2022

System and Risk Analysis of Cloud Manufacturing System

Trupti Narayan Rane
Old Dominion University

Original Publication Citation

Rane, T. N. (2022). System and risk analysis of cloud-manufacturing system. *International Journal of Computer Science and Engineering Survey*, *13*(3), 13-27. https://doi.org/10.5121/ijcses.2022.13302

System and Risk Analysis of Cloud-Manufacturing System

Article *in* International Journal of Computer Science & Engineering Survey · June 2022

DOI: 10.5121/ijcses.2022.13302

1 author:

Trupti Rane
Old Dominion University
3 PUBLICATIONS **0** CITATIONS

SEE PROFILE

SYSTEM AND RISK ANALYSIS OF CLOUD-MANUFACTURING SYSTEM

Trupti Narayan Rane

Department of Engineering Management and Systems Engineering
Old Dominion University, USA

ABSTRACT

The Cloud manufacturing(C-Mfg) system involves remote distributed manufacturing resources and capabilities collaborating as a single virtual entity. The system receives orders for custom products and provides manufacturing as a service to the end customers. The primary activities of the system, among others, are transaction control, resource allocation and monitoring, distributed manufacturing, quality control, and delivery of consignments to the customers. The actual manufacturing is done by a network of third-party partner manufacturers providing the services to end customers, helping them with cost reduction, shorter time-to-market, and enabling efficient collaboration between manufacturers in the C-Mfg network. This paper aims to deep dive into C-Mfg as a system and perform a risk analysis to assess and mitigate the risks associated with the system. While cybersecurity and data security-related concerns are deemed the most serious and need immediate management for the system to succeed, the control of data, compliance with manufacturing standards and guidelines, and lack of accountability and ownership are other serious risks that need significant attention. Identifying these factors will help channel the focus on the management and resolution of these risks to establish digital trust in the C-Mfg system leading to the system's success.

KEYWORDS

Cloud Manufacturing(C-Mfg), Manufacturing as a Service (MaaS), Digital Manufacturing, Digital Trust, Risk Assessment.

1. INTRODUCTION

Manufacturing is one of the primitive and most native industries in the history of humankind. Nonetheless, manufacturing today is not like how it was a few years back. Today, markets are more agile than ever. They have customized and agile needs. They need high-quality products in highly variable batches. TQCSEFK, which spells out fastest-Time to Market, highest-Quality, lowest-Cost, best-Service, cleanest-Environment, greatest-Flexibility, and high-Knowledge; is a complex yet well-meaning acronym and the definition of ideal standards in the manufacturing industry. High-performance computing, optimization and simulation tools, excellent connectivity alongside optimal computing and data resources, and high-precision domain-relevant equipment are required to achieve these high standards. It might not be feasible to achieve all these through ownership. MaaS or Cloud computing tries to address this by building a virtual enterprise of geographically distributed entities that manufacture custom products in bulk or limited quantities through collaboration.

The manufacturing industry saw its first significant uplift from man-made to man-and-machine-made during the 17th century with the Industrial Revolution's onset. Since then, one thing that has been constant across the years is the continuous change in the manufacturing outlook. With

the computers and advancements in the information technology space came Digital transformation, which has positively changed all the industries around us. Manufacturing is no exception, and digital transformation has added new dimensions in manufacturing.

Today, concepts like additive manufacturing and 3D printing have added massive value to the world. Some companies wanted to explore 3D printing but did not want to invest in the infrastructure. Also, others invested in the infrastructure and wanted to make optimal use of it and thus were exploring options to make these services and resources accessible remotely so that they could share the costs. And then some others only invested in the infrastructure to subsequently provide these as a service to multiple stakeholders. This phenomenon gave rise to a new kind of manufacturing called C-Mfg or Manufacturing as a service. While there is ample research on how big data analytics and MIoT analytics can be done for cloud manufacturing, the risks related to big data security and provenance aspects are still open for further research [1]–[3].

This paper explores the C-Mfg ecosystem and reviews the risks associated with the system and the assessment and mitigation strategies for enabling the system's success. Managing these risks in the context of the C-Mfg system will also open new avenues towards digitalization of not only manufacturing but other traditional industries such as supply chain, transportation, and warehouse management, where similar approaches apply due to its distributed multi-party nature and since these industries have similar compliance policies and guidelines. Identifying and managing risks to establish trust between geographically distributed stakeholders and communicating and coordinating towards a single goal can benefit several business and cross-functional areas.

While there is valuable research in the past focused on how cloud manufacturing as a model can be implemented, risk analysis specific to this context is a path less explored. What factors would affect or prevent wide adoption of the model, how these factors can be accounted for, and how risks identified can be mitigated would positively serve the system, leading to rapid digitalization in the manufacturing domain.

