Protecting Intellectual Property in a Cloud Manufacturing Environment: Requirements and Strategies

Yuqian Lu, Xun Xu

Protecting intellectual property in a cloud manufacturing environment: requirements and strategies

Yuqian Lu, Xun Xu

Department of Mechanical Engineering, The University of Auckland, Auckland, New Zealand
ylu633@aucklanduni.ac.nz, x.xu@auckland.ac.nz

Abstract. In today's knowledge economy, intangible knowledge assets have become the key drivers of organisational success. Protection of intellectual properties for all parties is a challenging issue in cloud manufacturing environment. This paper focuses on the protection of intellectual property in the cloud manufacturing environment. Several strategies for protecting intellectual properties are proposed in this paper. In addition, a privacy enhanced business interaction mechanism is presented. Furthermore, this paper discusses some practical technologies in the cloud context.

Keywords: Cloud manufacturing, Intellectual property protection, security policy

1 Introduction

In recent years, cloud manufacturing has been regarded as a novel way of organising fast collaborative product development [1]. Cloud manufacturing is a service-oriented business model, whereby distributed manufacturing resources are encapsulated as consumable services over the Web [2]. This business model is anticipated to bring unique opportunities; it turns a capital investment model (of a typical manufacturing business) into a recurring expenditure model. In the ever-increasing distributed, networked and crowd-sourced cloud environment, the protection of intellectual property (IP) is a critical challenge.

World Intellectual Property Organisation (WIPO) [3] gave the definition of intellectual property as "inventions, literary and artistic work, symbols, names, images, and designs used in commerce." IP contains two categories [3]: industrial property and copyright, both of which can be represented by intangible proprietary information. In cloud manufacturing environment, IP refers to the confidential information (product design, process, etc.) of industrial design and manufacturing. Therefore, the main objective of IP protection is to prevent leakage of confidential information in cloud manufacturing environment.

One of the prerequisites for cloud manufacturing is to share product information, which is the core IP of some businesses. Therefore, it is very likely that participants will face a dilemma in trying to balance protection of intellectual capital with the openness and information sharing needed to successfully carry out the joint tasks. To the best knowledge of authors, there has not been a satisfactory solution for protecting

IP in cloud manufacturing environment, though some studies investigated the security [1] [4] and user privacy [2] issues.

This paper focuses on the protection of intellectual property in the cloud manufacturing environment. The emphasis is placed upon proposing a feasible mechanism to ensure the privacy of confidential information from service consumers and service providers. The reminder of this paper is organised as follows. The next section presents a brief discussion on the significance of IP protection in a cloud manufacturing environment and reviews related approaches reported in the literature. Section 3 proposes several strategies for maximum protection of IP from all parties in cloud manufacturing environment. Following these strategies, a privacy enhanced business process is also proposed. Section 4 further discusses the enabling technologies for IP protection. Section 5 summarises the outcomes of this research and discuss future trends.

2 Significance of IP protection

The existing research on cloud manufacturing has recognised the significance of data security and user privacy in a cloud manufacturing environment. However, there is very little work on these aspects. This section summaries the significance of IP protection by analysing the pain point for each party in the cloud and reviews the existing approaches.

2.1 Requirements on IP protection

In cloud manufacturing, there are two fundamental business roles, namely service consumers and service providers (Fig. 1). Consumers request manufacturing services from the cloud, whereas service providers receive orders or sub-orders from the cloud system by outsourcing resources [2].

Fig. 1. High-level business interactions in cloud manufacturing [2]

From the technical perspective, requests from service consumers should contain the specifications of a product design, which is often in a form of computer aid manufacture file (like .dxf file for 2D design and .asm file for 3D design). After a design file is uploaded to the cloud, it will be sent to potential service providers for assessment and then some of them will be selected as the service providers. This process inevitably discloses product design to unwanted parties in the cloud. On the other hand, intelligent cloud systems require manufacturing resources being connected to

the cloud and production activities being monitored all the time. In addition, some of the proposed system frameworks even ask service providers to provide detailed machining operations to the cloud for simulation and cost estimation purposes. In fact, this is not a good practice for manufacturers. Knowledge on optimal machining processes is often regarded as intangible assets of a business. Storing this information on a remote server potentially put it at risk.

