Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 39 (2019) 185–193

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

25th International Conference on Production Research Manufacturing Innovation: Cyber Physical Manufacturing
August 9–14, 2019 | Chicago, Illinois (USA)

Challenges and Opportunities for Publishing IIoT Data in Manufacturing as a Service Business

Joaquín Ordieres-Meré[a,*], Javier Villalba-Díez[b,c], Xiaochen Zheng[a]

[a] *ETSII, Universidad Politécnica de Madrid, José Gutiérrez Abascal 2, Madrid 28006, Spain.*
[b] *Fakultaet fuer Management und Vertrieb, Campus Schwbisch-Hall, Hochschule Heilbronn, Germany.*
[c] *ETSIInformática, Universidad Politécnica de Madrid, Calle de los Ciruelos, 28660 Boadilla del Monte, Madrid, Spain.*

Abstract

Cloud manufacturing (CMfg) can manage mass manufacturing (MM) resources and capabilities, and provide them as services via the Internet. Undoubtedly, multiple manufacturing clouds will have abundant services in terms of function, price, reliability, location, etc. The implementation of such concept in a wider structure than a single MC requires to provide explicit data about production sequence, machine allocation, production parameters, quality of service (QoS), and several other key performance indicators (KPIs). However, the state of the art approach is based on private access to such data, under specific contract requirements, and it becomes a limitation to the evolution of the concept itself. In particular it becomes limiting when the CMfgs involve multiple process owners distributed throughout a complex value creating network, such as production, logistics, quality control, but also, third parties like auditor interested in energy consumption, or machine maintenance provider, also interested in monitoring the effective usage of the machines, etc. This paper will analyze deeply the structural and functional characteristics of such CMfgs and then, it will propose a business intelligence architecture that aims to enable publishing relevant KPIs related to interested process data, with the convenient layer of trustworthiness. Such public access will enable the assessment to different agents at different time frequency and, finally, with different motivation, thus bringing practical information about time delays for the data availability and scalability factors.

Keywords: Industrial Internet of Things; Distributed Ledger Technologies; IOTA; Manufacturing as a Service; Cloud Manufacturing; KPI.

* Joaquín Ordieres-Meré. Tel.: +34-91-067-7107 ; fax: ++34-91-336-3005. OrcID: 0000-0002-9677-6764
E-mail address: j.ordieres@upm.es

2351-9789 © 2019 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the ICPR25 International Scientific & Advisory and Organizing committee members
10.1016/j.promfg.2020.01.308

1. Introduction

Manufacturers and service providers look to operate globalized manufacturing networks. Such option allows to address challenges, such as increased product complexity and decreasing life-cycles [1]. These factors, caused primarily by mass customization and demand volatility, generate a number of issues related to the design and planning of manufacturing systems and networks. Another relevant factor to be considered is the growing demand for Social Manufacturing (SMf). Social Manufacturing is a manufacturing mode in which the consumers are involved fully into the production process by the internet, moreover, the manufacturing equipment (3D printers) connected directly on the network can make all the activities [2]. Its primary effect will be to contribute to reduce the component life-cycle by introducing variations to it which increases its volatility.

Nomenclature

DLT	Distributed Ledger Technologies
DAG	Directed Acyclic Graph
MAM	Masked Authenticated Messaging
IIoT	Industrial Internet of Things
KPI	Key Performance Indicator
OEE	Overall Equipment Effectiveness
WIP	Work In Progress
MaaS	Manufacturing as a Service
MM	Mass Manufacturing
MC	Manufacturing Clouds
ERP	Enterprise Resource Planning
CAD	Computer Aid Design
PLM	Product Lifecycle Management
CMfg	Cloud Manufacturing
SMf	Social Manufacturing
IFS	Intuitionistic Fuzzy Sets
AHP	Analytic Hierarchicy Process

The development of strategies and tools promoting the dynamic configuration and automatic routing through manufacturing networks and facilities under cost, time and environmental constraints to support advanced integration of products by means of smart services will become a needed context in the near future. Cloud manufacturing (CMfg) emerges as a novel business paradigm for the manufacturing industry, in which dynamically scalable and virtualised resources are provided as consumable services over the Internet, in such a way to understand manufacturing activity as a service. CMfg systems can be grouped into one of three deployment modes, i.e. private cloud, community cloud, and public cloud [3]. One of the challenges in the existing solutions is that few of them are capable of adapting to changes in the business environment. However, technology-based business approaches are enablers for increased enterprise performance. For public cloud it is understood as a set of manufacturing services in which manufacturing services are available to the general public. On the other side, the private cloud becomes a centralised management effort in which manufacturing services are shared within one company or its subsidiaries. In between, it is possible to identify the community cloud, as a collaborative effort in which manufacturing services are shared between several organisations from a specific community with common concerns.