2. RESEARCH QUESTION

What are the risks associated with cloud manufacturing/Manufacturing as a service platform, and how can these be assessed and mitigated?

3. SYSTEM ANALYSIS

To begin with, one of the first striking observations while working on the literature review of papers in this domain was the terminology used across several research efforts in this area. C-Mfg is a set of processes and concepts referenced using multiple terms across several research publications in this space. It is interchangeably called manufacturing as a Service, Digital manufacturing, Cloud Manufacturing, Service manufacturing on-cloud, Cyber Robotics, Cloud-based Computer-aided manufacturing, Cyber manufacturing, and even Smart manufacturing or Smart MaaS. The most commonly and frequently used term is Cloud manufacturing. Another key here is not to confuse C-Mfg with the concept of virtual manufacturing researched since the 2000s. There is much work published on virtual manufacturing, which though extensive, does not cover the concepts of C-Mfg. While the terms may sound similar, virtual manufacturing and C-Mfg are different. While C-Mfg is about manufacturing by consuming the resources virtualized through the cloud, virtual manufacturing is about interchanging models between their use in simulation and control environments to "Manufacture in the Computer." Virtual manufacturing involves a simulation of the actual process to identify issues in the real process, enhance decisions, and get control during the actual manufacturing.

Figure 1 shows the Benefits of C-Mfg as opposed to traditional manufacturing. Some of the noticeable benefits are scalability, reduction in cost and time-to-market, efficient resource utilization, collaboration efforts between multiple manufacturers, and a lower barrier to entry for new manufacturers.

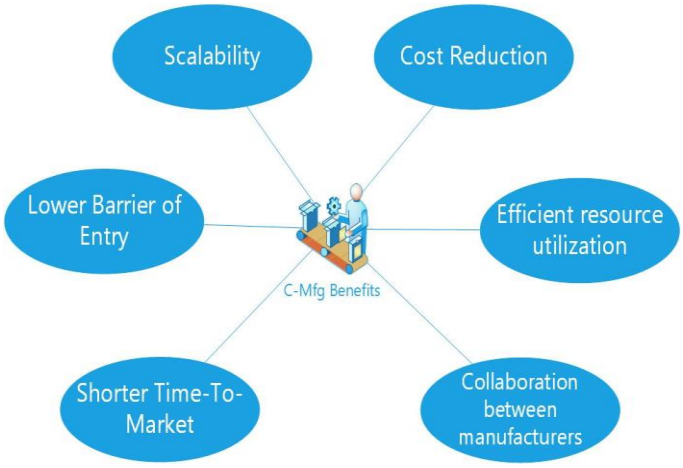

Figure 1. Benefits of C-Mfg

3.1. Service Provider

There can be two types of service providers in a C-Mfg system.

- Service providers like Xometry act like a digital manufacturing marketplace with a network of more than five thousand manufacturers distributed around the world. When an order is received, the service provider sends it to its manufacturers (either in parts or the whole order, based on allocation and resource utilization logic), and then the manufactured parts are brought in and inspected by Xometry for quality before getting delivered to the end client. Xometry takes ownership and liability to fulfill the order to the end customer.
- Service providers like MFG.com and Wor.Con acts as the B2B marketplace, facilitating the transaction between the end customer and the manufacturer. When an order comes, the customer asks for quotations through RFQs. The manufacturers in the network bid for getting the contract, and based on the terms, service providers outsource the manufacturing to the 3rd –party. The liability for the order delivery and quality lies with the actual manufacturer, but MFG.com has partnership contracts with actual manufacturers on the desired quality and precision required.

