Secure Cloud Manufacturing: Research Challenges and a Case Study

Weichao Wang[1], Yu Wang[2], Wesley Williams[3], and Aidan Browne[3]

[1] Department of Software and Information Systems, UNC Charlotte
weichaowang@uncc.edu
[2] Department of Computer Science, UNC Charlotte yu.wang@uncc.edu
[3] Engineering Technology and Construction Management, UNC Charlotte
wbwillia@uncc.edu, aidanbrowne@uncc.edu

Abstract. Cloud manufacturing (CM) is an open and service-oriented platform that virtualizes distributed design, manufacturing, and assembling resources together in order to provide a seamless, stable, and high quality transaction of manufacturing procedures. Despite the rich results in resource discovery and matching, the research in robustness and security of the systems falls behind in many aspects. The lack of such knowledge puts a serious challenge for the wide deployment and adoption of cloud manufacturing, which becomes an urgent demand for the sustainability of economy. To bridge this gap, we plan to investigate security of cloud manufacturing. As a specific example, in this paper we will discuss potential vulnerabilities of cloud manufacturing to side channel attacks and design defense mechanisms to balance user privacy and system efficiency. We propose to build a distributed manufacturing cloud prototype upon the RAMP (Remote Automation Management Project) system to form a closed loop evaluation environment. Mutual impacts between the cyber and physical sub-systems will be evaluated. Simulated cyber attacks and incidents on the shop-floor will be injected into the system to assess its security.

1 Introduction

With the fast development of cloud computing, its potential application to other fields has attracted a lot of research efforts. Cloud manufacturing [1–4] is an open and service-oriented platform that virtualizes and encapsulates distributed design, manufacturing, and assembling resources together in order to provide a seamless, stable, and high quality transaction of manufacturing procedures. Both China [1, 5] and EU [6, 7] have invested millions of dollars on related projects. In Germany, the concept is included in the platform of Industry 4.0. In United States, several projects have explored related topics such as composition of engineering services [8] and e-quality control of web-enabled manufacturing [9].

Different from the emphasis on resource discovery and capability matching in cloud manufacturing, the corresponding research in robustness and security of the systems falls behind in many aspects. As an example, the sharing of

resources in cloud environments enables side-channel attacks [10, 11]. However, to the best of our knowledge, there is no active research on the detection or defense of side channel attacks in the cloud manufacturing systems. The lack of such knowledge puts a serious challenge to the wide deployment and adoption of cloud manufacturing in the fast evolving mission critical industry [12, 13], which becomes an urgent demand for the sustainability of US economy [14, 15].

To bridge this gap, we plan to investigate security of cloud manufacturing. Since the topic of cloud manufacturing is still in its infancy stage, our discussion in this paper focuses on the problem statement and exploration of the approaches. Specifically, we will discuss potential vulnerabilities to side channel attacks during task dispatching, and design defense mechanisms to balance user privacy with system efficiency. The proposed approach could become an essential component of a unified management system in order to enforce security and robustness of manufacturing cloud.

To establish a closed-loop environment so that the proposed approaches can be assessed and further improved, the research team plan to build a distributed manufacturing and management platform upon the RAMP (Remote Automation Management Project) system [16]. Mutual impacts between the cyber and physical sub-systems will be evaluated with different threads of manufacturing tasks. Simulated cyber attacks and incidents on the shop-floor will be injected into the system to assess its security. The overall architecture of the proposed efforts is shown in Figure 1.

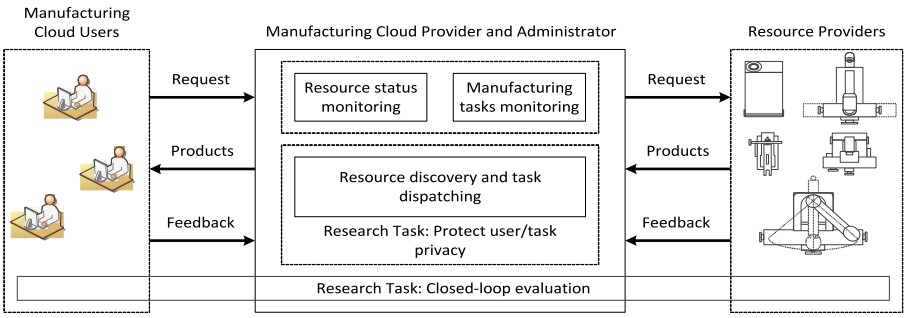

Fig. 1. Architecture of the proposed efforts.