In fact, different companies may have different cloud requirements in different business situations; even a company at different business stages may need different cloud modes to better react to the constraints that the situation on the market imposes. Because of such situations it becomes relevant to transform the traditional product-oriented business model into a service-oriented business model. Such transition enables the creation of intelligent factory networks that encourage effective collaborations. Therefore, Hybrid cloud conceived as a composition of two or more clouds (private, community or public) that remain distinct entities but are also bound together, offering the benefits of multiple

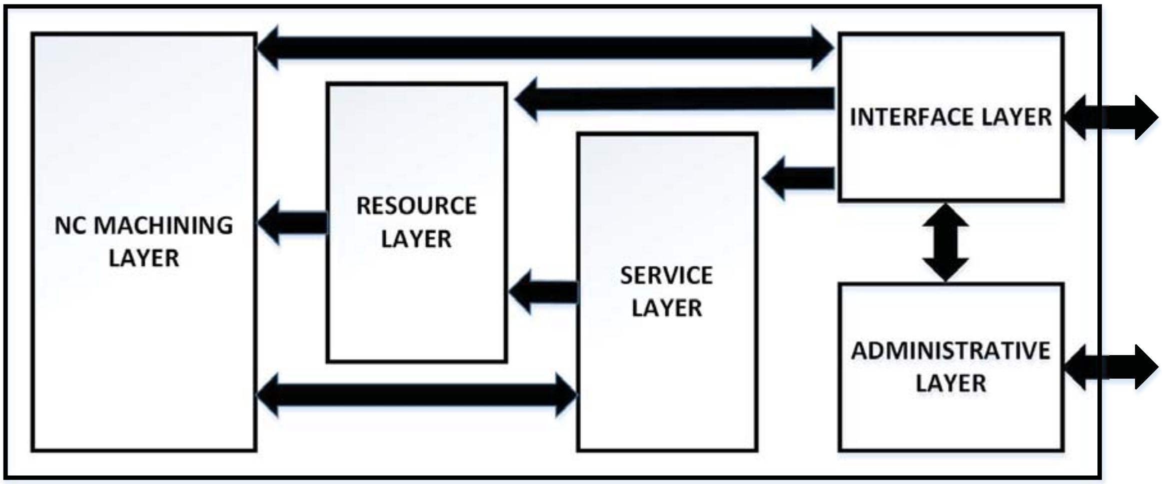

Fig. 1: Cloud Manufacturing generic architecture.

deployment modes becomes an interesting paradigm, as covers the elementary configurations but also the complex relationship between cloud functions.

For this purpose, the design and planning of manufacturing networks in mass customization and personalization landscape requires the introduction of a kind of taxonomy that contributes to the introduction of the essential functions for CMfgs. Indeed, the relationship between the functions can be identified. Adamson et al. [4] gave a Comprehensive review of the existing architecture and frameworks of Cloud Manufacturing. Although the technical solutions differ in their complexity and expandability, they share some commonalities and provide some guidance for additional research.

A cloud manufacturing system typically comprises of a resource layer, an application layer, and other layer(s) for translating manufacturing resources to manufacturing service regardless of its architecture [3]. The mapping of production performance requirements to process and production planning requires automated systems with process descriptions enabling machine to machine exchanges, which significantly challenges current systems. Such mapping applications have been allocated into the interface layer, as it handles the interactions with all the other layers and it is in charge from technical order reporting as well (see Fig. 1). Although the reference architecture can be somehow referred to the scheme presented in [3], the interest here is to enhance the relationship between layers as well as to identify the convenient layers to anchor the needed interfaces.

Extended systems such as the Monitoring system, the Enterprise Resource Planning (ERP) system, and the Product Lifecycle Management (PLM) system can also be integrated in the administrative layer, to provide essential information required by managerial functions.