3.2. Infrastructure

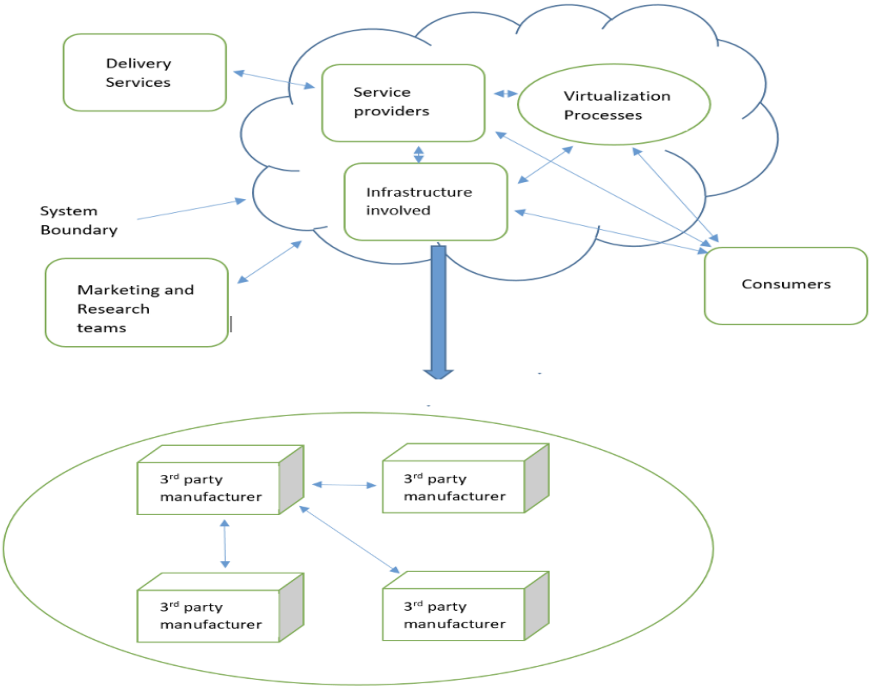

Figure 2. A broad classification of the C-Mfg System components

The infrastructure involved in manufacturing can also be classified as an internal entity of the complex system. This would include the high-precision manufacturing resources and equipment involved, the scheduling and enterprise software, and the artifacts necessary for the virtualizing of the process.

3.3. End Consumer/Customer

The customer who requests the manufacturing services is no doubt a vital stakeholder in the system

3.4. Environment

To realize the objective of TQCSEFK, a shift in traditional manufacturing became the need of the hour. With the sophistication needed for the highest quality, manufacturers needed complex and costly infrastructure, which would defeat the low-cost aspect of TQCSEFK unless manufacturers started thinking out of the box. And out of the box it was, with greater flexibility and fast and customized manufacturing services coming with C-Mfg into existence. This meant innovating the traditional environment and outlook toward manufacturing. To the traditional manufacturing environment, virtualization had to be integrated by including enterprise software for monitoring the effective use of resources, scheduling jobs on virtualized artifacts, and creating custom quotations through distributed resources. Together these components compose the environment for the complex system.

The environment consists of three aspects: the input, the operations on the inputs, and the outputs.

Input

The most significant inputs come from the end customer. Custom manufacturing focuses on and is driven by the end customer's needs. The consumer drives even the most vanilla scenario of custom-manufacturing, which could be as simple as a Dell computer with limited predefined plug-in customizations. The customer gives his inputs in the form of specifications needed from the custom manufacturing. Other inputs also come into the system through the delivery services of raw materials needed. Inputs also flow in from other entities, such as software developers bringing innovations and upgrades to the virtualized artifacts and software components. Inputs also go from marketing and research teams on how to improvise the manufacturing process.

Operations

The inputs from various stakeholders are processed either directly or indirectly in the C-Mfg process to bring out the end product for the consumers/end customers.

- **Scheduling:** The service provider's scheduling process determines which third-party manufacturers from the network would take up the job and in what proportions. This is a crucial part of the transformation process. The ownership of the manufacturing would be on the actual manufacturers, but the accountability to the end customer lies with the service provider. The manufacturers are bound contractually to the service provider but, in most cases, not to the end customer. The concept is very similar to an Uber ride. When you book a ride, you trust Uber to match you with a driver that works best for you. Uber does not have ownership of the car or the driver's resources. The driver performs the work of picking his ride up and dropping him at the end location. However, if there are any grievances, these would need to be brought to Uber's attention for resolution as Uber is accountable to you as a service provider.
- **Manufacturing:** The most apparent transformational process is the actual manufacturing using raw materials and other resources such as the internet, electricity, and labor. A manufacturer may produce the whole order for a customer or just a part of a big consignment. It is also possible for a manufacturer to produce only a subpart that will eventually be plugged in to make the actual product the customer ordered
- **Quality Control (QC):** QC is one of the most integral parts of the whole manufacturing process. I have segregated it from manufacturing only because, in a C-Mfg scenario, it would be performed by either of these parties based on the contractual agreement between the service provider and the third-party manufacturer. The manufacturer would manufacture, do the necessary checks as part of QC and ship the product directly to the end customer OR the service provider would consolidate the entire order, check on the specifications as part of QC, and hip to the end customer OR the service provider could also do an on-site QC at the manufacturers by sending in representatives and then the products may be shipped to the customers. The most significant inputs come from the end customer. Custom manufacturing focuses on and is driven by the end customer's needs.

