021.

[66] Jennifer Wortman Vaughan. Making better use of the crowd: How crowdsourcing can advance machine learning research. *The Journal of Machine Learning Research*, 18(1):7026–7071, 2017.

[67] Jie Xu and Fei Wang. Federated Learning for Healthcare Informatics. *arXiv*, 2019.

[68] Muhammad Yahya, John G Breslin, and Muhammad Intizar Ali. Semantic web and knowledge graphs for industry 4.0. *Applied Sciences*, 11 (11):5110, 2021.

[69] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):1–19, 2019.

[70] Tien-Ju Yang, Yonghui Xiao, Giovanni Motta, Françoise Beaufays, Rajiv Mathews, and Mingqing Chen. Online model compression for federated learning with large models, 2022. URL https://arxiv.org/abs/2205.03494.

[71] Yufeng Zhan, Jie Zhang, Zicong Hong, Leijie Wu, Peng Li, and Song Guo. A survey of incentive mechanism design for federated learning. *IEEE Transactions on Emerging Topics in Computing*, pages 1–1, 2021. ISSN 2168-6750. doi: 10.1109/TETC.2021.3063517. URL https://ieeexplore.ieee.org/document/9369019/.

[72] Caiming Zhang and Yong Chen. A review of research relevant to the emerging industry trends: Industry 4.0, iot, blockchain, and business analytics. *Journal of Industrial Integration and Management*, 5(01):165–180, 2020.

[73] Xiaoli Zhang, Fengting Li, Zeyu Zhang, Qi Li, Cong Wang, and Jianping Wu. Enabling execution assurance of federated learning at untrusted participants. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 07 2020. doi: 10.1109/infocom41043.2020.9155414.

[74] Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, Dusit Niyato, Zengxiang Li, Lingjuan Lyu, and Yingbo Liu. Privacy-preserving blockchain-based federated learning for iot devices. *IEEE Internet of Things Journal*, 8:1–1, 2020. doi: 10.1109/jiot.2020.3017377.

[75] Yuze Zou, Shaohan Feng, Jing Xu, Shimin Gong, Dusit Niyato, and Wenqing Cheng. Dynamic games in federated learning training service market. In *2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, pages 1–6, 2019. doi: 10.1109/PACRIM47961.2019.8985096.