

# *IET Collaborative Intelligent Manufacturing* Special issue Call for Papers

---

**Be Seen. Be Cited.  
Submit your work to a new  
IET special issue**

Connect with researchers and  
experts in your field and share  
knowledge.

Be part of the latest research  
trends, faster.

[Read more](#)



The Institution of  
Engineering and Technology

## ORIGINAL RESEARCH

# Trusted and secure composite digital twin architecture for collaborative ecosystems

Pasindu Manisha Kuruppuarachchi<sup>1</sup>  | Susan Rea<sup>2</sup> | Alan McGibney<sup>2</sup>

<sup>1</sup>Department of Computer Science, Munster Technological University, Cork, Ireland

<sup>2</sup>Nimbus Research Center, Munster Technological University, Cork, Ireland

## Correspondence

Pasindu Manisha Kuruppuarachchi, Department of Computer Science, Munster Technological University, Rossa Avenue, Cork, Munster T12 P928, Ireland.  
Email: [p.kuruppuarachchi@mycit.ie](mailto:p.kuruppuarachchi@mycit.ie)

## Funding information

Science Foundation Ireland, Grant/Award Number: 18/CRT/6222

## Abstract

Digitalisation creates new opportunities for businesses to implement and manage collaborative ecosystems both internally and externally. Digital twin (DT) is a rapidly emerging technology that can be used to facilitate new models of interaction and sharing of information. DT is the digital version of a physical process or asset that can be used to model, manage, and optimise its physical counterpart. Connecting multiple DTs is vital to provide a holistic integration and view across complex ecosystems. To create a DT-based collaborative ecosystem architecture, the following concerns need to be addressed. Trust is a fundamental requirement because multiple parties will work together as part of a composite DT. Interoperability is essential, as DTs from various domains will be required to interconnect and operate seamlessly. Finally, the governance is challenging as different scenarios require various mechanisms and governance structures. This study presents an architecture to enable multiple DT-based collaborative ecosystems, and example use case scenarios to demonstrate its applicability in collaborative manufacturing.

## KEYWORDS

composite digital twin, digital ecosystems, digital twin, governance, interoperability, trust

## 1 | INTRODUCTION

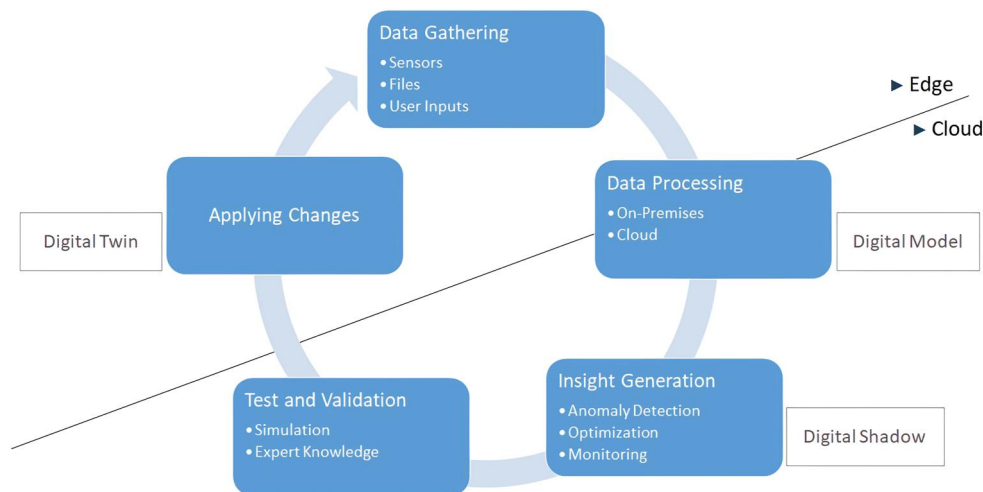
The definition of DT currently varies across the literature. In 2002, Michael Grieves defined the term DT focusing on product life cycle management [1, 2]. Other interpretations of the term DT are an object-oriented model of a physical asset that contains all the relevant information about the physical asset [3]; modelling and simulation-based mirror of the physical twin [4]; digital representation of an asset, process, or system that captures a physical counterpart behaviour [5]. Kritzinger et al. [6] describe the DT as an evolution of the concept of connecting physical and digital models. The starting point is a DM, an information model that describes the physical asset in a digital form. There is no automated communication channel between physical objects and digital objects. The DM will only hold information related to the physical object. This concept evolves towards an entity termed a digital shadow (DS). As the name suggests, DS is a real-time data copy of a physical asset. Unlike the DM, DS

