

Federated Learning for Anomaly Detection in Industrial IoT-enabled Production Environment Supported by Autonomous Guided Vehicles

Bohdan Shubyn^{1,2}[0000-0002-3051-1544], Dariusz Mrozek¹[0000-0001-6764-6656],
Taras Maksymyuk²[0000-0002-2739-9862], Vaidy Sunderam³[0000-0002-5128-7852],
Daniel Kostrzewa¹[0000-0003-2781-3709], Piotr Grzesik¹[0000-0001-8868-0765], and
Paweł Benecki¹[0000-0003-4674-5393]

¹ Silesian University of Technology, Department of Applied Informatics, Gliwice,
Poland Bohdan.Shubyn@polsl.pl

² Lviv Polytechnic National University, Department of Telecommunications, Lviv,
Ukraine

³ Department of Computer Science, Emory University, Atlanta, GA 30322, USA
vss@emory.edu

Abstract. Intelligent production requires maximum downtime avoidance since downtimes lead to economic loss. Thus, Industry 4.0 (today's IoT-driven industrial revolution) is aimed at automated production with real-time decision-making and maximal uptime. To achieve this, new technologies such as Machine Learning (ML), Artificial Intelligence (AI), and Autonomous Guided Vehicles (AGVs) are integrated into production to optimize and automate many production processes. The increasing use of AGVs in production has far-reaching consequences for industrial communication systems. To make AGVs in production even more effective, we propose to use Federated Learning (FL) which provides a secure exchange of experience between intelligent manufacturing devices to improve prediction accuracy. We conducted research in which we exchanged experiences between the three virtual devices, and the results confirm the effectiveness of this approach in production environments.

Keywords: federated learning · predictive maintenance · smart production · Artificial Intelligence · long-short term memory · recurrent neural networks

1 Introduction

The main goal of Industry 4.0 is automated production with real-time decision-making. Modern manufacturing relies on a complex ecosystem that consists of many elements, various sensors, intelligent devices, people, and is a rich environment for data collection and analysis.

Leading technologies being rapidly adopted into production environments include Autonomous Guided Vehicles (AGVs). The use of AGVs in production systems has many advantages as it allows production lines to be automated

and accelerates logistics. AI-driven analytics at the edge (i.e. edge computing) plays a significant role in coordinating a fleet of AGVs and enabling robust production cycles. These analytics cover the development and use of Machine Learning (ML) algorithms to analyze the behavior of AGVs on the edge IoT device to detect any anomalies, possible problems, or failures. However, AGVs operate as separate units, with own characteristics and sometimes in specific production environments. Thus, they gain experience during their operational cycles within different environments (e.g., different types of pavement on the floor, different temperature and air humidity in the room).

Real-time analysis of production data and advanced data exploration can provide remote condition monitoring and predictive maintenance tools to detect the first signs of failure in industrial environments long before the appearance of the early alarms that precede failures of AGVs in a short period. However, for the effective use of such approaches in real production, it is necessary to have large amounts of useful information, which is very difficult and expensive to obtain. Thus, to solve this problem and make AGVs in production more effective in detecting failures on a broader scale, we investigate the use of Federated Learning (FL), which allows the exchange of experience-data between AGVs.

The main idea of FL is that the same type of intelligent devices or AGVs in production has the opportunity to share experiences. As a result of sharing experience, it is possible to optimize production by increasing the amount of knowledge about various breakdowns of production, which allows better prediction and avoidance. To ensure security, and to prevent information from all these devices from being intercepted or stolen, it is transmitted in the form of neural network weights, which are suitable only for further processing at the highest level, without carrying directly helpful information.

Federated Learning originated from the fact that much of the data containing helpful information used to solve specific problems are challenging to obtain in quantities that would be sufficient to train a powerful model of deep learning. In addition to the helpful information needed to train the model, the data sets also contain other information that is not relevant to the problem. Moreover, Federated Learning benefits from the fact that IoT devices can store all the necessary information for training. Therefore, there is no need to store vast amounts of training data in the cloud, which improves decentralized, edge-based data processing.

In this paper, we show that FL improves the efficiency of failure prediction on edge IoT devices by building a global prediction model based on many local prediction models of particular AGVs. The rest of the paper is organized as follows. In section 2, we review the related works. Section 3 describes a new approach to data exchange between devices, which allows intelligent devices to share experiences with one another to increase the accuracy of recurrent neural networks. In Section 5, we conduct a study that demonstrates the efficiency of the proposed approach in a smart production environment. And finally, Section 5 concludes the paper.