Access policies are related to the administrative layer also, and they can change dynamically over time. Such changes can affect the nature of the access permitted, and the participants to whom access is available. These policies may be defined implicitly by the rules, in such a way that the Interface Layer can bring timely the required information to the different stakeholders. Interoperability is a fundamental dimension, as access policies need to be established among arbitrary parties, accommodating new participants and request types dynamically. Without interoperability, there is no guarantee that the mechanisms in use will extend to any other suitable participants.

This paper does not look to contribute on the interoperability dimension itself, but on a related topic, which is the availability of information in public CMfgs, which could also benefit hybrid ones. By extending the concept presented [3] in (Fig. 9), it is clear that web services can be the essential tool handling detailed information between production systems, and to some extension covering the service related information. However to provide just a human oriented interface through a web browser, consuming information from the CMfg internal web-server is significantly limiting the capabilities. Actually, in order to achieve the effective management, convenient use, and reliable transactions of resources and tasks, a framework of trust evaluation system in CMfg, allowing trust evaluation, oriented to mechanical manufacturing field is needed [5, 6].

Several authors [7, 8, 9] have promoted different trust/reliability evaluation methods, than can help to provide trust among participants in Hybrid CMfgs. They aim to address the specific challenges for such systems, like

- manufacturing devices are distributed among different providers, including different geographic locations.
- resources are monitored and their availability refreshed regularly.
- task resource searching and matching should be accurate.
- variety of service composition and distributed execution.

When trust/reliability is considered, not only specific information delivered to customers is required. Instead, wider range of information need to be regularly released, in order to enable independent assessment for QoS and other relevant KPIs, not compromising the business capability of the CMfg. In particular, KPIs related to enviromental performance per item class, but also those related to the on-time start processing per item of workflow or percentage of items finished on time will contribute to increase the reliability of the cloud itself. Therefore, the challenge is to get such information automatically delivered, in a trusted way, and without additional overheads or extra computing services.

2. State of the Art

The accuracy and efficiency of CMfgs has great dependency on the management, sharing, and scheduling of resources and tasks. Many studies have been conducted in order to achieve the effective management, convenient use, and reliable transactions of resources and tasks between resource service providers and consumers. Different trust evaluation frameworks and models have been created. In study [5], a framework of trust evaluation system was established and a trust evaluation model based on analytic hierarchy process (AHP) method was proposed. In this model, six trust evaluation indexes are obtained defined, including time control, economical efficiency, processing quality, service attitude, business scale, and logistic effectiveness. The research presented in [6] extended the previous trust evaluation models and proposed a new method by adopting the third-party trust evaluation model based on existing direct and indirect trust evaluation models as well as the time decay factor. This method also quantifies the fuzzy indexes by using Intuitionistic Fuzzy Sets (IFS). While these evaluation methods have been proved useful, several key challenges still remain unsolved. For instance, the lack of a service oriented description framework for product data is a thorny one [10]. To overcome this issue, semantic web technologies have been used in many studies to develop product ontologies in manufacturing domain [11, 12, 13, 14, 15].

In order to develop a service-oriented, which is not the characteristic of previous methods, product data model, the authors of [10] developed the ManuService ontology. It consists of many of the necessary concepts for description of products in a service-oriented business environment, including product specifications, quality constraints, manufacturing processes, organisation information, cost expectations, logistics requirements. It could enable a module-based, reconfigurable, privacy-enhanced and standardised approach to modelling customised manufacturing service requests. These traditional models mainly focus on modeling the attributes, interfaces, and descriptions of the resources into resource information services. Although these models are suitable for local environment, they still suffer semantic heterogeneity in open cloud environment [16]. Some recent studies [17, 18, 19] tried to create unified domain ontologies in advance and apply them in resource service models to unify the schema and eliminate the semantic heterogeneities among the services.

However, the effectiveness of these ontology-based models mainly depends on the expertise of the ontology experts in ontology designing and it is difficult to catch the dynamic changes in the cloud once the ontology has been embedded [16]. In order to overcome these limitations, a semantic model using semantic links instead of ontologies was proposed in study [16]. This model takes advantage of semantic links to enable automated integrating and distributed updating in resource service cloud. It is suitable for modeling manufacturing resources into cloud services and enables the flexible and distributed manipulation on resource services in the cloud environment.