The proposed research, if succeeds, would contribute to the technology and engineering of CPS. Sharing of resources has become a common property of multiple types of CPS. Through exploring security vulnerabilities caused by the sharing and designing defense mechanisms, we expose insights of CPS security and provide guidelines for future defense mechanisms. The remainder of the paper is organized as follows. In Section 2, we will introduce the concept of cloud manufacturing and the research challenges in security. In Section 3, we investigate the protection of user privacy from side channel attacks. Section 4 describes the development of a closed-loop evaluation platform. Finally, Section 5 concludes the paper.

2 Manufacturing Cloud and the Research Challenges

With the fast development of a global market, manufacturing jobs are now diversified by various factors including outsourcing, joint ventures, and cross-border collaborations. Nowadays we are facing a shop-floor environment geographically distributed across corporate and national boundaries. To support the required level of agility, creativity, and connectivity, the concept of cloud manufacturing is proposed. Cloud manufacturing is a customer-centric manufacturing model that exploits on-demand access to a shared collection of diversified and distributed resources. These resources (hardware, software, and knowledge) form temporary and reconfigurable production lines so that we can improve resource usage efficiency and reduce product lifecycle cost.

While the architecture of cloud manufacturing has been presented in different ways [4, 17, 18], in our research we follow the structure shown in Figure 1. Here **Users** can range from individuals to large OEMs who generate engineering requirements of the desired object and its final manufacturing conditions. The **Physical Resource Providers** own and operate manufacturing equipments. They offer users instantaneous access to manufacturing capabilities that are provided through the cloud as a service. The **Cloud Providers and Administrators** are responsible for managing all aspects of the cloud manufacturing environment and interpreting user requirements into data for production equipments. In addition to locating and matching the required resources, the application providers also need to plan for and handle service interruptions. The three groups form a closed-loop to represent the supply-demand market in cloud manufacturing.

Since the concept of cloud manufacturing is proposed, research efforts have been focusing on the construction of service infrastructure and the support of properties such as flexibility. For example, service composition represents the capability of the cloud to effectively and efficiently combine manufacturing services. Researchers have studied the problem through correlation among the virtual services [19] under multiple objectives and constraints [20]. To enable fast and accurate discovery of required services, semantic [21, 22] and ontology [23] based matching algorithms have been designed. Researchers have also designed a layered model to support service aggregation and sharing [24]. Considering the dynamic nature of cloud manufacturing, it should allow for variation in the marketplace and changes in the manufacturing environment. A Flexibility Management Architecture was proposed in [25]. LaSelle [26] suggests to use mass customization to produce unique products of varying complexity on demand.

Built upon the early advanced manufacturing models [27–30], several commercial companies have built cloud manufacturing prototype systems. For example, Quirky [31] provides virtualized manufacturing resources to distributed designers. The Ponoko system [32] offers both 3D objects and electronic components manufacturing services to designers. MFG.com [31] connects consumers with over 200,000 manufactures in 50 states so that a complete manufacturing procedure including design, quoting, production, and shipping can be accomplished at one site.

Although all the proposed architectures of cloud manufacturing [2, 3, 33, 4] treat information and infrastructure security as an essential component, the state-of-the-art research still focuses only on the engineering side. The lack of research efforts in system security and robustness, however, poses a serious challenge to future deployment and adoption of cloud manufacturing. Our proposed research tries to enhance cloud manufacturing security through information technology approaches during the task planning and production phases. The approaches will be tested in a closed-loop environment for assessment and improvement.

3 Protecting User Privacy against Side-channel Attacks in Cloud Manufacturing

Although some research efforts [33] treat cloud manufacturing as a natural extension of cloud computing, we believe the resources in CM have at least the following differences from those in cloud computing. First, while virtual machine migration in cloud computing is almost free [34], shipping of parts in cloud manufacturing causes extra delay and costs. Therefore, we have to consider the physical distances among the resource providers that we choose. Second, although in cloud computing you can interrupt and recover a virtual machine almost instantly with very little performance penalty, in cloud manufacturing it is usually very costly to interrupt a task. Last but not least, while the capabilities of the physical boxes in a computing cloud are almost the same (either CPU cycles or storage spaces), the capabilities of the manufacturing equipments vary greatly. These special properties introduce new vulnerabilities into cloud manufacturing. We propose to systematically investigate the problems and design mechanisms to strengthen the system safety.