2 Related Works

Manufacturing companies use new technologies to monitor and better understand their operations, perform them in real-time, thus, turning *classical production* into *intelligent production*. Intelligent production is equipped with technology that ensures machine-machine (M2M) and machine-human (M2H) interaction in tandem with analytical and cognitive technologies so that decisions are made correctly and in a timely manner [2]. The most significant and influential technologies that facilitate conversion from classical production to smart production include Predictive Maintenance, Machine learning, Recurrent Neural Networks, and Federated Learning. Predictive Maintenance (PdM) monitors the state of production during its expected life cycle to provide advanced insights, which ensures the detection of anomalies that are not typical for the task. The purpose of predictive maintenance for manufacturing is to maximize their equipment parts' useful life, avoid unplanned downtime, and minimize planned downtime [9]. An excellent example of this technology is described in [5, 7]. In [7], the authors rely on the Numenta Anomaly Benchmark (NAB) [1]. NAB was designed to fairly benchmark anomaly detection algorithms against one another. The approach proposed by the authors scored 64.71 points, while LSTM and GRU scored 49.38 and 61.06 points, respectively.

Predictive maintenance often applies Machine learning (ML) for anomaly detection. ML is a subset of artificial intelligence that is actively being used in industrial settings. The use of machine learning in production is described in detail in [10, 6], showing that ML and Deep Learning (DL) can make current manufacturing systems more agile and energy-efficient and lead to optimization of many production processes.

The analysis of literature related to PdM shows that one of the most promising failure forecasting methods is Artificial Neural Networks (ANNs). In the case of manufacturing, it is even more appropriate to use Recurrent Neural Networks (RNNs). The most popular architectures of RNNs in the production environment are Gated recurrent unit (GRU) and Long short-term memory (LSTM). An example of using the GRU model for predictive analytics in intelligent manufacturing is presented in [12]. The authors proposed a hybrid prediction scheme accomplished by a newly developed deep heterogeneous GRU model, along with local feature extraction. Essien and Giannetti [4] proposed to use a novel deep ConvLSTM autoencoder architecture for machine speed prediction in an intelligent manufacturing process by restructuring the input sequence to a supervised learning framework using a sliding-window approach. Table 1 provides the summary of technologies and references to the literature related to intelligent production.

The most recent works for detecting anomalies in production environments rely on the idea of Distributed Learning and Federated Learning (FL) [8, 13, 14]. In [14], the authors introduced the architecture of the two-level FL named Real-Time Automatic Configuration Tuning (REACT) with local servers hosting the knowledge base for gathering the shared experience. This paper extends the idea by pushing the construction of the local models down to the edge IoT devices

without exchanging the production and operational data. In this work, we show both alternative architectures and test the edge-based approach, in terms of the accuracy of performed prediction.

Table 1. A brief summary of technologies related to smart production idea.

Technology	Survey	Brief description
Predictive Maintenance for manufacturing	[5, 7, 1, 9]	The purpose of predictive maintenance (PdM) for manufacturing is to maximize the useful life of their equipment parts, avoiding unplanned downtime.
Recurrent Neural Networks	[12, 4]	Recurrent Neural Networks have effect of “memory”, which will allow to create various patterns of errors in production, in order to understand what problems can await on it and solve them in real-time.
AGVs in manufacturing	[11, 3]	The use of AGV in production systems has many advantages as it allows production lines to be automated and accelerates logistics, moreover it can be introduced in almost all branches of industry and areas of production.
Federated Learning	[14, 8, 13]	The main idea of FL is that intellectual devices or AGVs in production has the opportunity to safely share experiences with each other.

3 Federated Learning for Intelligent Manufacturing

Federated Learning allows companies to train machine learning models without moving data from devices where this data is generated, and therefore, it has the inherent characteristics of preserving the privacy of data and reducing the amount of transferred data. These characteristics are required for industrial IoT environments that need data processing solutions working in real-time. We have been introducing this idea in the production environments operating based on the fleet of AGVs that are manufactured by the AIUT company in Poland. Fig. 1 shows the loaded Formica-1 AGV that we have been supplementing with edge-based AI/FL methods.