In addition to the reliability and efficiency issues, the transformation of manufacturing industry from the traditional production-oriented approach to the service-oriented approach, envisioned by cloud manufacturing, still faces some obstacles and the the safety and security issues are two of the most concerned [20]. The networks used to support collaborations and cooperation convey business-critical information, while the virtualization and service orientation of manufacturing resources make enterprises vulnerable to a new series of attacks not seen in traditional manufacturing approaches. The productivity and reputation could be significantly affected due to the compromise of a cloud manufacturing solution caused by amateur attackers or experts. Therefore, equipping cloud manufacturing solutions with proper security management mechanisms and policies is critical to avoid such threats [21].

A distributed peer to peer network architecture could improve the safety and security of the cloud manufacturing networks. The study in [22] developed a distributed peer to peer network with high security for cloud manufacturing based on blockchain technology. With such blockchain-based system, not only customers could be connected to specific service but also can share data and information in a distributed manner. The rise and success of Bitcoin during recent years proved that blockchain technology has real-world value. However, these protocols also have several drawbacks that prevent them from being used as a generic platform for IoT data sharing in the cloud manufacturing environment, such as scalability issue, transaction fees, not fully decentralized due to large mining pools, and vulnerable to quantum attack [23]. To overcome these limitations and better protect the security of the cloud manufacturing networks, more advanced distributed network architectures are required.

3. DLT and IOTA technologies

A distributed ledger is a distributed database, maintained by a consensus protocol run by nodes in a peer-to-peer network. This consensus protocol replaces a central administrator, since all peers contribute to maintaining the integrity of the database [24]. As one of the most widespread DLT, the blockchain technology has gained substantial popularity in recent years, primarily in financial field, due to the cryptocurrencies. It has attracted the attention of the research community from different academic domains [25, 26, 27] due to its unique characteristics, such as the absence of centralized control, an assumed high degree of anonymity and distributed consensus over decentralized networks. By applying DLT to data sharing, it could dramatically simplify data acquisition process for research and commercial projects and provide an opportunity for users to gain the ownership and the privileges of their own data and get benefits from them [27]. It could also lead to better control over their data and guarantees fine-grained tracking of all their data usage activities [28].

IOTA is a tangle-based cryptocurrency designed specifically for the IoT industry where machine-to-machine data exchange is required. The tangle is the next evolutionary step of blockchain by overcoming some of its fundamental limitations in data sharing, such as scalability issue, transaction fees and vulnerable to quantum attack. The main feature of the tangle is that it uses a directed acyclic graph (DAG) for storing transactions instead of sequential blocks. In the Tangle, users must perform a small amount of computational work to approve two previous transactions in order to issue a new transaction. This new transaction will be validated by some subsequent transactions [29]. This structure of the Tangle makes possible of high scalability. There is no maximum throughput, since the more activities in the Tangle, the faster transactions can be confirmed. In addition, with this 'pay-it-forward' system of validations, there is no need to offer financial rewards. Transacting with IOTA can be completely fee-free. Moreover, IOTA has no miners, therefore it is truly decentralized.

The typical structure of the IIOT data sharing system based on IOTA Tangle and MAM is as shown in Fig. 2. This structure is composed of three layers including IIOT devices, private or public IOTA nodes and the Tangle. An IIOT device could act as data publisher or receiver, or both roles at the same time. Usually the data from several sensors in a smart environment will be integrated on a mobile computing device or a local server which is connected to a public or private IOTA node through Internet. An IOTA node is a computer connected to the Tangle network. To be a node the computer need to have at least four gigabyte RAM and enough computing capability to perform the proof-of-work required for publishing transactions to the Tangle.

IOTA provides a data communication protocol named Masked Authenticated Messaging (MAM) which adds functionality to emit and access an encrypted data stream over the Tangle regardless of the size or cost of device [30]. MAM uses channels for message spreading like many other medias. IOTA users can create a channel and publish a message of any size at any time. A small amount of proof-of-work is required to allow the data to propagate through the network and to prevent spamming. Other users can subscribe this channel through the channel address and receive a message that is published by the channel owner. The subscribers can decode and consume the message with the