3.1 Example Side-Channel Attacks in Manufacturing Cloud

An advantage of cloud manufacturing is the sharing of resources. Such sharing can greatly improve the equipment usage efficiency and allow middle or small scale manufacturers to conduct tasks that used to be impossible. The sharing of resources, however, also creates a channel through which malicious attackers can steal information from other users or gain advantage during the competition. Below we use two examples to illustrate the vulnerabilities and the need to strengthen the system.

Example 1: Gaining a Competitive Advantage in Business Assuming that company X and company Y are bidding for a contract and each has to produce a prototype product for the requester as soon as possible. The product needs to go through equipments A, B, and C in order. The availability of the equipments is shown in Figure 2.(a). To gain a competitive advantage, company X reserves not only the equipments A, B, and C at Factory 1 but also B at Factory 2. Now company Y can no longer find all equipments in need that are located in a single place. It may lose the contract because of the shipping

delay and cost. Please note that the extra reservation of X does not hurt the manufacturing capabilities of the overall system since all types of equipments in need are still available. Company X uses this method to gain some advantage in the competition.

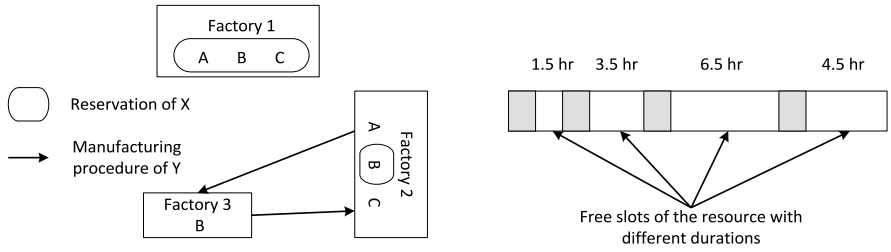

Fig. 2. Example attacks in manufacturing cloud.

Example 2: Compromising User Privacy in Manufacturing Cloud Assuming that company X is designing the next generation of $iFone$. Its competitor company Y tries to figure out whether the new design adopts a shining mirror finish or a mother-of-pearl finish. The two designs will require three and six hours of processing time respectively on a special kind of grinding machine. Through reserving the grinding machine with time gaps of different lengths and observing the time slot chosen by X, Y will be able to figure out the property of the product and compromise user privacy. For example, if Y finds out that X reserves the slot of 3.5 hours, it will know that the shining mirror finish will be adopted. The attacking procedure is shown in Figure 2.(b).

In the two attacks described above, the malicious parties take advantage of the sharing property in manufacturing cloud. The reservations of services that they make do not hurt the functionality of the system. However, they will impact the operations of other users and compromise security and privacy of the cloud. We propose to systematically investigate this problem so that we can identify the potential threats and mitigate their impacts.

3.2 Measuring the Impacts of Service Requests on User Privacy and System Safety

As the examples above show, the objective of side channel attacks is not to disable the operations of the manufacturing cloud but to derive out information about other requests or gain an advantage in competition. Therefore, traditional robustness improvement mechanisms such as multipath or alternative gear sets [35, 36] will not solve the problem. We need a mechanism that can quantify the impacts of a user request on other users' privacy and system safety at a fine granularity.

To solve this problem, we propose to design an algorithm to estimate the increases in cost and delay of satisfying a similar request in the cloud. When a user submits a request to the manufacturing cloud, the dispatching/scheduling

software will locate the resources that can satisfy the request. After reserving the resources for the transaction, the software will hypothetically submit a similar request into the system. This time, the software will estimate the cost and delay of the hypothetical request and compare them to those of the real transaction. If the increases are larger than a threshold value, the software will notify the system since this request may impact subsequent transactions in a negative way. The system will then issue a warning and keep a close eye on the subsequent requests from the same user.