The complete process of exchanging data between AGVs is called a *round*. The round operates according to Algorithm 1 (also graphically visualized in Fig. 2). First, each AGV trains a local model on a specific data set locally (lines 1-4). In the second step, all AGVs send updated local models to the server (lines 5-7). Next, all local models are averaged on the server to create a global model that takes into account the experience of all AGVs (line 8). Finally, the server sends the updated global model back to the AGVs to update their local model with the new global model (lines 9-11).



Fig. 1. The Formica 1 AGV used in our tests.

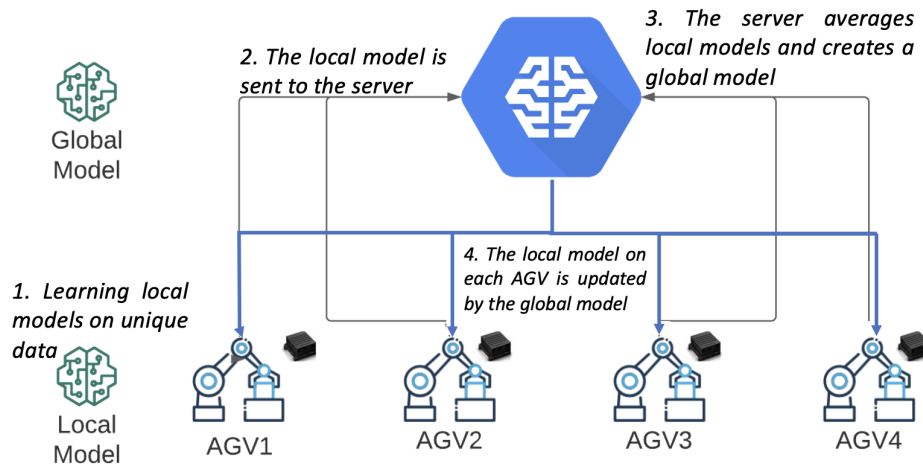


Fig. 2. The complete process of exchanging data between devices (Round)

Algorithm 1: Algorithm of the round

Data: lm (Local models on AGVs), gm (Global model), $AGVs$ (the fleet of AGVs), N (the number of AGVs), sgm (Server with a global model)
Result: $upAGVs$ (AGVs updated by global model)

```

1 for  $i \leftarrow 1$  to  $AGVs$  do
2   | Train the RNN of  $AGV_i$  locally on unique, AGV-specific data;
3   |  $lm \leftarrow$  weights of the local RNN;
4 end
5 foreach  $lm \in AGVs$  do
6   | Send  $lm$  to the  $sgm$ ;
7 end
8 Build the  $gm$  by averaging  $lms$  on the  $sgm$ ;
9 foreach  $lm \in AGVs$  do
10  | Update  $lm$  by the  $sgm$ ;
11 end
```

Given the technical characteristics of the operational, industrial environment for the AGVs, we have identified two main architectures for the integration of FL into production. They are suitable for the manufacturing ecosystem, and their choice depends on the specifics of the production.

3.1 AI on the local servers

In this case, each production line must have its own local database and computing resources, which will collect information and analyze all AGVs in this line (Fig. 3). Data from devices are sent to local servers (marked in blue in Fig. 3). These local servers create the global neural network model for this line, taking into account data from all devices in this line. The second step covers transferring the weights of neural networks from the local knowledge base to the data center (e.g., in the cloud), where a general global model is created. This global model takes the experience of all production lines (blue lines). And this global model of a neural network is sent back to all local knowledge bases (green lines). This approach is cheaper and suitable for improving prediction accuracy for static production lines.

3.2 AI on the on-board IoT devices

In this case, each AGV creates its own local neural network (Fig. 4). It learns from its unique data, thereby modifying the weights of neural networks. In the next step, the weights of the local neural networks are sent to the data center in the cloud (marked with blue lines), where one global model is created, taking into account the experience of all similar devices. Finally, the global model from the cloud is sent to all devices (marked with green lines). As a result, this process allows each AGV to gain experience from other AGVs, taking more anomalies and production-critical situations into account.