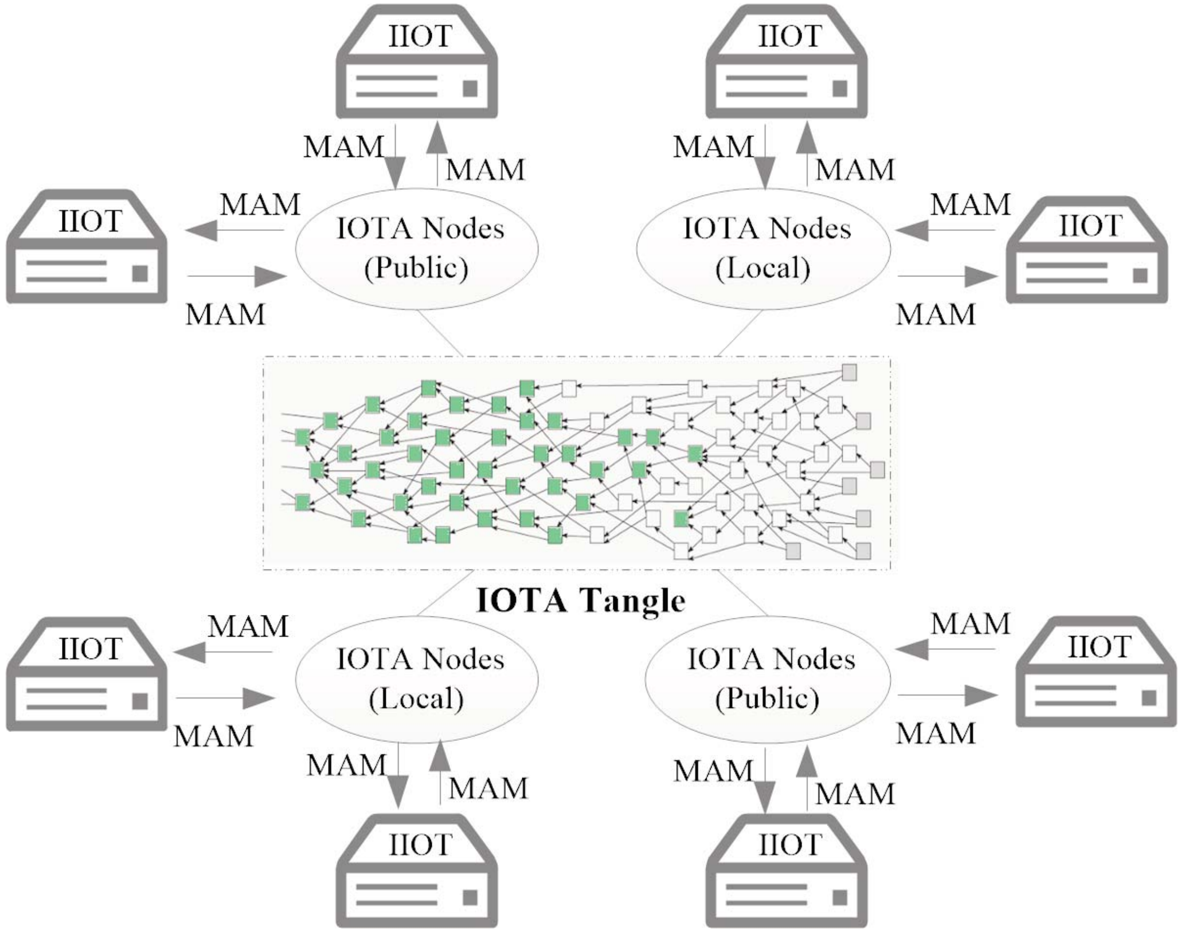

Fig. 2: The typical structure of the IIOT data sharing system based on IOTA Tangle and MAM.

channel address if the it is published in public mode, otherwise, an extra key is necessary to decrypt the message. This prevents random users from decrypting the message if they stumble across it.

The MAM communication protocol is the fundamental mechanism to protect the data security and realize flexible data access management. A signature scheme based on Merkle Hash Tree (MHT) [31, 32] is used to sign the cipher digest of an encrypted message [30]. The address of a channel is the root of this Merkle tree which itself is created using the seed of the user [23]. MAM supports three privacy and encryption modes to control the visibility and access of a channel: public, restricted and private. The public mode is used for broadcasting messages to all users in the Tangle like a public radio channel. Any user who knows the channel address can fetch and consume the message. In contrast, the private mode is used for recording data for private use only.

