MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies

Andy Ludwig\textsuperscript{1,2}, Michael P. Heinl\textsuperscript{1,2}, Alexander Giehl\textsuperscript{1,2}

\textbf{Abstract:} The digitization of shop floors opens up opportunities for innovative applications and business models due to the vast amount of generated data. However, a lot of this potential is currently not utilized because companies consider the risk of data sharing as too high compared to the corresponding benefit. Focusing on the machine tool sector, the research project MINERVA addresses these concerns by experimentally repurposing privacy-enhancing technologies as confidentiality-protecting technologies and applying them to the use case of condition monitoring to protect intellectual property and other information deemed critical by machine tool operators. Thereby, MINERVA's goal is to reduce the risk of data sharing and support the establishment of data-driven business models in the machine tool sector in the long term.

\textbf{Keywords:} Machine Tool Data; Confidentiality-Protecting Technologies; Privacy-Enhancing Technologies; Industrial Internet of Things; Defense-in-Depth; Supply Chain Security

\section{Introduction}

Industry 4.0, the digitization and interconnection of shop floors, leads to a steadily increasing amount of production-relevant data. This data has a large potential which the machine tool industry leverages only in parts [Ve21]. Applications such as condition monitoring or predictive maintenance are currently used mainly for single or few machines on the local shopfloor. In order to fully harness the data's potential and to build a broad basis for data-driven business models, the data has to be aggregated and analyzed across company borders. However, this data-driven innovation is hindered by the concerns of many machine tool operators who worry to suffer a competitive disadvantage due to data sharing.

\section{Objectives}

MINERVA addresses this conflict by creating a secure and transparent edge and cloud architecture for the Industrial Internet of Things (IIoT). In contrast to existing architectures,
MINERVA technologically underpins the machine tool operators’ data sovereignty by applying Privacy-Enhancing Technologies (PETs) as an additional layer of defense. This corresponds to the widespread paradigm of defense-in-depth promoted by the established ISA/IEC 62443 series of standards [IE09] covering industrial security. Condition monitoring, which is highly relevant to the industry partners, serves as a tangible use case. For this, suitable Machine Learning (ML) / Federated Learning (FL) algorithms are used to train models in the cloud using “anonymized” data protected by PETs. PET parameters will be selected in accordance with the use case, also considering potential for automation, such as in the fine-tuning of Differential Privacy (DP). Subsequently, these models are transferred back to the shop floor, where they are used to assess the machines’ condition. In the medium term, the industry partners can use collaboratively trained ML models without having to disclose sensitive data. The long term goal is to strengthen the trust of the entire machine tool industry in data-driven business models. Since MINERVA does not primarily use PETs to protect privacy due to the lack of Personally Identifiable Information (PII) but rather to protect confidentiality of industrial data, the term Confidentiality-Protecting Technology (CPT) is proposed and from now on used instead of PET in order to semantically match its purpose. For the same reason, the term additionally protected will be used instead of anonymized. Currently, MINERVA is in an early phase of development and the analysis of potential CPTs beyond the few explicitly mentioned during the course of this paper is part of the ongoing work.

3 Related Work

In security research, data privacy is an important area due to the dilemma between data-driven functions and the risks associated with data disclosure [CGL20]. CPTs are possible countermeasures that have been applied in different use cases [DB20; Th23; TM21]. Ensuring privacy in the context of big data is currently one of the main challenges [Cu21]. There are few published research items in the specific field of data sovereignty in Industry 4.0. For example, the industrial data space concept describes an implemented platform but does not incorporate common CPTs [Ot16]. There are also platforms for collaborative data usage, but not in the area of Industry 4.0 [Kh21]. However, future research directions have been suggested in this context [Ca19]. The importance of anonymization models in Industry 4.0 research is increasing [Fu10; Ji21]. DP has gained attention in this regard [HRC19; Hu21] and there are different developments due to the necessary adaptation for each use case [Fu10]. Advantages of DP include the ability to set an explicit privacy level due to its mathematical definition as well as its real-time capability [DR14; Dw08] which significantly increases the acceptance of DP [GHB21; Gi19]. Failure to apply data privacy models to machine data may lead to the reconstruction of product geometry, resulting in a loss of Intellectual Property (IP) [Gi19].

Summarized, there are basic approaches in the area of collaborative data utilization in Industry 4.0. However, there are still various unsolved issues that prevent companies from sharing their data. This is where MINERVA starts.
4 Methodology

The concept of trustworthy collaborative IIoT-as-a-service can facilitate data-driven business models. This can be achieved by implementing CPTs in a secure system architecture to prevent the loss of IP. The following sections outline the concept of trustworthy collaborative usage of machine tool data. The concept will be applied to the use case of condition monitoring for machine tools, in particular milling machines. Figure 1 schematically illustrates the planned workflow which is also described in the following sections.