While the basic idea is straightforward, several issues must be carefully studied before the approach can be deployed. The first question is to determine the appropriate range of the threshold value. We propose to use stochastic optimization to determine the threshold values for the system [37]. The perturbation analysis techniques [38] can be used to obtain consistent gradient estimates based on the simulation runs. We can experiment with different simulation configurations to explore the relationship between the studied scenarios and threshold values.

Second, we need to identify all hypothetical requests that need to be resubmitted to the system. Under many conditions, the real request and the hypothetical request do not have a one-to-one mapping. For example, in Figure 2.(a) the attacker will first reserve resources A, B, and C at Factory 1. At this moment, a hypothetical request with the same resource demand can be easily satisfied with the equipments at Factory 2. If only the current request is examined, when the attacker reserves resource B at Factory 2, no alarm will be triggered since B is still available at Factory 3. However, we can no longer find a series of resources A, B, and C that are located at a single place. Therefore, any competitors requesting these resources will be placed in a disadvantage situation. To defend against such attacks, we propose to construct hypothetical requests based on not only the current request but all open transactions from the same user. In this way, the attackers can no longer fool the system through manipulating the order of submitting requests.

The last problem is to generalize the proposed mechanisms so that they can detect collaborative attacks. So far, the proposed approach can defend against only attacks from a single malicious party. Multiple attackers can group together and jointly conduct the misbehavior. To defend against such attacks, we propose to use the classification algorithms to identify user groups based on the similarity of their requests. We will then leverage our expertise in detection of collaborative attacks [39] to refine the proposed algorithms.

3.3 Balancing Manufacturing Efficacy with Improvements in System Security

A user request to the manufacturing cloud could often be satisfied by diverse resource reservation plans. This adds some flexibility to our security enforcement mechanisms since we do not have to choose the resources with the lowest cost or shortest delay. The resource selection problem in manufacturing cloud is different from the scheduling procedures involving only one factory. Since the service

providers in a manufacturing cloud can distribute all over the world, we must take this geographical factor into consideration. We plan to build the resource allocation algorithms upon the multi-plant scheduling problem [40]. Specifically, two sets of mechanisms will be explored. In the first group, we plan to use constraint programming as the computation mechanism in collaborative scheduling and planning [41]. The flexibility of production schedules can be represented by the start times of the operations. The manufacturing cloud will resolve the conflicts caused by the constraints and generate feasible solutions to the requests.

The second group of mechanisms will treat the production planning at multiple sites with substitutable capacities [42]. A linear programming model will be developed to produce the time and capacity aggregation plan. To reduce the processing overhead at the cloud, different time grids and planning horizons for aggregation will be used. The results will then be integrated in a heuristic solution so that production and distribution planning can be jointly determined.

4 Closed-loop Evaluation with a Prototype Manufacturing Cloud

As an essential component of the proposed research, we plan to build a prototype manufacturing cloud upon the RAMP (Remote Automated Management Program) system that we already have and use at UNC Charlotte. The efforts will focus on expanding the system with the proposed security enforcement mechanisms, running closed-loop evaluation with real industrial and manufacturing equipments associated with the cloud, and investigating mutual impacts between the cyber and physical systems in the cloud.

4.1 RAMP and the Prototype Manufacturing Cloud

UNC Charlotte has been awarded by the US Department of Labor for $1.5M to develop a workforce training pipeline for mission critical operations including advanced manufacturing and smart power grid. The fund allows UNC Charlotte to establish a RAMP (Remote Automated Management Program) system that includes all software and hardware resources to be expanded to a manufacturing cloud. The architecture of RAMP and the proposed manufacturing cloud are illustrated in Figure 3.

The front side of the manufacturing cloud is managed by NetLab+ [43]. It allows remote users to login from any position. NetLab+ will create a virtual machine for every user, through which the user could reserve hardware resources. Our proposed security enforcement mechanisms will be implemented and integrated into the cloud administration software. The newly implemented component will be in charge of reservation of resources, detection of side channel attacks, and aggregation and management of the sensing data. Behind the cloud administration software will be real equipments located in two buildings on campus. The platform allows us to connect any equipment with an Ethernet interface to the system. Examples of equipments that we plan to connect to

our cloud include programmable logic controller (PLC), Siemens controllers, hydraulic trainer, and robotic arms, as shown in Figure 3. The proposed manufacturing cloud prototype will provide real-time, laboratory-based, and interactive and collaborative working experiences in advanced technical skills to researchers and students.