The restricted mode is the most commonly used in IIOT data sharing. In this mode an authorization key adopted. The address used to attach to the network is the hash of the this authorization key and the root. It enables the publisher to revoke access to future messages from subscribers by changing this key. Because in order to consume a MAM message, the receiver need to use the root to calculate the address of the transaction and fetch the masked message and Then use the authorization key to decrypt the masked message.

The IOTA foundation provides a Javascript library (https://github.com/iotaledger/mam.client.js) to implement the publishing and receiving of messages using MAM. Fig. 3 presents two examples of published message using public and restricted MAM mode respectively. It is shown in Fig. 3 (a) that, in public mode, the root and the address are the same, while they are different in restricted mode as shown in Fig. 3 (b). More technical details about publishing

```
Root:  IDTGV9BUO9BDHLNVCQPWXXPJAZHWX99KWQLPBBSIVNCLOEPOJVILLOUMZJJZJF9NOTAIMIQZYPIDESJOO
Address:  IDTGV9BUO9BDHLNVCQPWXXPJAZHWX99KWQLPBBSIVNCLOEPOJVILLOUMZJJZJF9NOTAIMIQZYPIDESJOO
waiting_time:18191
location: Celsa Group Office, timestamp: 2019-01-09 00:02:00, pm2_5: 12.286, pm10: 13.143,tv
oc: 0.036, co2: 0.2, temperature: 26.7, humidity: 14.913,illumination: 0.0, noise: 66.897, h
cho: 0.02, co: 0, c6h6: 0.0, no2: 0, o3: 0
```

(a) Published message using public MAM mode

```
Root:  TQERCS9CVORDZDADSZMPFUSOYYHHLCTMLTEOPYYNOJSIGGCSNDIUVB9TKNAXUHUAEGHKXXOEVCLDJKJSI
Address:  CXDZEWQPZSJNAZY9KGAZAGVILDHCFOTCWEACPCYDXHUFOTZRNQGXEQQWFERFHCIGFNNGYHGPHCQUNMDUA
waiting_time:8325
location: Celsa Group Office, timestamp: 2019-01-09 00:00:00, pm2_5: 10.5, pm10: 10.833,tvoc
: 0.034, co2: 0.2, temperature: 26.7, humidity: 14.925,illumination: 0.0, noise: 75.257, hch
o: 0.02, co: 0, c6h6: 0.0, no2: 0, o3: 0
```

(b) Published message using restricted MAM mode

Fig. 3: Two examples of published messages using different MAM modes

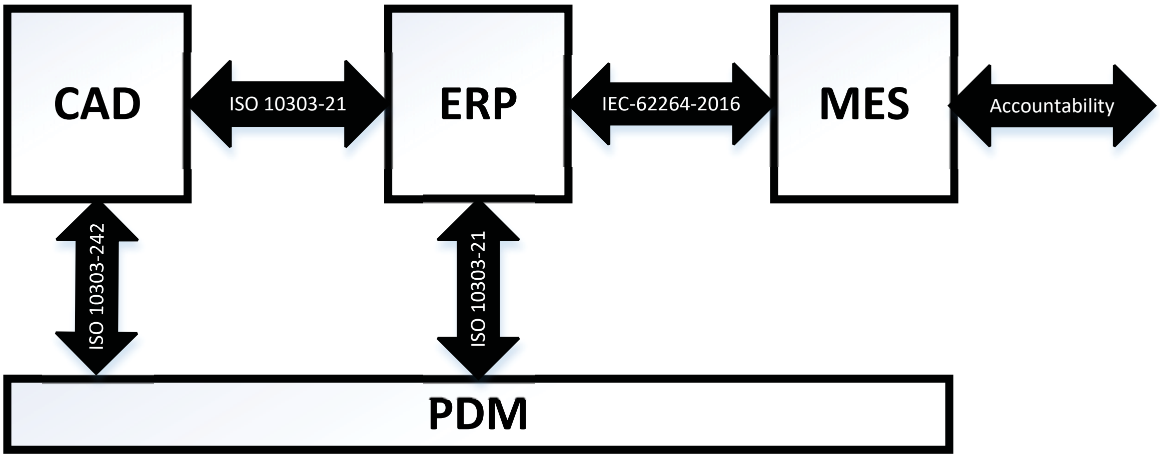

Fig. 4: Information exchange between relevant systems for CMfg.

and receiving data over the Tangle using MAM are introduced in our previous work [23] and the complete Javascript codes are available online (https://github.com/zhengxiaochen/iota_mam_data_sharing).