Output

The output is the finished customized products that go to the end-users/consumers through the delivery services. The system also outputs new industry standards and best practices, processes, and knowledge artifacts for future innovations, usually consumed by the marketing and research teams and other enterprises.

4. RISK ANALYSIS

The Risk analysis cycle, as shown in Figure 2, includes the following phases:

- Risk Identification
- Impact Analysis
- Risk Prioritization
- Risk Mitigation
- Implementation

Figure 3. Risk Analysis cycle

4.1. Risk Identification and Impact Assessment

4.1.1. Operational Risks

Risks due to IoT sensors:

With the advent and wide acceptance of IoT in technologies like Smart Homes, smart cities, health care, and security surveillance, IoT has also found its way into manufacturing through smart technology in the form of RFIDs and various sensors. There are a variety of advanced manufacturing systems such as Computer Integrated Manufacturing, Flexible Manufacturing, and Networked Manufacturing. C-Mfg is an amalgamation of concepts from several of the advanced manufactured systems with addressing the bottlenecks of these systems through cloud computing and IoT. [4] and [5] speak about Internet-of-things-based sensors that help identify issues and provide operational data that can be used in predictive analytics to prevent issues. IoT sensor-based monitoring is interchangeably referred to as Smart Monitoring.

However, IoT technology poses some risks.

- These have been known to be easy entry points into the corporate networks for cyberattacks because the IoT technology is relatively new; these devices are very close to operational devices since they act as sensors and because these are retrofitted into existing architecture that was not designed for this innovation.
- The amount of data generated by these devices is humongous, and the insights it can give into the manufacturer's operations make it extremely sensitive. So there is a risk of unauthorized access to this data if not covered efficiently.

Risks with Cloud computing:

It is only recently that people have started trusting the cloud with sensitive data. However, there are still risks that need to be mitigated.

- Lack of ownership and accountability: when you do not own any resources that would help manufacture custom products for you, and the accountability of getting the job right lies with stakeholders with whom you have no direct contracts, it is difficult to establish trust.
- Security Concerns: Security has a pivotal role in averting system failures and promoting trust in cloud computing. With virtualization, the primary security issues include data leakage because multiple third-party manufacturers (in our system of interest) share physical resources, identity management, access control, the physical protection of virtual resources, and the prevention of cross-virtual machine channel attacks.
- Control over own data: Control is another important aspect of trust. We cannot trust a system completely when we do not have complete control over the system.

For a cloud solution, one mathematical equation that is relevant is

Opportunity + Digital Trust = Growth

Trust is a crucial factor for a cloud solution to excel. However, how do cloud providers establish trust with their customers when a third party deals with their sensitive information in a remote environment distributed across the globe? Even though we address trust as a system problem and assess it as a risk, it is natively a human emotion. So, to analyze this issue, we would need perspectives from multiple prospective customers on what would make them trust a cloud model. This would also be an iterative process to establish that the problem is resolved with the utmost certainty.

Risks with Distributed Manufacturing through multiple manufacturers:

- Lack of transparency: on how the information will be stored, what processes will be involved in the manufacturing, and who will manufacture the product. etc. would be essential
- Assurance of compliance from the third party: Complexity involved in a cloud-based system can create disorganized overlying gaps or controls that may lead to legal or regulatory non-compliance. How do you ensure that a third-party manufacturer located in a far-away country will adhere to the legality and regulations involved in your industry?
- Maintenance, warranty, and after-care: It is unfair that C-Mfg would not guarantee after-care or maintenance of the manufactured product, but the process can be tricky and not straightforward.
- Quality concerns: Since there are no direct contracts or interaction between end customers and manufacturers, there could be concerns with the quality of products manufactured.
- Intellectual property management: When custom products are being manufactured, the intellectual property on how these products will be used would need to be secured. With a cloud model, the customers may not trust the service provider or third-party manufacturers with their intellectual property.

4.1.2. Non-Operational Risks

Jurisdictional and Political Risks:

When we talk about a system geographically distributed globally, we are talking about collaboration across entities located in different countries or even continents. Such a collaboration would have legal, economic, jurisdictional, and political risks and boundaries. Everything right from the transaction currency to the labor market and rules, export, import, and customs would need to be ironed out. C-Mfg or any other cloud-computing-based solution implies centralizing both computing resources and information in data centers, posing the threat of potential for organizational and the government's control over this data. So, it is crucial to have an adequate evaluation of these geographical issues, especially jurisdiction. The customers would need transparency of where the legal cases involving the service provider if any arise, be adjudicated? How favorable that jurisdiction would be to the cloud provider's interests?'