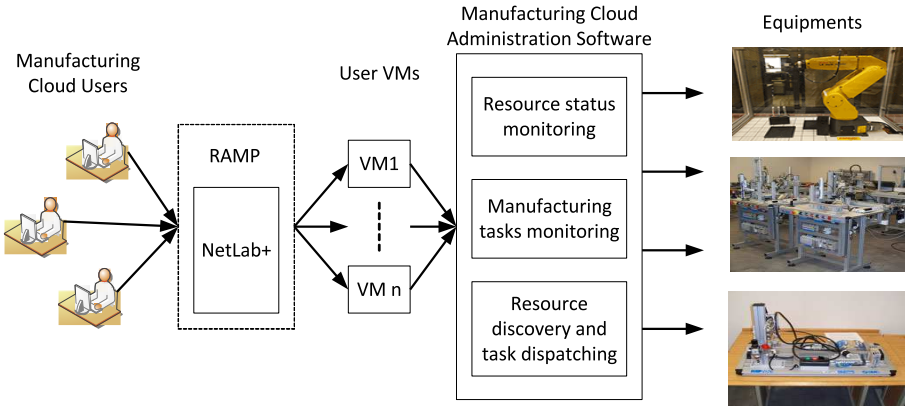

Fig. 3. Platform to evaluate our approaches.

4.2 Experiments on the Manufacturing Cloud Prototype

We plan to conduct two groups of experiments to evaluate the proposed mechanisms and the mutual impacts between the cyber and physical systems. A top-down approach [44] will be used to select parameters for evaluation. In the first group, we will articulate different resource availability and user request scenarios and submit them to the cloud administration software. The objective is to examine the impacts of the newly designed mechanisms on the overall performance of the cloud such as equipment usage efficiency, productivity, and cost and delay to users. In the second group, we will evaluate how well the proposed mechanisms can adapt to sudden changes in the cloud such as resource availability on the shop floor. While a comprehensive set of experiments will be conducted, below we describe two examples in detail.

Example Experiment 1: Mitigation of Side Channel Attacks and Protection of User Privacy In this experiment, an attacker tries to figure out the properties of another user's request. Through submitting a series of requests with different resource demands, the attacker restricts the selection space of the victim and learns properties of her task. We will examine three schemes for attack mitigation: (1) no action; (2) assess only the current request; and (3) assess all unfinished requests from the attacker. The parameters that we will measure include: (1) at what stage the system starts to raise alarms; (2) false alarm rate; (3) the productivity of the cloud; and (4) cost and delay to end users. The objective of the experiment is to assess the detection capability of

the proposed mechanism and its impacts on system performance so that we can refine our approach for future deployment.

Example Experiment 2: Responses to Dynamic Cloud Environment The manufacturing cloud can change in real time in many ways. For example, end users may update details of their requests while the tasks are processed in the system. As another example, equipments may suddenly become unavailable because of malfunction. While the dispatching and scheduling algorithms for manufacturing clouds are designed to handle such dynamics, we must carefully assess our security mechanisms and see how well they adapt to such changes. The system dynamics that we plan to test include: (1) duration of a resource that a request needs; (2) types of resources that a request needs; (3) availability of resources; and (4) changes of routing paths among resources. We will investigate the overhead of the security mechanisms that is incurred by the changes.

5 Conclusion

In this paper we investigate the security of manufacturing cloud. Specifically, we discuss the detection of side channel attacks on privacy of user requests. Since the concept of cloud manufacturing is still in its infancy stage, our investigation focuses on the statement of research problems and exploration of approaches. The examples show that sharing of resources creates a new path for malicious parties to compromise user privacy through side channel attacks. Such attacks need to be mitigated at the task dispatching and scheduling phase. We discuss an idea to quantify the impacts of a user request on subsequent requests. We also propose to build a prototype system upon our current RAMP platform.

Since the work discussed in this paper focuses on problem statements and emerging ideas, our next step is to implement the approach and thoroughly evaluate it. We will first run simulations with different combinations of user requests and available resources to determine the threshold value for raising alarms. We will then implement the prototype manufacturing cloud and test the detection capability of the proposed approach. Mutual impacts between the cyber and physical sub-systems under these scenarios will be studied so that our approach can be generalized to other systems with shared resources.