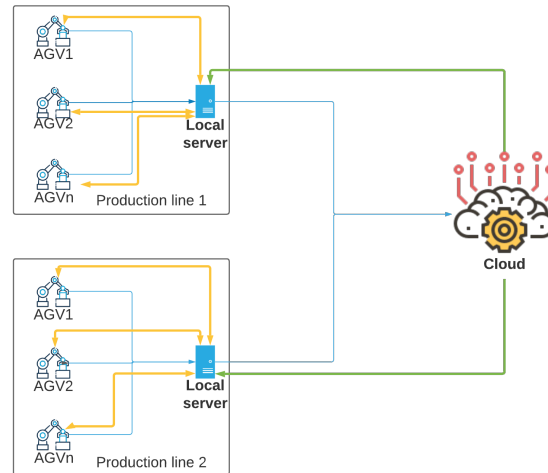


Fig. 3. Distributed architecture with AI/FL on the local servers.

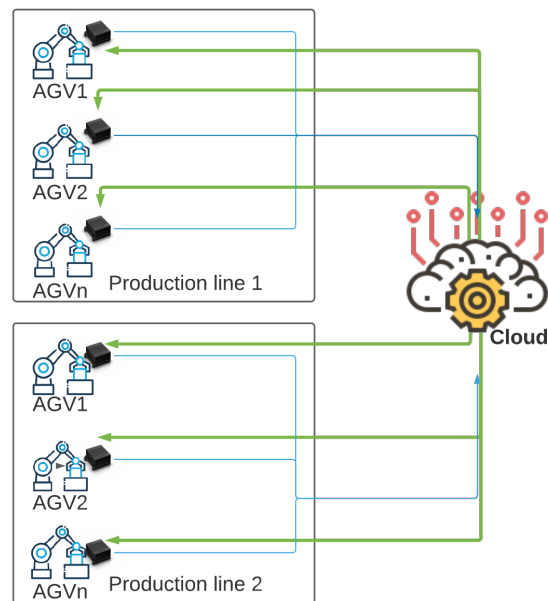


Fig. 4. Distributed architecture with AI on the on-board IoT devices.

Also, the data obtained in real-time are compared with those predicted by our FL-based neural network on the IoT devices themselves, thus checking whether the AGV is working correctly. The advantages of this architecture are:

1. The capability to detect failures as quickly as possible;
2. Maximum data security, as data from AGVs are not transmitted to the cloud, and most of them will be processed locally. Only the weights of neural networks are transferred, from which it will not be possible to extract any information.

4 Testing Effectiveness of FL

We conducted several experiments with the real Formica-1 AGVs, obtaining various data from them, including momentary and cumulative power consumption, battery cell voltage, motor RPM, energy consumption and current consumption, cumulative distances, bearing temperatures, transportation pin actuator signals, and momentary frequencies. However, at present, this data set is not sufficient to train models that can be shared between other AGVs, since the work on embedding intelligence into the AGVs is still ongoing. Thus, we simulated the working environment with virtual AGVs (virtual clients). For this purpose, we used a Numanta Anomaly Benchmark (NAB) data set [1] that contains information from temperature sensors of an internal component of a large, industrial machine. The temperature is one of the essential monitored parameters for the proper operation of many production machines. For example, changes in the bearing temperature may suggest its failure and, consequently, the shutdown of the production machine or increased energy consumption and shorter operating time of the AGV. The data from the NAB data set were collected around the clock for 70 days at a sampling interval of 5 minutes. This data set allowed us to understand the problems of implementing FL in AGVs as well as average deviations of device temperature over time. For this study, we used FL architecture with the AI/FL implemented on the IoT device monitoring the AGV. This option does not require additional local servers for separate production lines. It also provides better security for industrial data, as all the data will be processed locally on the devices and won't be sent anywhere, reducing the communication needs (and the amount of transferred data). We divided the data set into four main parts. The first three parts of the data (each one of them was 30 percent of the data set) were used as training data for three different virtual clients. Then, we used the last part of this data set (10 percent) to test the efficiency of local models from the virtual clients and the global model to compare their effectiveness with each other.

4.1 Choosing Artificial Neural Network model

Given the fact that we work with time series, we decided to use Recurrent Neural Networks (RNN). Therefore, we decided to use modified RNN architectures based on Long short-term memory (LSTM) cells.

A key component of the LSTM cell-based architecture is the state of the cell. It goes directly through the whole cell, interacting with several operations. The information can easily flow on it, without any changes. However, LSTM can remove information from the cell state using filters. Filters allow skipping information based on some conditions and consist of a sigmoid function layer and element-multiplication operation. LSTM is well-suited to predict time series given time lags of unknown duration. It trains the model by using back-propagation.