communicates with its physical asset and keeps updating the state of the asset. DS can support applications such as real-time monitoring and visualisation to provide insights into the behaviour of the physical assets. The more data harvested from the physical asset, the richer the digital asset gets. According to Kritzinger et al., the step towards DT is where the communication is bi-directional. Considering all the available definitions and interpretations, DT can be summarised as a 'digital representation of a real-world object or process covering the entire object life cycle and offers seamless communication to enhance its physical counterpart' [7].

A common trait of implementing these concepts is availability and access to data extracted from the physical environment. Figure 1 shows DM, DS, and DT concepts, respectively, and how they are positioned in a data value chain context. The DM will mainly be placed in the data processing phase while DS moves one step above to generate valuable insights about the physical asset. Finally, the DT will apply the changes back to the physical asset after verifying the changes

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

© 2022 The Authors. *IET Collaborative Intelligent Manufacturing* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.



**FIGURE 1** Different concepts and their role in the digital value chain

using simulation and optimisation models. This will improve the quality of the physical counterpart operations and minimise destruction to the operations because of the simulated environment to validate the applicability of the changes.

DT concept is receiving significant attention from both academia and industry. Various sectors, including health [8], intelligent cities [9], smart manufacturing [3–5], and energy management [10, 11], explored the possibilities of using DTs. Smart manufacturing shows more significant interest in the benefits of the DT, such as data-driven insights and automation, support to manage competitive manufacturing demands, cost-effectiveness using optimised manufacturing processes, sustainable production, and integration of complex supply chains. Lockheed Martin<sup>1</sup> has developed a digital twin maturity model (DTMM) [12], as shown in Figure 2, that allows researchers and industrial decision-makers to understand the level of maturity required in their DTs. The DTMM encapsulates five levels of maturity. A level 1 DT is more like a DM used to simulate and create virtual prototypes. Levels 2 and 3 can be represented as a DS, where data communication is supported only in one direction. Level 4 is equivalent to DT, which supports capturing the data from the physical counterpart and providing learning to improve the physical counterpart.

Connecting multiple DTs is presented in level 5 of the DTMM. This means DTs will communicate with other DTs and create a digital ecosystem to support physical level operations. This opens up a new set of possibilities to develop cross-domain systems that enable digitisation of an entire system regardless of the industry/locations/organisations, thus aiding in breaking operational silos. The DTMM level 5 is akin to what is referred to within this work as composite digital twins (CDTs).

CDT is still an emerging concept. There is a need to explore the challenges and concerns in detail for connecting multiple DTs, regardless of the technologies used to

implement, industry, organisation structures, locations etc. As such, this study will make the following contributions:

- 1) Conduct a comprehensive state-of-the-art analysis to identify and summarise the CDT requirements, considering operational, management, and security needs.
- 2) An architecture specification for CDT that enables creating trust and secure CDT for collaborative ecosystems.
- 3) Present potential real-world use case scenarios and discuss how the proposed architecture can enable and address the challenges of these use cases.

The remainder of this study is structured as follows: Section 2 will present an overview of related work and highlight the research gaps. Section 3 outlines the proposed CDT architecture to overcome the current challenges from an implementation and management perspective. Section 4 will present the implementation challenges of concrete architecture deployment. Section 5 will present three use case scenarios to highlight the capabilities of the CDT architecture. Finally, the learning outcomes and future perspectives are summarised in Section 6.