4. Application to CMfg systems

There are different information systems allowing to exchange information at different levels (CAD, PDM, ERP, MES) (see Fig. 4), which facilitate the CMfg interoperability among agents.

In addition to the technical exchange of information as presented in Fig. 4, which is helpful between agents linked by contracts in the CMfg to produce agreed products, an additional layer of data is needed to have different stakeholders informed about different items, with variable frequencies and not requiring previous agreements or data access to private services. The presented IOTA technology can be useful to deliver regularly information about relevant KPIs of the CMfgs, in accordance to the previously required constraints, because of the two modes, messages to the tangle and MAM streaming.

Therefore, according to the relevant KPIs for the CMfg, a layer in its information system related to the MES will share such values. The immediate effect is that agents can be aware of the specific level of information distributed, that can be related to different dimensions and aggregation level:

- Performance indicators like OEE, WIP, etc.
- Energy/Environmental indicators like CO_2/hour, etc.
- Other relevant factors decided by CMfg managers.

Distributed information about CMfg characteristics enable different agents to better elaborate their decisions involving such knowledge, because of the information can become helpful either the auditors, or potential customers, public agencies or different organizations. A prototype has been created to distribute information related to polution in indoor working areas.

5. Conclusions and future Implications

In this paper the CMfg configuration was reviewed and different aspects and significant dimensions were highlighted, like interoperability, trust, timely information, etc. The identification of relevant information systems and standards making it possible the interactions provides enough room for additional information layer, responsible for additional value contributing to increase the trust levels and the interoperability.

The proposal is based on public Distributed Ledger Technologies, where no specific and secured access is required because the information is created from the MES system and published on public IoT oriented solutions. Doing so, different agents and usages are enabled for further developments, without compromising the access to the resources or being exposed to specific attacks when information is accessed.

The business possibilities that publishing IIoT Data offer are quite promising and range from a higher reliability and more stable topology of structural and functional manufacturing networks, more trustworthy cooperation between manufacturing network partners, and subsequently a more environmentally friendly manufacturing networks due to a higher transparency of information flow and the more effective resource-management that goes with it.

Acknowledgements

The authors acknowledge to the EU RFCS program for funding the research project WISEST with ID 793505, which supports partially this research. Also they recognize the support from the Spanish Agencia Estatal de Investigacin, through the research project with code RTI2018-094614-B-I00 into the Programa Estatal de I+D+i Orientada a los Retos de la Sociedad".

References

[1] X. Shang, X. Liu, G. Xiong, C. Cheng, Y. Ma, T. R. Nyberg, Social manufacturing cloud service platform for the mass customization in apparel industry, in: Proceedings of 2013 IEEE International conference on service operations and logistics, and informatics, Ieee, 2013, pp. 220–224.

[2] D. Mourtzis, M. Doukas, Design and planning of manufacturing networks for mass customisation and personalisation: challenges and outlook, Procedia Cirp 19 (2014) 1–13.

[3] Y. Lu, X. Xu, J. Xu, Development of a hybrid manufacturing cloud, Journal of Manufacturing Systems 33 (4) (2014) 551–566.

[4] G. Adamson, L. Wang, M. Holm, The state of the art of cloud manufacturing and future trends, in: ASME 2013 international manufacturing science and engineering conference collocated with the 41st North American manufacturing research conference, American Society of Mechanical Engineers, 2013, pp. V002T02A004–V002T02A004.

[5] C. Li, S. Wang, L. Kang, L. Guo, Y. Cao, Trust evaluation model of cloud manufacturing service platform, The International Journal of Advanced Manufacturing Technology 75 (1-4) (2014) 489–501.

[6] K. Yan, Y. Cheng, F. Tao, A trust evaluation model towards cloud manufacturing, The International Journal of Advanced Manufacturing Technology 84 (1-4) (2016) 133–146.

[7] Y. Feng, B. Huang, A hierarchical and configurable reputation evaluation model for cloud manufacturing services based on collaborative filtering, The International Journal of Advanced Manufacturing Technology 94 (9-12) (2018) 3327–3343.

[8] F. Tao, Y. F. Hu, Z. D. Zhou, Application and modeling of resource service trust-qos evaluation in manufacturing grid system, International Journal of Production Research 47 (6) (2009) 1521–1550.