When customers opt for a cloud solution of any kind of exceptionally high cost involving domains like manufacturing, they would expect complete and clean Fungibility and portability of user data from one location to another—this warrants standardization of the data distributed across the network. The lack of a political outlook and supporting political infrastructure that responds dexterously to rapid technological changes in domains like manufacturing is a significant risk to a system.

Risks with Maintenance Costs:

Sustainment of a C-Mfg system: With Cloud Mfg., the sky is the limit. At the same time, the efficient sustainability of the system should not be off-limits for the service provider to turn in profits. The infrastructure, the resources, and the scheduling should be such that it is cost-efficient as well as time-efficient, without which the purpose of the system would be defeated. This would need to be in the frontline of the risk assessment.

Architectural issues related to unification, reusability, and scalability: These characteristics are relatively easier to implement in a homogenous on-premise solution, but when cloud architecture comes into play, additional challenges arise given the emerging and fast-changing technologies and diverse industrial practices. It is thus crucial to consider different perspectives while establishing the architecture for the system. A higher sample size of data would be needed to bring in the diversity needed for the analysis. This would mean reaching out to a broader section of stakeholders for their input.

Risks associated with "studying" the system:

For a model to work successfully, adapt to changing conditions and evolve, it should be easy for researchers to collect data about the system by performing experiments, conducting surveys, etc. Data collection is one of the highest impact risks with a system like C-Mfg. Since C-Mfg as a concept is relatively new, there are limited preexisting datasets available. The literature review revealed very few references to data that could be used to establish and attempt to resolve the problems of the complex system at hand. Since most service providers will not provide this information readily due to security and privacy concerns, the system analysis and design effort would need to be creative and concrete enough to extract data from suitable sources and of the right relevance.

Another factor that would need considerable energy is to consider the system's geographical diversity and distributed nature. It would be highly challenging to collaborate with stakeholders

during data collection and analysis. All the stakeholders, be it service providers, customers, or different manufacturers, would be distributed across the globe. So data collection and analysis would need to be well planned and orchestrated to be contextually relevant and comply with any regulations for the system for both data collection and hosting.

4.2 Risk Prioritization

Based on the literature review done in this area, the highest priority risks are the ones below:

Likelihood	Impact: Insignificant	Minor	Moderate	Serious	Catastrophic
Certain			Lack of ownership/ accountability	Control of Data(especially for large enterprises	Security/ Cybersecurity concerns
Likely				manufacturing standards and guidelines	
Possible		Risks with IoT devices			
Unlikely				Lack of transparency	
Rare	Intellectual property management	Quality concerns, aftercare and warranty			

Figure 4. Risk prioritization matrix

Security Risks: Cybersecurity is one of the major concerns for manufacturers when C-Mfg is brought into the frame. [6] touches upon the cybersecurity-related challenges faced by cloud manufacturers and service providers. How do we ensure that the integrated systems are secure when we introduce advanced technology into a legacy system and retrofit it with sensors and IoT devices?

Control over own data: C-Mfg is economical for small and medium enterprises due to the removal of dependency on an IT infrastructure. However, moving a large enterprise's data and physical artifacts might not be as economical. Also, moving an already existing on-premises legacy system to the cloud may not be as feasible economically or be challenging. If you need to switch cloud providers later due to more advancements in a different cloud solution may not be as feasible. One striking difference between He & Xu's work in [4] and the work of other researchers in the domain of C-Mfg, is that they provide a statistical outlook of how much research has been done before. It also provides the influential critical technologies like cloud computing and IoT, which depend on high-performing computing (HPC) solutions that use supercomputers and computer clusters to handle multiple tasks at high speed, and Service-oriented architecture (SOA) for on-demand resource allocation.

Lack of Transparency: Virtualizing the manufacturing resources and processes may also not be straightforward, and there will be several risks involved, such as

- Availability issues during network failures or system outages,
- Interoperability with more than one cloud,
- More than one information system,

- Scalability

Lack of Ownership and accountability: What if a cloud provider that stages your data goes out of business? Or has an outage? How would critical services in manufacturing function even with an hour-long outage? Through the mitigation steps, cloud services would need to establish a trust mechanism with the customers, especially those on mission-critical paths.

We need a process-based risk management approach to mitigate this risk rather than a compliance-based approach.

- Use trusted cloud services with high trust in the industry, such as AWS, GCP, and Azure, especially for mission-critical manufacturing.
- Have contractual agreements around the availability of cloud service, especially with the services that are needed for day-to-day operations
- Have a security model that suits your needs the best.

Compliance: Since C-Mfg has a distributed architecture, there is a lack of a core governance body that can control the whole system [7]. How to ensure all involved parties comply with the legal components of all the governing bodies involved? For example, the manufacturing of medical devices, which by law should comply with FDC'S sterility guidelines. How do we ensure all the third-party manufacturers and subcontracts comply with these guidelines?