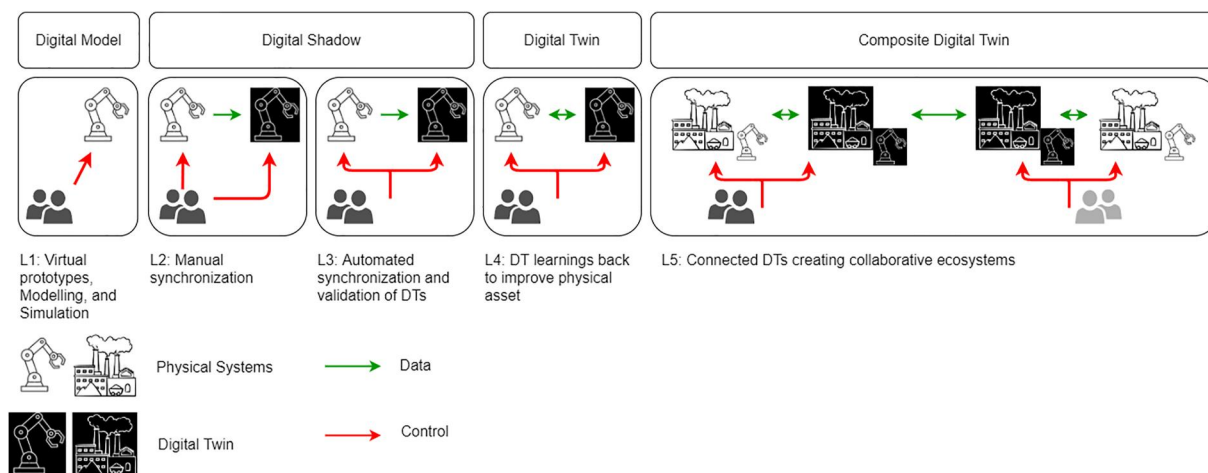
## 2 | RELATED WORK

The main focus of this study is to explore the architectural requirements for enabling DT-based collaborative ecosystems in a trusted and secure manner. To describe the connection of multiple DTs, the following terms are used in the literature review: federated DT [13–18], integrated DT [19, 20], system of systems DT [21–23], composable DT [24, 25], and collaborative DTs [26, 27]. The term CDT [5] is used throughout this study to represent the interconnection of discrete DT to create new collaborative applications.

Based on a review of these concepts in the literature, governance, trust, and interoperability were highlighted as primary concerns for creating a DT-based collaborative ecosystem [7].

<sup>1</sup><https://www.lockheedmartin.com/>.





**FIGURE 2** DM, DS, DT, and proposed CDT concept placement in the Lockheed Martin DTMM [12]. CDT, composite digital twin; DM, digital model; DS, digital shadow; DT, digital twin

- 1) **Governance**: Managing and coordinating many parties, processes, and policies are essential for CDT. Based on the requirements/needs of individual DTs, keeping all the participants aligned with the CDT goals requires a robust governance strategy. This will ensure that everyone in the CDT ecosystem is aware of their responsibilities and contributions.
- 2) **Trust**: As various stakeholders will be involved in collaborative interactions as part of the overall CDT ecosystem, trust is a crucial consideration. Trust representation provides a system to ensure that participants act as expected and contribute to achieving CDT goals.
- 3) **Interoperability**: It remains a significant barrier when aiming to have systems that link and function together, as separate systems tend to adhere to different standards, information models, protocols etc. (such as in CDT). This is particularly challenging when systems operate across organisational, security, and infrastructure boundaries.

While literature considers these challenges to varying degrees of detail and for different application cases, there is no solution that considers all architectural concerns holistically. Performance overhead, scalability, and complexity of incorporating all three concerns into one solution make it a challenging problem to solve. While the connection and integration of multiple DTs is still emerging as a specific use case, there have been significant contributions to the state of the art that focus on a system of systems and data integration across systems.

## 2.1 | Governance

Governance is considered the foundation of any collaborative ecosystem, and it defines the policies and procedures for operating the ecosystem to achieve common CDT goals in a secure environment. The most fundamental policies will govern CDT joining requirements, sensitive data management (e.g. encryption methods), access control (e.g. role-based), and authorisation

(e.g. participant privilege groups). Governance is also responsible for the specification of procedures for updating a policy, participant voting for new changes, conflict resolution etc.

Two types of governance structures are discussed in the literature, namely, centralised and decentralised [28]. Considering the possible CDT applications, a hybrid governance structure that encapsulates both centralised and decentralised governance characteristics is required.

### 2.1.1 | Centralised governance structure for CDT

In a centralised approach, one or more privileged groups of participants make the decisions for everyone in the ecosystem. This will create different levels of participant groups, and responsibilities will be assigned based on their group privileges. One of the best examples to explain this is multiparty product manufacturing. In multiparty manufacturing, many manufacturers work together to build one product. This can also be categorised as a supply chain problem. For example, one party is the product owner, and due to current market demands, the product owner will outsource some parts of the product to other manufacturers. Since a single party manages this CDT, they can dictate the rules, and other manufacturers can negotiate and participate in the CDT. This kind of CDT does not have a dynamic participant joining as the CDT owner will maintain control over all participants. However, in this example, one owner will govern the entire CDT, while in some cases, there will be more than one party holding the responsibility of the governance, but still being controlled using a centralised approach.