[9] K. Mubarok, X. Xu, X. Ye, R. Y. Zhong, Y. Lu, Manufacturing service reliability assessment in cloud manufacturing, Procedia CIRP 72 (2018) 940–946.

[10] Y. Lu, H. Wang, X. Xu, Manuservice ontology: A product data model for service-oriented business interactions in a cloud manufacturing environment, Journal of Intelligent Manufacturing 30 (1) (2019) 317–334.

[11] M. Dong, D. Yang, L. Su, Ontology-based service product configuration system modeling and development, Expert systems with applications 38 (9) (2011) 11770–11786.
[12] K.-Y. Kim, D. G. Manley, H. Yang, Ontology-based assembly design and information sharing for collaborative product development, Computer-Aided Design 38 (12) (2006) 1233–1250.
[13] H. Panetto, M. Dassisti, A. Tursi, Onto-pdm: Product-driven ontology for product data management interoperability within manufacturing process environment, Advanced Engineering Informatics 26 (2) (2012) 334–348.
[14] J. Lee, H. Chae, C.-H. Kim, K. Kim, Design of product ontology architecture for collaborative enterprises, Expert Systems with Applications 36 (2) (2009) 2300–2309.
[15] Y. Zhang, X. Luo, J. Li, J. J. Buis, A semantic representation model for design rationale of products, Advanced Engineering Informatics 27 (1) (2013) 13–26.
[16] C. Xie, H. Cai, L. Xu, L. Jiang, F. Bu, Linked semantic model for information resource service toward cloud manufacturing, IEEE Transactions on Industrial Informatics 13 (6) (2017) 3338–3349.
[17] H. Dibowski, K. Kabitzsch, Ontology-based device descriptions and device repository for building automation devices, EURASIP Journal on Embedded Systems 2011 (2011) 3.
[18] J. Ploennigs, A. Schumann, F. Lécué, Adapting semantic sensor networks for smart building diagnosis, in: International Semantic Web Conference, Springer, 2014, pp. 308–323.
[19] Y. Evchina, J. Puttonen, A. Dvoryanchikova, J. L. M. Lastra, Context-aware knowledge-based middleware for selective information delivery in data-intensive monitoring systems, Engineering Applications of Artificial Intelligence 43 (2015) 111–126.
[20] D. Wu, M. J. Greer, D. W. Rosen, D. Schaefer, Cloud manufacturing: Strategic vision and state-of-the-art, Journal of Manufacturing Systems 32 (4) (2013) 564–579.
[21] C. Esposito, A. Castiglione, B. Martini, K.-K. R. Choo, Cloud manufacturing: security, privacy, and forensic concerns, IEEE Cloud Computing 3 (4) (2016) 16–22.
[22] Z. Li, A. V. Barenji, G. Q. Huang, Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform, Robotics and Computer-Integrated Manufacturing 54 (2018) 133–144.
[23] M. R. V. R. O.-M. J. Zheng X, Sun S, Integrating iot and distributed ledger technologies to accelerate health data sharing: A solution based on iota tangle and mam, Journal of Medical Internet Research, Preprints 01/02/2019:13583 (2019).
[24] J. Brogan, I. Baskaran, N. Ramachandran, Authenticating health activity data using distributed ledger technologies, Computational and Structural Biotechnology Journal 16 (2018) 257–266.
[25] R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, Journal of Economic Perspectives 29 (2) (2015) 213–238.
[26] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. Mukkamala, R. Vatrapu, Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning, in: Proceedings of the 51st Hawaii International Conference on System Sciences, 2018.
[27] X. Zheng, R. R. Mukkamala, R. Vatrapu, J. Ordieres-Mere, Blockchain-based personal health data sharing system using cloud storage, in: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2018, pp. 1–6.
[28] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, et al., Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare, Oncotarget 9 (5) (2018) 5665.
[29] S. Popov, The tangle, iota.org (2018) 131.
[30] P. Handy, Introducing masked authenticated messaging, IOTA Foundation Medium blog (2017).
[31] R. C. Merkle, A certified digital signature, in: Conference on the Theory and Application of Cryptology, Springer, 1989, pp. 218–238.
[32] R. C. Merkle, A digital signature based on a conventional encryption function, in: Conference on the theory and application of cryptographic techniques, Springer, 1987, pp. 369–378.