4.1 Data Collection from Machine Tool

First, the local data of machine tools is collected and processed unprotected in the corresponding data lake of the edge device. For instance, this data contains the coordinates of the tool or specific forces over time. This can be enriched using sound sensors attached to the machine. Structure-borne noise data is an additional input for condition monitoring algorithms. The larger quantity of data allows a more detailed analysis of processes within the machine. The local data needs to be labelled for later usage of ML algorithms like condition monitoring. For this purpose, a human-machine interface at the edge device is necessary, allowing employees to assess the machine conditions. In general, the labels do not need to be determined throughout the entire life cycle or operational use but only during the training process at the beginning. Automated support for the labelling decision may be possible but will be conducted later, which further simplifies the collection of machine states. In addition to the machine condition, the corresponding data criticality must be determined. The criticality level is essential for applying CPTs with suitable parameters to the data in order to reach an appropriate level of protection.

4.2 Application of CPTs

Depending on the associated data criticality level, a suitable CPT is applied to the data in the edge device of the machine tool within the company boundaries. This additional protection strengthens the owner’s data sovereignty and reduces the risk of losing IP. The impact of the CPT must be reliable and comprehensible. In cases where a company utilizes multiple machine tools, a local server can collect all the data and apply the CPT in an aggregated manner. The selection of appropriate CPTs depends on various factors, including the level of data criticality, basic suitability of data, its layout, and finally, the compatibility with subsequently applied ML algorithms. Furthermore, a synchronisation layer must be established between all participants. If each company can set data criticality independently, data could be preprocessed in different ways. Either the cloud service can handle these differences in data quality and format or a policy has to restrict the pool of possible CPTs.
4.3 Cloud Communication and Collaboration

After the preprocessing, the data can be transmitted to a central entity, where all data from all participating machine tool operators is aggregated. This comprehensive data set can be used to train ML models for specific use cases. A server collecting all data represents an attractive target for attackers. Although the usage of CPTs to protect data is an additional layer of defense, the infrastructure must also be hardened against attacks. State-of-the-art security mechanisms are necessary to protect not only the integrity and confidentiality of the data itself but also the services ingesting and processing the data. These objectives can be in parts accomplished through the utilization of other types of CPTs, such as Trusted Execution Environments (TEEs) or group signatures.

For instance, the secure infrastructure must include an authentication process, allowing only known and trustworthy partners to participate and contribute data for training purposes because data poisoning attacks are a potential risk for the system, leading to erroneous model results. However, what seems to be a straightforward task to be solved by established technology such as Public Key Infrastructure (PKI) can involve a couple of challenges. First of all, there has to be a PKI which is trusted by all participants. Since the operator of such a PKI represents a single point of failure, utmost care during its selection [He19] and compliance with special requirements [He23] are crucial. In order to establish an additional layer of defense against compromises involving information extraction attacks, IP should be separated from the participants’ identities or the latter be protected by the usage of anonymous credentials. At the same time, this measure increases the risk of poisoning attacks conducted by untrustworthy or unnoticedly compromised participants. Therefore, a ring signature-like mechanism might be employed to establish a secure channel with a certain degree of anonymity which can, however, be revoked in case of misuse.

4.4 Leveraging the Model in Companies

Using the same secure channel, the model which has been collaboratively trained in the cloud can be transmitted back to each participating company. They can use the model without accessing the input data which enables each participant to benefit from sharing their data while at the same time protecting it from competitors or adversaries. Local data stored within company boundaries can be classified using the model without establishing a connection to external partners. Depending on the use case, a repeated transfer of new training data as well as the generated model is possible. Additionally, feedback loops must be implemented to increase model performance.

5 Conclusion

A major challenge of sharing data across company borders is the loss of IP. A possible threat is the competitors’ capability to reconstruct specifics about a work piece. As a result,
companies are torn between optimizing their production flow and the fear of disclosing internal knowledge. Additionally, aggregated data at a central point, such as a cloud server, represents an attractive target for adversaries because one successful attack can result in the compromise of data from a plethora of companies (so-called supply chain attack). Generally, two main attacker models can be distinguished: an attack on intellectual property, which could also be conducted by an honest but curious participant. Additionally, the data can be compromised in its integrity, leading to a distorted model.

CPTs may provide a comprehensive solution. If each company maintains data sovereignty, the risk of IP loss by sharing data can be reduced. CPTs can be directly applied to data within the company boundaries. Afterwards, only additionally protected data is transferred to the cloud. This approach will be combined with a secure, transparent, and reliable data infrastructure between each company and the cloud. Possible application areas include improved energy consumption or reduced machine tool down times through the use of algorithms for condition monitoring or predictive maintenance. Detecting and eliminating product weaknesses through the implementation of these algorithms can lead to optimization for component suppliers or machine manufacturers.

The overall goal of reducing the machine tool operators’ concerns regarding data sharing are evaluated by a survey taking place at the beginning and once again at the end of the project duration after presenting the project results to the survey participants. Finally, potentials to transfer the results to other areas will be identified to generally increase the willingness to collaboratively use data for the good of all.

Fig. 1: Planned workflow: (1) Data Collection from Machine Tool; (2) Application of CPTs; (3) Cloud Communications and Training of Condition Monitoring Algorithm; (4) Using the Model in Companies.
Acknowledgement

This work was supported by the German Federal Ministry of Education and Research (BMBF) under grant number 16KIS1803K.

References