### 2.1.2 | Decentralised governance structure for CDT

Decentralised CDT is a collection of DTs interacting to achieve mutual benefiting goals. For example, in autonomous vehicle platooning, multiple vehicles can interact with each

other to share the destination that they are travelling to and environmental conditions such as road, traffic, etc. [29]. This dynamic operating scenario will require vehicles to create collaborative ecosystems that can operate on a temporary basis. All vehicles will try to achieve their goals, such as reaching their destinations effectively and making operations economically via utilisation of fuel and resources. In this scenario, there is no governing group, and all the participants will govern the CDT collectively based on the agreement that everyone is agreed upon. A decentralisation governance structure is more suitable for this scenario because a large number of autonomous vehicles can be connected without the need for a centralised authority. This will allow for high scalability and less time to make connections with other DTs.

### 2.1.3 | Hybrid governance structure for CDT

A hybrid approach allows some parts of the CDT to be operated in a centralised way and some parts to be operated in a decentralised manner. The main advantage of hybrid governance is that CDT creators can maintain control over some aspects, such as the administration of CDT policies and joining criteria, using a specific group of stakeholders and leave some aspects to be defined based on the direct interactions between participants (e.g. data sharing frequencies and data ownership). For example, consider a wind farm scenario; multiple wind turbines will operate to generate power. DT can help the operational and maintenance teams to gather data and perform various optimisation tasks to generate electricity more efficiently [30]. When the wind turbines work collectively, they can share data that helps other wind turbines to prevent operational disruptions. Connecting wind turbines also helps to harvest more energy by leveraging one wind turbine's wind drag and optimising it to rotate another wind turbine effectively [31]. Considering an extension to the wind turbine scenario to include additional energy generation methods such as solar, natural gas, hydro-power etc. In that case, one group, such as the ministry of energy, can create a CDT to enable communication between different power-generating sectors. That means CDT will operate under centralised governance. The ministry will control the operation of the CDT. Connecting similar power sources like wind turbines can use decentralised governance and a centralised structure to group them by source, ownership, geography etc. This will create different levels of governance in one scenario.

The centralised management is based on a controlling authority, however, considering a single point of failure, trust, single authorisation, and data ownership concerns are raised in centralised systems [32]. To address these issues, a decentralised governance structure is introduced. However, centralised governance still remains the most utilised approach in practice due to privacy and data sharing issues, collective accountability concerns, resistance to changing operating practices, and technological maturity for complete decentralisation [33].

The current state of the art is exploring distributed ledger-based technologies to address the problems of centralised

systems and concerns about complete decentralised governance. Distributed ledgers will improve overall transparency by openly sharing the ledger while using cryptographic key-based signing, which helps to keep participants accountable for actions [32]. Current literature uses decentralisation for collecting data [33–35], while some use distributed ledgers to hold access control information among participants [28] transparently. However, none of the studies discuss how to govern a centralised system structure while incorporating transparency using distributed ledgers. This requires a hybrid governance structure supporting both centralised and decentralised characteristics. One survey report also suggests that industry expert participants did not favour complete decentralisation for a framework proposed to create DTs [33].

Considering the current state of the art related to governance structures in similar concepts, the following conclusions can be drawn.

- **Support for multiple governance structures:** current architectures do not facilitate both centralised and decentralised characteristics in the same architectural design. Implementations tend to be polarised into one or the other. Those papers do not support hybrid governance structures, it is our view that these will be a critical requirement in future collaborative business models.
- **Ability to change governance structures:** Based on the [33] survey results, there are some doubts regarding implementing systems in a completely decentralised architecture. The ability to change the governance structure will provide greater flexibility by incorporating the ability to adapt to changing operating conditions over the course of time. This will ease the stigma behind giving total authority to everyone and provide support for new, emerging collaborative business models.

## 2.2 | Trust

Collaborating with external parties can often be viewed as a risk, as external organisations may have different operating environments, standards and practices, policies, and intentions. Therefore, most collaborations are initiated with trusted known parties. However, current systems rely on third-party systems and data sets. This creates operational challenges and demands collaborations in trustless environments [32, 36]. The definition of trust can be subjective; however, for computer systems, trust is not taking advantage of the trustor's vulnerable position when sharing information [36] or providing a service to a trustor to satisfy its needs and expectations [37].