4.2. Risk Mitigation, Implementation, and planning

The following summarizes the mitigation alternatives identified for all the high-priority risks.

Security Risks: To mitigate this risk, encryption, intrusion detection, and new access controls are required. How manufacturers will be able to detect and prevent the embedded defects introduced by attackers so that a system or a component will no longer perform its intended functions. To counter these defects, monitoring manufacturing systems and processes and non-destructive testing or non-destructive inspection techniques are required. The paper identifies Intrusion detection, Authentication, Encryption, and Access control as the four control mechanisms to counter cybersecurity-related issues and concerns in the domain. [8] also brings to attention the Security, trust, and reliability management-related concerns. [9], [10] highlighted terms like Agile Manufacturing, Concurrent Engineering, Networked Manufacturing, Manufactured Grid, and Crowdsourcing used towards rapid manufacturing by responding quickly to the customer needs without taking a hit on the quality or cost. This paper provides valuable insights into how security risks can be mitigated by newer innovations in the cybersecurity space, such as zero-trust methodologies, which are different from the perimeter-based firewall-based security model. In such a model, once the firewall is breached and the attacker gets access, there is no other mechanism to avoid unauthorized access and damage. Instead of a password, the users' fingerprints, faces, and eyes are used for authentication in zero-trust. Similarly, the metadata related to the user, such as devices that the user has registered, is used for authentication. Also, only access required for the current task is provided instead of role-based access providing service-based access.

Other alternatives are:

Alternative 1: Certification: an independent security certification authority could certify cloud services regarding their security properties and capabilities.

Alternative 2: Demonstrate confidence in your security: that the systems are secure to protect customers and that other data and identity/privacy issues have been dealt with. Demonstrate the confidence in your system to have the proper controls and monitoring to ensure that the system is secure.

Control over own data

Alternative 1: Establish a Remote Access Control Cloud: Irrespective of the service provider's location, provide remote access control capabilities to customers for better jurisdictions over their data. Even though customer information is remotely stored and processed, the data owner would retain control of these data management activities.

Alternative 2: Hybrid cloud: A Hybrid CMfg service platform that combines public and private platforms. Noncritical services and non-sensitive information are sourced to the public CMfg platform accessible to third-party manufacturers, whereas critical services and sensitive data are in the service provider's control in a private CMfg platform.

Lack of Transparency

Alternative 1: Provide tracing/logging: What happens to my data once I place an order? Who manufactures it? Where does the raw material come from? How much time does it take for the third-party manufacturer to get the product ready? Who does the quality inspection manufacturer or service provider? How is my data used? Answers to these questions would provide transparency to the customers. One way is to provide a trace of activity by logging them and making it available to the customer to access from his cloud instance.

Alternative 2: Provide a set of information to the customer with his invoice. This would include which manufacturers were involved in making the products, how much the infrastructure cost, the servicing cost, and other detailed breakdowns.

Alternative 3: Provide full disclosure on any security breaches or issues during the order fulfillment. Customers entrust the cloud service provider, so they should get an honest and realistic view of the service provider's management of their information.

Lack of Ownership and accountability:

Alternative 1: Have legally bound contracts: between the end customer and service provider to establish accountability

Alternative 2: Have Quality control of manufactured products with the service provider rather than third-party manufacturers. Also, hire efficient and on-time delivery services when delivering to end customers.

Compliance

Alternative 1: Have external independent third-party quality control inspections of processes and practices followed.
Alternative 2: Build your reputation by example: Provide past legal and regulatory compliance instances to prospective customers. When given an opportunity, prove it to your customers, so they come back to you in the future.

5. ETHICAL, CULTURAL, AND SOCIAL CONSIDERATIONS

5.1. Ethical Risk Analysis (eRA)

Ethical analysis is required for effective decision-making on risk policies. An eRA compliments and supplements but never replaces traditional risk analysis that focuses on the likelihood and impact of undesirable events. eRA covers ethical issues such as interpersonal relationships and justice.

eRA is a three steps process.

1) Identify the stakeholders or people concerned and categorize them as roles being risk-exposed, a beneficiary, or a decisionmaker.
2) A deep dive into the detailed classification of roles identified in step 1 to identify role combinations as ethically problematic role combinations.
3) Further detail analysis and ethical reflection emphasize individual risk-benefit weighing, distributional analysis, and power analysis. Ethical issues about subsidiary risk roles, such as those of experts and journalists, are also treated in this phase.