References

1. Tao, F., Zhang, L., Venkatesh, V., Luo, Y., Cheng, Y.: Cloud manufacturing: a computing and service-oriented manufacturing model. Journal of Engineering Manufacture **225**(10) (2011) 1969–1976
2. Wang, X., Xu, X.: An interoperable solution for cloud manufacturing. Robotics and Computer-Integrated Manufacturing **29**(4) (2013) 232–247
3. Wu, D., Greer, M., Rosen, D., Schaefer, D.: Cloud manufacturing: Strategic vision and state-of-the-art. Journal of Manufacturing Systems (JMSY) **32**(4) (2013) 564–579
4. Xu, X.: From cloud computing to cloud manufacturing. Robotics and Computer-Integrated Manufacturing **28**(1) (2012) 75–86

5. Zhang, L., Luo, Y., Tao, F., Li, B., Ren, L., Zhang, X., Guo, H., Cheng, Y., Hu, A., Liu, Y.: Cloud manufacturing: a new manufacturing paradigm. Enterprise Information Systems **8**(2) (2014) 167–187
6. EU Seventh Framework Programme: Manucloud: The next-generation manufacturing as a service (maas) environment. http://www.manucloud-project.eu/ (2010)
7. Rauschecker, U., Stöhr, M.: Using manufacturing service descriptions for flexible integration of production facilities to manufacturing clouds. In: ICE conference. (2012)
8. Cheng, J., Law, K., Björnsson, H., Jones, A., Sriram, R.: A service oriented framework for construction supply chain integration. Automation in Construction **19**(2) (2010) 245–260
9. Chiou, R., Mookiah, P., Kwon, Y.: Manufacturing e-quality through integrated web-enabled computer vision and robotics. The International Journal of Advanced Manufacturing Technology **43**(7–8) (2009) 720–730
10. Owens, R., Wang, W.: Non-interactive os fingerprinting through memory deduplication technique in virtual machines. In: IEEE International Performance Computing and Communications Conference (IPCCC). (2011)
11. Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T.: Cross-vm side channels and their use to extract private keys. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS). (2012) 305–316
12. Curtis, P.M.: Maintaining Mission Critical Systems in a 24/7 Environment. Wiley (2011)
13. Damodaram, A., Ravindranath, K.: Cloud computing for managing apparel and garment supply chains - an empirical study of implementation frame work. International Journal of Computer Science Issues (IJCSI) **7**(6) (2010)
14. Goucher, E., Wassermann, J.: Harper government boosts manufacturing capabilities in the west. Government of Canada News Releases (2014)
15. Katz, B., Bradley, J.: How can networks help modernize a manufacturing economy? In: The Metropolitan Revolution book. Melcher Media (2013)
16. Daniell, K.S.: Remote automation management project (ramp). Moultrie Technical College (2008)
17. Li, B.H., Zhang, L., Wang, S.L., Tao, F., Cao, J.W., Jiang, X.D., Song, X., Chai, X.D.: Cloud manufacturing: a new service-oriented networked manufacturing model. Computer Integrated Manufacturing Systems **16**(1) (2010) 1–7
18. Wu, D., Thames, J.L., Rosen, D.W., Schaefer, D.: Towards a cloud-based design and manufacturing paradigm: Looking backward, looking forward. In: Computers and Information in Engineering Conference. (2012) 315–328
19. Tao, F., Zhao, D., Yefa, H., Zhou, Z.: Correlation-aware resource service composition and optimal-selection in manufacturing grid. European Journal of Operational Research **201**(1) (2010) 129–143
20. Tao, F., Laili, Y., Xu, L., Zhang, L.: Fc-paco-rm: A parallel method for service composition optimal-selection in cloud manufacturing system. IEEE Transactions on Industrial Informatics **9**(4) (2013) 2023–2033
21. Cai, M., Zhang, W., Chen, G., Zhang, K., Li, S.: Swmrd: a semantic web-based manufacturing resource discovery system for cross-enterprise collaboration. International Journal of Production Research **48**(12) (2009) 3445–3460
22. Cai, M., Zhang, W., Zhang, K.: Manuhub: a semantic web system for ontology-based service management in distributed manufacturing environments. IEEE Transactions on System, Man, and Cybernetics Part A: Systems and Humans **41**(3) (2011) 574–582