This definition also holds in the context of CDT. A trustor DT wants to get the information or services as expected from another DT. In an ideal situation, centralised CDT will be formulated between trusted parties. However, CDT needs robust trust and security measures to ensure everything will operate as expected regardless of the CDT type because bad actors can attack the systems both internally and externally.

### 2.2.1 | Evaluating trust in systems

There are two different ways to ensure a given system is trustworthy, Trust by design (belief base) [38] and computational system trust evaluations [37, 39].

## Trust by design

In trust by design, system implementation needs to ensure all the components and uses will behave as expected most of the time and adversary disruption is kept to a minimum level. Hence, trust by design strategies starts early in the system ideation phase. In the design phase, it is crucial to ensure all the components are designed, keeping trust as one of the core requirements. To facilitate this, there are a number of system design and implementation support artefacts analysis tools available [39–42]. The Industrial IoT Consortium (IIC) has introduced the Security Maturity Model (SMM) to help system owners ensure the system's security is up to some level that stakeholders agreed upon and is undergoing continuous improvement. However, the SMM does not stop in the analysing system implementation phase while continuing throughout the system operation through to system decommissioning. Hence, some subdomains such as threat modelling and risk assessment, supply chain, and dependency management are captured within the SMM to ensure the system is trusted by design [43].

Most recent literature uses DLT to achieve trust as the DLT implementation helps to keep all the participants accountable for their actions and transparent [26, 33–35, 44]. Most of these characteristics address trust concerns because immutability means no one can change once the transactions are recorded in the ledger. Furthermore, the use of cryptographic keys and other security mechanisms ensures non-repudiation, as such, it is extremely difficult and resource intensive to imitate another party, as such, the system can hold the participants accountable for their actions. Considering all these factors, the current state of the art favours Blockchain technology to resolve trust issues between participants [34, 35].

Zero trust is another trust-by-design concept. In traditional network security, internal networks are considered trusted because they are controlled by the organisation. However, bad actors can disrupt the systems both externally and internally [45]. In the zero-trust concept, there are no trusted areas. Instead, always evaluate and approve the actions. This may be good for some system implementations; however, this will affect the performance [46].

### Computation-based trust evaluations

In some CDT environments, multiple DTs will interact with others in an ad hoc manner. Therefore, trust must be analysed before starting communication and throughout the operation to ensure all connected DTs operate as expected. Examples of computation-based trust include quality of service (QoS) analysis [32, 47–49], ranking, and reputation management based on past behaviours [17, 37, 38, 48, 49].

Another way of computing trust is based on the behaviour of the system, Ref. [50] proposes a DT-based

goal analyser. Trust is calculated by common goals the system will achieve. In this case, an autonomous vehicle will evaluate trust based on the goals set by the ecosystem, such as lowering fuel consumption, preventing accidents, vehicle platooning to reduce air drag etc. If autonomous behaviours deviate, these goal systems will raise flags about vehicle trust. This is one of the effective ways to evaluate trust, but it is required to define all possible action scenarios based on the ecosystem goals.

Reference [48] proposes an approach utilising operative contexts to analyse trust. There are three operative contexts: user, resource, and organisation. User operative context is mainly about minimising attacking possibilities. Hence, security protocols, encryption technologies, digital signatures, and tokens will be considered in the user-operative context. Resource operative context will analyse the systems' capability to deliver quality service. Higher QoS provides a predictable service to all users. Service level agreements, usage, and procurement-related parameters are considered for the organisation operative context. This is more aligned with the organisation's legal capabilities to take responsibility for its actions. Even though this study highlights other potential requirements that can be considered, it only uses resource operative context (QoS) for its analysis [48].

The IIC defines trust as safety, security, privacy, reliability, and resilience [29]. Some of these characteristics, such as safety and privacy, are heavily controlled by government authorities to ensure all the organisations follow proper guidelines. For example, the European General Data Protection Regulation (GDPR<sup>2</sup>) is responsible for data protection and privacy in the European Union and European Economic Area. IIC trust characteristics are somewhat generic for many industrial applications, but trust also has an industry-specific viewpoint. Barrane et al. conducted an interview-based survey to identify essential factors for multi-stakeholder trust [51]. According to this survey, many criteria define trust between two stakeholders, such as industry type, previous experiences, and perception. The most common trust-related concerns are operation accountability, partnership goals, and long-term relationship focus. However, operational accountability can be achieved through systematical implementation, but partnership goals and long-term focus are highly subjective. Considering CDT, operational accountability needs to be addressed using architectural components to ensure all the participating DTs will act as expected. However, partnership goals and the long-term vision for the CDT will depend on the use case.