4.2 Comparison of classical Machine Learning and Federated Learning

To verify the suitability of implementing FL in the AGV-based production environment, we decided to compare the effectiveness of three virtual clients trained with different parts of the training data set to the effectiveness of Federated Learning. For the FL-based approach, the model was obtained as a result of averaging the weights of neural networks of these clients.

The whole experiment was organized as follows:

1. We divided the whole data set into four parts. Three parts were used to conduct training on different virtual devices (using the LSTM). The fourth part of this data set was used to test the effectiveness of models.
2. On each IoT device (virtual client), we conducted the training and saved the trained model in the form of weights of neural networks.
3. The models of these three virtual devices were transferred to a separate device (which played the role of the general knowledge base), which averaged the models and created a global model based on the experience of all devices.
4. Local models on virtual devices were updated to a global model.
5. Based on the global model, we predicted the temperature of the device for a particular timestamp.

Our experiments also allowed us to compare the effectiveness of local models on virtual clients and global models obtained through Federated Learning. To verify the effectiveness of the built models, we used several metrics, including *Mean Squared Error* (MSE), *Mean absolute percentage error* (MAPE), and *Root Mean Squared Error* (RMSE). The effectiveness of the local models for virtual client 1, client 2, client 3 and the global model is shown in Fig. 5, Fig. 6, Fig. 7, and Fig. 8, respectively. We can observe that client 2 (Fig. 6) provides the best prediction results. The curves for the predicted and actual temperature are following a similar path. The MSE, MAPE, and RMSE are on the low level, which proves that this client predicts the temperature well. The results provided by clients 1 and 3 are not so good as for client 2. Especially above the timestamp 1,500, the temperature prediction is much worse, which is also visible in Figs. 5 and 7 and the values of the error metrics.

In order to see the difference in accuracy between all the models in more detail, we decided to show them all in one Fig. 9. The results show that the

Mean Squared Error (MSE) = 39.97
 Mean absolute percentage error (MAPE) = 6.02 %
 Root Mean Squared Error (RMSE) = 6.32

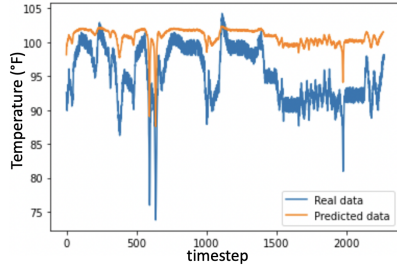


Fig. 5. Effectiveness of the local model for the virtual client 1.

Mean Squared Error (MSE) = 11.81
 Mean absolute percentage error (MAPE) = 3.02 %
 Root Mean Squared Error (RMSE) = 3.44

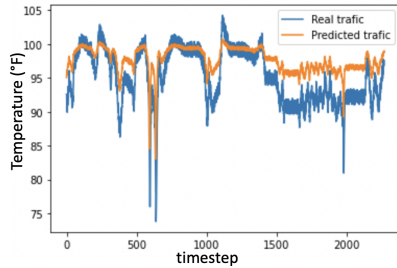


Fig. 7. Effectiveness of the local model for the virtual client 3.

Mean Squared Error (MSE) = 4.74
 Mean absolute percentage error (MAPE) = 1.91 %
 Root Mean Squared Error (RMSE) = 2.18

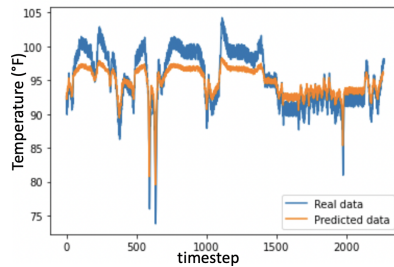


Fig. 6. Effectiveness of the local model for the virtual client 2.

Mean Squared Error (MSE) = 9.43
 Mean absolute percentage error (MAPE) = 2.74 %
 Root Mean Squared Error (RMSE) = 3.07

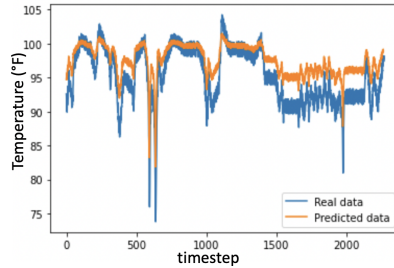


Fig. 8. Effectiveness of the global model.