Some of the Ethical considerations when considering C-Mfg are:

Environmental impacts: [11] highlights that the Information and Communication Technologies industry generates about 2% of the total global carbon dioxide emission, equal to the aviation industry. Even though cloud data centers afford to pay the cost of their vast energy consumption, they must minimize the energy consumption and strive to use as many green energy sources as possible to mitigate the ethical risks associated with moving manufacturing to cloud computing.

Human factors and manufacturing in the cloud: The C-Mfg system will be used by humans of various levels of technical expertise around different aspects of the system, depending on their duties. C-Mfg has three groups of actors: consumers, who request and use C-Mfg processes; application providers, who provide the software to enable the manufacturing cloud and associated ICT; and service providers, who provide, own, and operate the manufacturing services.

Making the system efficient for the human actors is part of the ethical consideration. Considering the sensitivity of the situation that the system will be addressed, it will be required to be as simple as possible. For example, during critical functions like resource allocation and resource health monitoring, the last thing on an operator's mind would be to remember how to operate a system or how it works. It should not be a bottleneck in his functioning. This requirement for the system to be as easy to operate as possible should be implicit. No stakeholder may mention it, or they might fail to mention that they need the system to be easily operable without using a lot of their short-term human recall. The risk engineer would need to figure this out based on the other aspects of the ethical risk analysis.

The limit of short-term human recall is not more than seven +/- two items. This essentially means that humans will tend to forget what they wanted to achieve at the max by the eighth or ninth step. System engineers should understand these limitations of humans to focus on multiple things in parallel while designing. So, the system design should be as simple as possible when designed, operated, and evolved by people.

5.2. Cultural Considerations

When we talk about a system geographically distributed across the globe, we are talking about collaboration across entities located in different countries or even continents. Such a collaboration would have legal and economic, jurisdictional, and political constraints and boundaries. Everything right from the transaction currency to the labor market and rules, export, import, and customs would need to be ironed out. C-Mfg or any other cloud computing-based solution implies centralization of both computing resources and information in data centers, posing the threat of potential for organizational and the government's control over this data. So, it is crucial to have an adequate evaluation of these geographical issues, especially jurisdiction. The customers would need transparency of where the legal cases involving the service provider if any arise, be adjudicated? How favorable would that jurisdiction be to the cloud provider's interests?

When customers opt for a cloud solution of any kind, especially with high costs involving domains like manufacturing, they expect complete and clean Fungibility and portability of user data from one location to another—this warrants standardization of the data distributed across the network. The lack of a political outlook and supporting political infrastructure that responds dexterously to rapid technological changes in domains like manufacturing is a significant bottleneck to a system.

5.3. Social Considerations

5.3.1. Establish trust between stakeholders

Stakeholders:

- Primary stakeholders: The service providers, partnering manufacturers, and the end consumers are all primary stakeholders of the system
- Secondary stakeholders: The marketing team can be classified as secondary stakeholders as they impact the overall decisions on the system objectives even though they are not vital drivers.
- Tertiary stakeholders: Researching teams who have an indirect interest in the system but are not directly impacted by the system of interest

Design artifacts should include clear guidelines on processes that should be in place for establishing trust between the service provider, partnering manufacturers, and end customers. If trust cannot be established between key stakeholders, the system will not be able to function to meet its objectives. Policies and processes should be identified in advance of how handshake will happen between key stakeholders, what level of information will be exchanged, and how the information will be used.

As an end consumer, the primary interest is to get the custom product of interest manufactured with high quality in the optimal timeframe and within the set budget limits. Whether it is manufactured by one company at a single site or manufactured in parts across a distributed network is less important to the consumer. In the same breath, the end consumers would have other concerns with a distributed network, such as the trust issues that may arise, data security, intellectual property protection, compliance management (both legal and process-oriented compliance), and grievance addressing process which may keep the end-consumer at bay from effectively consuming the services provided by the C-Mfg system.

Optimal use of their infrastructure, human resources, and other resources are of interest to the manufacturing partners. They are also interested in maximizing their profit margins while subcontracting with the service provider. When they participate in a cloud-manufacturing architecture, they also have non-monetary benefits such as increasing the customer base to their credit and building their manufacturing expertise through continued work for a wide range of clients.

5.3.2. How much information is too much information?

A delicate balance would need to be achieved by establishing constraints so that the resources are not overexploited, leading to their failure, and not underutilized so that the system can be optimally utilized. For example, to gain a customer's trust, transparency would need to be maintained by the service provider. This would include who will manufacture the product and how customers' sensitive data will be handled. However, the system should not be constrained so that the service provider has to give full disclosure of how a particular manufacturer is selected, the payment terms between the service provider and the customer, etc. These would be the trade secrets, and these aspects are of no relevance to the end customer, and putting unnecessary constraints of full disclosure on the system may harm the system.