It has to be noted that the cloud manufacturing environment is a much more open environment than traditional PLM environment. In cloud manufacturing, model models, resource capability information and other business-critical information are all stored remotely in the cloud. For a manufacturing project, a global search and match process of task-service pairs is required to be carried out. In contrast, in the conventional PLM environment, there is a clear closed boundary for product data and knowledge exchange.

In summary, the requirements around IP protection in cloud manufacturing can be extracted as follows:

1. Complete product designs can only be seen by authorised users.
2. Complete product designs can only be visible to confirmed service providers.
3. Only a minimum amount of data should be sent to relevant service providers.
4. Exclusive know-how about manufacturing resources should not be visible to service consumers.

These basic requirements should be taken as ground rules when designing a manufacturing cloud.

2.2 Approaches to achieving data security and IP protection

Data security is one of the bottlenecks that hinders the application of cloud manufacturing [2]. The security and privacy management in cloud manufacturing environment is still in the early stage. This is because things are more complicated in cloud manufacturing environment. Xu [1] point out that manufacturers are more concerned about the confidentiality and privacy of their data.

Lu et al. [2] discussed the importance of authorisation mechanisms for resource access in cloud environment. Resource sharing in cloud manufacturing is conditional: each service provider makes resources available, subject to constraints on who, when, where and what can be done. Access policies change dynamically over time, in terms of the resources involved, the nature of the access permitted, and the participants to whom access is available. A semantic web-based approach is proposed for setting resource access policies. By defining unique sharing policies for each manufacturing resource, enhanced privacy can be achieved as only authorised users can have access to a service in the cloud.

Kim et al. [5] proposed a multi-level modelling technique based on feature-based modelling and mesh simplification to enable information protection in computer-aided collaborative design. The techniques are integrated with an access control mechanism to enable role-based user authorization. In a more recent research, Deng et

al. [6] proposed an original approach to decompose product structures for the purpose of controlling IP leakage risk in supply chains using design structure matrix.

Following the notion of information partition in collaborative environment, Wang and Xu [7] proposed a product data exchange mechanism based on STEP/STEP-NC data models to provide information with the right level of detail to partners in a supply chain. In this mechanism, data extracting algorithms were developed to generate data packets.

3 IP protection strategies for cloud-based business interaction

This section discusses the overall strategy for preventing IP leakage in a cloud-based environment. As this is a new topic in cloud manufacturing research, we first present some general rules for protecting IP and then examine how rational business processes can enhance data confidentiality.

3.1 Rules of thumb for protecting IP in cloud environment

As mentioned earlier, service consumers send product designs to the cloud for matched manufacturers. This process can potentially put product designs at risk. Similarly, service providers need to detail the capability of manufacturing resources, which can disclose manufacturing know-how to other parties. In addition to diffusing critical knowledge, the open environment may allow a partner a window to gauge the strengths, weaknesses, and strategic orientation of its competitors, providing advantages in future competition with them. Therefore, this issue put service consumers and service providers in a dilemma in trying to balance protection of intellectual capital with the openness and information sharing needed to successfully carry out the product development tasks.

In terms of approaches to securing intellectual property, the most common strategy is the trusted-entry approach. This approach only works well for the first tier of trusted partners; the control of document is lost as the production activities move farther to multiple tiers of suppliers. Nevertheless, there are still some general rules to follow in complex engineering environments, especially in cloud manufacturing environment.

It is best to share as little information as possible for all the parties in cloud manufacturing. This means for service consumers, it is better to outsource only peripheral items, keeping all core IP at home. Even for a product design, it is not necessary to share all the details with manufacturers at the bid point. Only a simplified version of the product manufacturing information is required for potential manufacturers to tell if they are able to take the job. For service consumers, they only share a minimum amount of information for resource description and service monitoring. The detailed manufacturing processes for a task cannot be disclosed to other parties.

A second strategy is to break up the IP – not giving all of it to any one business entity, which is especially critical for service consumers. In other words, a cloud manufacturing system should balance the centralisation of manufacturing activities with the separation of whole IP into multiple pieces. The optimal scenario is to let a contract

manufacturer see one part of the overall design and give it only the information needed to do the job.

3.2 Privacy enhanced business process in cloud environment

Following the above strategies, we highlighted the critical business processes requiring special attention on IP protection in cloud manufacturing as in the following UML sequential diagram (Fig. 2). This business process is a simplified version of the business interaction process in [2].