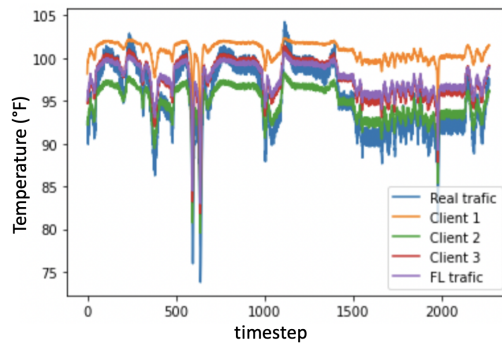


Fig. 9. Comparison of the prediction effectiveness of local models and the global model with real data.

accuracy of the prediction for the global model has increased compared to local models of virtual clients. In particular, we can see the most significant increase for the first client. Due to learning the neural network only on local data, the MSE was equal to 39.97. After averaging the models of three virtual clients and obtaining a global model, the MSE decreased to 9.43, which indicates better model performance. For the third client, the improvement of effectiveness is not so significant, but before the update of the prediction model, the value of MSE was equal to 11.81. For the second client, the value of MSE before updating the global model was 4.74. This result indicates that this client carried most of the valuable information at the time of testing. It could learn based on the most appropriate cases to predict the temperature level adequately. In contrast, clients 1 and 3 (for which the effectiveness is shown in Figs. 5 and 7) seem not to have many occasions to learn correctly, and thus, their prediction results are not perfect. As a result, the second client shared his experience with other clients, making the global model predictions for the test data set more accurate. However, we can also see that the aggregated experience includes also aggregated errors. This is visible in Fig. 9 for timestamps above 1,500, where we can observe the increased prediction error between the real temperature and the one that was predicted by the FL global model. The FL global model aggregates the wrong experience from clients 1 and 3, and this resulted in imperfect (but still better than for client 1 and 3) global model prediction accuracy in this period.

5 Discussion and Conclusions

Federated Learning is currently being actively integrated into Industry 4.0. In smart production, responding to changes in real-time is very important to ensure uninterrupted operation. Predictive Maintenance is used to predict anomalies and breakdowns in production. The more data is available, the more accurate the detection of anomalies and prediction of failures. However, managing such data requires the integration of efficient and secure mechanisms for data exchange between intelligent production devices. In order to provide a secure exchange of experience between smart devices both within one production and between different production environments, we proposed the use of Federated Learning. It provides the maximum safety for industrial data and allows increasing the effectiveness of predicting time-series parameters for big industrial machines or AGVs. In [14], the authors proposed to use a two-level FL architecture based on AI on the local servers, which is well suited for a static production line, demonstrating the benefits of such architecture for their case. However, in our case, we are dealing with AGVs that move independently in production. In this case, it is more appropriate to use the architecture of FL based on AI on the on-board IoT devices, which will provide a deeper understanding of the production environment for AGVs. Our results also show that despite aggregating some prediction errors the accuracy of predicting time-series parameters of the device increases after sharing experiences between AGVs. We have tested the proposed model on virtual clients and conducted experiments to evaluate the effectiveness

of Federated Learning. The results show that the overall accuracy of prediction among all virtual clients is increased, which allows better detection of anomalies in autonomously controlled devices and leads us to the conclusion that this approach can be deployed on the AGVs, like the Formica-1 we smarticize.

Acknowledgements The research was supported by the Norway Grants 2014-2021 operated by the National Centre for Research and Development under the project “Automated Guided Vehicles integrated with Collaborative Robots for Smart Industry Perspective” (Project Contract no.: NOR/POL-NOR/CoBotAGV/0027/2019-00), the Polish Ministry of Science and Higher Education as a part of the CyPhiS program at the Silesian University of Technology, Gliwice, Poland (Contract No.POWR.03.02.00-00-I007/17-00), and by Statutory Research funds of the Department of Applied Informatics, Silesian University of Technology, Gliwice, Poland (grants no. 02/100/BKM21/0015, BKM/RAu7/2022 and 02/100/BK_22/0017).