23. Zhang, W., Zhang, S., Cai, M., Liu, Y.: A reputation-based p2p architecture for semantic service discovery in distributed manufacturing environments. Concurrent Engineering: Research and Applications **20**(3) (2012) 236–252
24. Shi, S., Mo, R., Yang, H., Chang, Z., Chen, Z.: An implementation of modeling resource in a manufacturing grid for resource sharing. International Journal of Computer Integrated Manufacturing **20** (2007) 169–177
25. Zhang, L., Guo, H., Tao, F., Luo, Y., Si, N.: Flexible management of resource service composition in cloud manufacturing. In: IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). (2010) 2278–2282
26. LaSelle, R.: Assembly automation: manufacturing in the cloud. assembly magazine, BNP media (2011)
27. Lomas, C., Matthews, P.: Meta-design for agile concurrent product design in the virtual enterprise. Int. J. of Agile Manuf. **10**(2) (2007) 77–87
28. Tao, F., Hu, Y.F., Zhang, L.: Theory and practice: Optimal resource service allocation in manufacturing grid. China Machine Press (April 2010)
29. Ulieru, M., Norrie, D., Kremer, R., Shen, W.: A multi-resolution collaborative architecture for web-centric global manufacturing. Information Sciences **127**(1–2) (2000) 3–21
30. Yusuf, Y.Y., Sarhadi, M., Gunasekaran, A.: Agile manufacturing: The drivers, concepts and attributes. Int. J. of Production Economics **62**(1–2) (1999) 33–43
31. Special report from the editor: Collaborative manufacturing: All together now, the advantages of crowdsourcing. Economist, April 21st, (2012)
32. Chafkin, M.: The future of manufacturing. Inc. Magazine (2009)
33. Wu, D., Thames, J., Rosen, D., Schaefer, D.: Enhancing the product realization process with cloud-based design and manufacturing systems. Transactions of the ASME, Journal of Computing and Information Science in Engineering (JCISE) **13**(4) (2013) 041004–1–14
34. Medina, V., García, J.M.: A survey of migration mechanisms of virtual machines. ACM Comput. Surv. **46**(3) (2014) 30:1–30:33
35. Graves, R., Agrawal, A., Haberle, K.: Estimating tools to support multipath agility in electronics manufacturing. Components, Packaging, and Manufacturing Technology, Part C, IEEE Transactions on **19**(1) (Jan 1996) 48–56
36. Houser, D., Harianto, J.: Manufacturing robustness analysis of the noise excitation and design of alternative gear sets. In: SAE Noise and Vibration Conference and Exposition. (2001)
37. Yan, H., Yin, G., Lou, S.X.C.: Using stochastic optimization to determine threshold values for the control of unreliable manufacturing systems. Journal of Optimization Theory and Applications **83** (December 1994) 511–539
38. Ho, Y.C.: Performance evaluation and perturbation analysis of discrete-event dynamic systems. IEEE Transactions on Automatic Control **32** (1987) 563–572
39. Hu, X., Song, H., Harrison, L., Lu, A., Gao, J., Wang, W.: Towards effective collaborative analysis for distributed intrusion detection. In: IASTED International Conference on Human-Computer Interaction (HCI). (2011)
40. Alvarez, E.: Multi-plant production scheduling in smes. Robotics and Computer-Integrated Manufacturing **23** (2007) 608–613
41. Chou, Y.C., Chen, C.J., Tang, C.W., Su, J.H., Wang, L.: Integration of supply chain scheduling by constraint satisfactory. In: Proceedings of the conference on flexible automation and intelligent manufacturing. (2004) 1316–1324
42. Kanyalkar, P., Adil, G.: An integrated aggregate and detailed planning in a multi-site production environment using linear programming. Int J Prod Res **43**(20) (2005) 4431–4454

43. Dinita, R., Wilson, G., Winckles, A., Cirstea, M., Jones, A.: A cloud-based virtual computing laboratory for teaching computer networks. In: International Conference on Optimization of Electrical and Electronic Equipment (OPTIM). (2012) 1314–1318
44. Basili, V.R., Caldiera, G., Rombach, H.D.: Goal question metric paradigm. In Basili, V.R., Caldiera, G., Rombach, H.D., eds.: Encyclopedia of Software Engineering. John Wiley and Sons (1994) 528–532