A typical service provision process is as follows. A service consumer submit a service request to the cloud by uploading a customised design file. This design file is often in a computer-aided manufacturing file, such as .dxf file, .step file and .asam file. During this process, the membership management module checks the identity of the service consumer before sending a request to the request processing module. The request processing module provides a comprehensive analysis for service requests by comparing new service request with historical data. The manufacturability of a service request is assessed in this process, and thereafter a response is sent back the service consumer. If a service request passes the assessment process, the PMI (Product Manufacturing Information) parser in this module is triggered to convert the product information in user-uploaded file into a simplified PMI file following an abstract product data model. This process is critical to the protection of product designs as only abstract PMI information is extracted for down-stream decision-making processes. This abstract file only contains a small portion of the original product data that is enough for manufacturing resource selection. Once this PMI file is generated, it will be sent to the knowledge base for resource searching and matching. When feasible manufacturing resources are outputted, the service composition module goes through all the possible combinations of service units and the best solutions are send to the service consumer for reviewing. Once the service consumer confirms the final decision, the detailed product designs will be passed to participated service providers for service provision. It has to be noted that in this process, only the right amount of information will be send to service providers. The data a service provider receives is only enough for processing the anticipated tasks. On the other hand, a service provider updates available manufacturing resources in the knowledge base by changing their physical descriptions and working schedule. Manufacturing know-how regarding a specific manufacturing resource is not part of the required descriptive information.

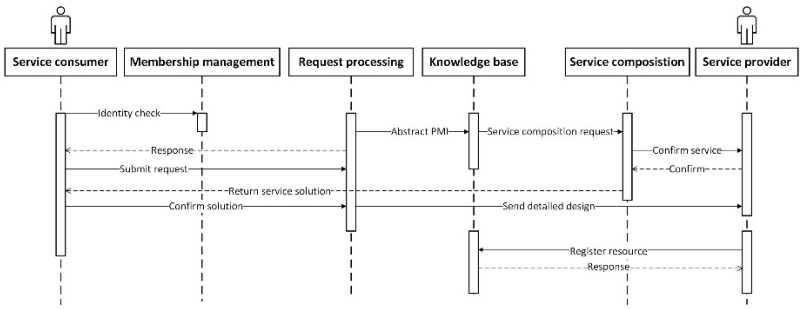

Fig. 2. Simplified business process in cloud manufacturing environment

4 Enabling technologies for IP protection

The business processes in Fig. 2 reveal that there are at least two technological challenges to be addressed for protecting intellectual properties in the cloud environment. These challenges are (1) developing a unified data model to represent abstract PMI information, and (2) developing a unified scheme for representing manufacturing resources without disclosing detailed manufacturing process for each resource.

4.1 Data model for simplification of product design

The most straightforward approach for protecting IP in a product design is to hide the detailed geometrical information in a design. Feature-based approach can be a potential solution. Feature technology is integral to the integration of CAD/CAM. This is because almost all CAPP systems function on the basis of features. One critical step in process planning is to covert a geometric model of lower-level entities (lines, points, etc.) into a feature based model of higher-level entities (holes, pockets, etc.). Hence, there is a need to develop a description model for all the manufacturing features. Parameters on all the machining features of a product are the main data that are required for selecting the right manufacturing resources. This means a mechanical part is described as a combination of a list of elementary machining features. For each of the machining features, the required attributes are the information merely sufficient for determining feasible manufacturing resources that can be used to carry out the required machining process. This approach potentially reveals little information about the geometry of a part.

Manufacturing features can be classified by means of manufacturing processes, namely milling feature, turning feature, and holemaking feature. There are several machining features under each category. For example, milling features include pocket, slot, planar surface, chamfer, etc.