References

1. Ahmad, S., Lavin, A., Purdy, S., Agha, Z.: Unsupervised real-time anomaly detection for streaming data. *Neurocomputing* **262**, 134–147 (2017). <https://doi.org/https://doi.org/10.1016/j.neucom.2017.04.070>, <https://www.sciencedirect.com/science/article/pii/S0925231217309864>, online Real-Time Learning Strategies for Data Streams
2. Coleman, C., Damodaran, S., Deuel, E.: Predictive maintenance and the smart factory. Deloitte University Press (2017)
3. Cupek, R., Drewniak, M., Fojcik, M., Kyrkjebø, E., Lin, J.C.W., Mrozek, D., Øvsthus, K., Ziebinski, A.: Autonomous guided vehicles for smart industries – the state-of-the-art and research challenges. In: Krzhizhanovskaya, V.V., Závodszyk, G., Lees, M.H., Dongarra, J.J., Sloot, P.M.A., Brissos, S., Teixeira, J. (eds.) *Computational Science – ICCS 2020*. pp. 330–343. Springer International Publishing, Cham (2020)
4. Essien, A., Giannetti, C.: A deep learning model for smart manufacturing using convolutional lstm neural network autoencoders. *IEEE Transactions on Industrial Informatics* **16**(9), 6069–6078 (2020). <https://doi.org/10.1109/TII.2020.2967556>
5. Klein, P., Bergmann, R.: Generation of complex data for ai-based predictive maintenance research with a physical factory model. In: Gusikhin, O., Madani, K., Zaytoon, J. (eds.) *Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics, ICINCO 2019 - Volume 1*, Prague, Czech Republic, July 29-31, 2019. pp. 40–50. SciTePress (2019). <https://doi.org/10.5220/0007830700400050>, <https://doi.org/10.5220/0007830700400050>
6. Kotsiopoulos, T., Sarigiannidis, P., Ioannidis, D., Tzovaras, D.: Machine learning and deep learning in smart manufacturing: The smart grid paradigm. *Computer Science Review* **40**, 100341 (2021). <https://doi.org/https://doi.org/10.1016/j.cosrev.2020.100341>, <https://www.sciencedirect.com/science/article/pii/S157401372030441X>

7. Malawade, A.V., Costa, N.D., Muthirayan, D., Khargonekar, P.P., Al Faruque, M.A.: Neuroscience-inspired algorithms for the predictive maintenance of manufacturing systems. *IEEE Transactions on Industrial Informatics* **17**(12), 7980–7990 (Dec 2021). <https://doi.org/10.1109/tii.2021.3062030>, <http://dx.doi.org/10.1109/TII.2021.3062030>
8. McMahan, B., Ramage, D.: Federated learning: Collaborative machine learning without centralized training data. *Google Research Blog* **3** (2017)
9. Pech, M., Vrchota, J., Bednář, J.: Predictive maintenance and intelligent sensors in smart factory: Review. *Sensors* **21**(4) (2021). <https://doi.org/10.3390/s21041470>, <https://www.mdpi.com/1424-8220/21/4/1470>
10. Sharp, M., Ak, R., Hedberg, T.: A survey of the advancing use and development of machine learning in smart manufacturing. *Journal of Manufacturing Systems* **48**, 170–179 (2018). <https://doi.org/https://doi.org/10.1016/j.jmsy.2018.02.004>, <https://www.sciencedirect.com/science/article/pii/S0278612518300153>, special Issue on Smart Manufacturing
11. Ullrich, G.: The history of automated guided vehicle systems (2015)
12. Wang, J., Yan, J., Li, C., Gao, R.X., Zhao, R.: Deep heterogeneous gru model for predictive analytics in smart manufacturing: Application to tool wear prediction. *Comput. Ind.* **111**, 1–14 (2019)
13. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: Concept and applications (2019)
14. Zhang, Y., Li, X., Zhang, P.: Real-time automatic configuration tuning for smart manufacturing with federated deep learning. In: Kafeza, E., Benatallah, B., Martinelli, F., Hacid, H., Bouguettaya, A., Motahari, H. (eds.) *Service-Oriented Computing - 18th International Conference, ICSOC 2020, Dubai, United Arab Emirates, December 14-17, 2020, Proceedings. Lecture Notes in Computer Science*, vol. 12571, pp. 304–318. Springer (2020). https://doi.org/10.1007/978-3-030-65310-1_22, https://doi.org/10.1007/978-3-030-65310-1_22