6. CONCLUSIONS

Considerable research has gone into the need to address issues with traditional manufacturing and embrace the advancements with digital transformation in the domain. Researchers have done extensive work on how digital trust can be established in Cloud computing, but it needs to be customized and deep dive into the specifics relevant to C-Mfg [12]. C-Mfg has the potential to be the next big thing, but it has a few risks that need to be addressed before it can get there. These risks must be suitably handled and mitigated for the widespread adoption of C-Mfg practices. Risks related to cybersecurity and data security are the most serious and need immediate management for the system to succeed. Control of data, compliance with manufacturing standards and guidelines, and lack of accountability and ownership are other serious risks that warrant significant attention. Identifying these factors will help channel the focus on the management and resolution of these risks to establish digital trust in the C-Mfg system leading to the system's success. Resolving these risks in the context of the C-Mfg system will also open new avenues towards digitalization of not only manufacturing but other traditional industries such as supply chain, transportation, and warehouse management, where similar approaches may apply due to its distributed multi-party nature and since these industries have similar compliance policies and guidelines.

REFERENCES

[1] H. N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," Enterp. Inf. Syst., vol. 14, no. 9–10, pp. 1279–1303, 2020, doi: 10.1080/17517575.2019.1633689.

[2] J. Wang, C. Xu, J. Zhang, and R. Zhong, "Big data analytics for intelligent manufacturing systems: A review," J. Manuf. Syst., vol. 62, no. November 2020, pp. 738–752, 2022, doi: 10.1016/j.jmsy.2021.03.005.

[3] C. Yang, S. Lan, L. Wang, W. Shen, and G. G. Q. Huang, "Big data-driven edge-cloud collaboration architecture for cloud manufacturing: A software-defined perspective," IEEE Access, vol. 8, pp. 45938–45950, 2020, doi: 10.1109/ACCESS.2020.2977846.

[4] W. He and L. Xu, "A state-of-the-art survey of cloud manufacturing," Int. J. Comput. Integer. Manuf., vol. 28, no. 3, pp. 239–250, 2015.

[5] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," Manuf. Lett., vol. 8, pp. 11–15, 2016, doi: 10.1016/j.mfglet.2016.05.002.

[6] D. Wu et al., “Cybersecurity for digital manufacturing,” J. Manuf. Syst., vol. 48, pp. 3–12, Jul. 2018, doi: 10.1016/j.jmsy.2018.03.006.
[7] P. Helo, Y. Hao, R. Toshev, and V. Boldosova, “Cloud manufacturing ecosystem analysis and design,” Robot. Comput. Integer. Manuf., vol. 67, no. March 2019, p. 102050, 2021, doi: 10.1016/j.rcim.2020.102050.
[8] D. Wu, M. J. Greer, D. W. Rosen, and D. Schaefer, “Cloud manufacturing: Strategic vision and state-of-the-art,” J. Manuf. Syst., vol. 32, no. 4, pp. 564–579, 2013, doi: 10.1016/j.jmsy.2013.04.008.
[9] L. Zhang et al., “Cloud manufacturing: a new manufacturing paradigm,” Enterp. Inf. Syst., vol. 8, no. 2, pp. 167–187, 2014.
[10] S. Barbhuiya et al., “SmartMaaS : A Framework for Smart Manufacturing-as-a-Service,” 17th Int. Conf. Manuf. Res. ICMR 2019, vol. Proceeding, pp. 1–7, 2019.
[11] H. R. Faragardi, “Ethical Considerations in Cloud Computing Systems,” Multidiscip. Digit. Publ. Inst. Proc., vol. 1, no. 10, p. 166, 2017, doi: 10.3390/is4si-2017-04016.
[12] T. Borangiu, D. Trentesaux, A. Thomas, P. Leitão, and J. Barata, “Digital transformation of manufacturing through cloud services and resource virtualization,” Comput. Ind., vol. 108, pp. 150–162, 2019, doi: 10.1016/j.compind.2019.01.006.

AUTHORS

Trupti Rane is a Sr. Solutions Architect at Fortanix. She is pursuing her Ph.D. in Engineering, specializing in Engineering Management and Systems Engineering at Old Dominion University, Norfolk, Virginia, USA. She has completed her Master of Science in Information Technology from the University of Cincinnati, Ohio, USA, and Bachelor of Engineering in Computer Engineering from Goa University, India. Her research interests include Cloud Manufacturing, Digital Trust, Blockchain, Data provenance, and cybersecurity. Contact her at trane002@odu.edu.