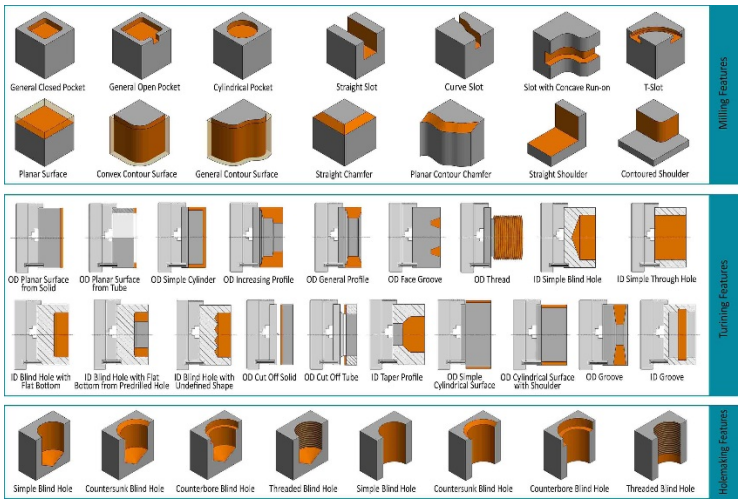

Fig. 3. Classification of machining features

Feature-based product description creates a way of meta-data modelling for service requests. It has to be noted that the feature-based approach introduced in this paper is different from the feature-based approaches used in commercial CAPP systems or STEP-NC data format. In STEP-NC file, features are still in geometrical representation. For instance, for the feature of General outside profile, the contour of the spare is given by the attribute feature_boundary, which is a type of profile. This means the detailed shape of a profile is still given in a STEP-NC file. In contrast, in the meta-data model the definition of a profile only pays attention to the minimum radius in the concave corner, which is one of the critical attributes for selecting feasible cutters. Figure 4 gives an overview of the level of detail for three different data description methods. CAD files contain all the details of a product design. STEP-NC file simplifies the product design, neglecting the detailed geometry of an overall workpiece and some geometry information of some features. This could compress a CAD file to 80% of its original volume. If these machining features are further simplified as only providing the key information for selecting manufacturing resources, the whole file can be compressed down to 50% of its original volume. In this way, most of the geometrical information of a product design is removed, and the associated core IP is protected.

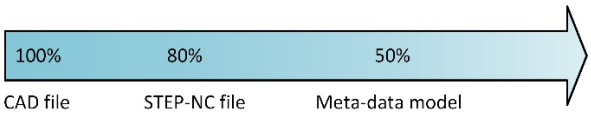

Fig. 4. Level of details for different data description methods

4.2 Description framework for resource virtualisation

Protecting the IP associated with a manufacturing resource is equivalently important. One feasible approach is to exclude manufacturing know-how and detailed manufacturing process as part of the description model. The description of a manufacturing resource should include its technical properties and functional capabilities. Take CNC milling machine as an example. Technical properties include its manufacturer, manufacturer instructions, machining envelope, control system, maximum spindle speed, mass, etc., whereas functional capabilities include planar face milling, 3D free-form surface milling, drilling, boring, pocketing, etc. These data should be all the information for describing a manufacturing resource.

5 Conclusions

Intellectual property protection is critical to business success in cloud manufacturing environment. This paper analysed the requirements of intellectual property protection in cloud manufacturing environment and proposed some strategies for preventing IP leakage. Furthermore, several technological approaches were proposed for implementing a privacy enhanced cloud manufacturing environment. In general, it is best to share as little information as possible for all the parties in cloud manufacturing. This means for service consumers, it is better to outsource only peripheral items, keeping all core IP at home. For a product design, only the information for selection of manufacturing resources can be disclosed at the bid point. For service consumers, they only share a minimum amount of information for resource description and service monitoring. A second strategy is to break up the IP – not giving all of it to any single business entity.

References

1. Xu, X., *From cloud computing to cloud manufacturing.* Robotics and Computer-Integrated Manufacturing, 2012. **28**(1): p. 75-86.
2. Lu, Y., X. Xu, and J. Xu, *Development of a Hybrid Manufacturing Cloud.* Journal of Manufacturing Systems, 2014. **33**(4): p. 551-566.
3. Organization, W.I.P., WIPO Intellectual Property Handbook: Policy, Law and Use. 2004.
4. Liu, X., et al., *Enhancing the security of cloud manufacturing by restricting resource access.* Journal of Homeland Security and Emergency Management, 2014. **11**(4): p. 533-554.
5. Kim, T., et al., Multi-Level modeling and access control for data sharing in collaborative design. Advanced Engineering Informatics, 2006. **20**(1): p. 47-57.
6. Deng, X., et al., Product decomposition using design structure matrix for intellectual property protection in supply chain outsourcing. Computers in Industry, 2012. **63**(6): p. 632-641.
7. Wang, X.V. and X.W. Xu, *A collaborative product data exchange environment based on STEP*. International Journal of Computer Integrated Manufacturing, 2015. **28**(1): p. 75-86.