A CDT ecosystem architecture must integrate both trust by design and computational-based trust. While currently, DT specific trust analysing methods are not commonly implemented, existing trust concepts can be leveraged to implement a CDT ecosystem.

<sup>2</sup><https://gdpr-info.eu/>.

## 2.3 | Interoperability

Interoperability across different domains, standards, and practices signifies one of the main challenges of CDT and plays a significant role in the success of enabling collaborative ecosystems. Different organisations, such as International Organization for Standardisation (ISO)<sup>3</sup>, Digital Twin Consortium (DTC)<sup>4</sup>, and Industrial Digital Twin Association (IDTA)<sup>5</sup> have come forward to initiate a discussion with industry, academia, and other interested stakeholders to implement standards and practices.

ISO has specified a standard ISO 23247-1:2021 Automation systems and integration DT framework for the manufacturing domain [52]. This standard presents a reference architecture for DTs. It supports the idea of connecting multiple DTs by introducing an interface to connect other DTs in the architecture. This four-part document provides basic conceptual ideas and uses case-based implementation suggestions.

The DTC aims to address DT-related concerns in other domains by initiating working groups consisting of industry leaders, academia, and other interested parties. To date, the DTC has generated publications to aid early adaptors in understanding the DT concepts.

The IDTA is also working in the manufacturing domain and specifically addresses problems raised in Industry 4.0. The IDTA uses Asset Administration Shell to represent information related to the physical asset and share it as a common information model with other stakeholders.

Microsoft introduces a Digital Twin Definition Language (DTDL)<sup>6</sup> to describe DTs and help create DTs in their Azure cloud platform. The DTDL is a JSON-based design as well as useable in Resource Description Framework systems. This will improve the interoperability with other systems. However, there is no information that other vendors using DTDL for their platform or whether it is a universal standard for DTs.

As discussed, II-B, a distributed ledger is identified as a potential solution for improving the system's trustworthiness. Dib et al. has identified distributed ledgers as a potential solution to interoperability concerns [53]. Since all participants share the distributed ledger in the system, they can use it to share information between participants. This way, the distributed ledger will act as a common information-sharing medium.

Trust, interoperability, and governance are considered the main concerns for enabling the connection of multiple DTs to create collaborative ecosystems [7]. Section 2 presented a state-of-the-art review to highlight current issues related to the lack of architectural support for multiple governance structures, interoperability, and the need to improve trust considering architectural designs both at systems and individual DT levels.

## 3 | COMPOSITE DIGITAL TWIN ARCHITECTURE

Figure 3 represents the proposed CDT architecture to enable collaborative ecosystems incorporating trust, interoperability, and governance as the primary architectural concerns. This section will summarise architecture components to highlight how the proposed architecture addresses the architectural requirements identified in Section 2, further details can be found in Ref. [7].

The proposed architecture has two main tiers: digital twin connector (DTC) and composite digital twin ecosystem network (CDTEN). The DTC is responsible for facilitating the required services for individual DTs to connect to CDT ecosystem. The CD TEN will assist in governing all participating DTs in a secure, trusted manner. Composite digital twin governance policy (CDTGP) is one of the main functional components in the CD TEN and specifies each participant's rules and responsibilities. CDTGP is also used to maintain the main operational details such as the type of encryption for communication, supported data schemas, data ownership information, etc. Governance service (GS), observer service, trust management service, and common data services (CDS) are other functional blocks in the CD TEN. Another notable feature in the proposed architecture is leveraging the distributed ledgers to track both transactions for CDT data as well as recording immutable records of governance data. Since the proposed architecture needs to support multiple governance structures, it is essential to have the flexibility to separate governance related transactions from the general CDT transactions. For example, in a centralised governance structure, only selected parties will access this ledger, while in a decentralised governance structure, everyone will have access to both the ledgers.

In a CDT collaborative ecosystem, trust and security need to be considered holistically, as well as individual data feeds between ecosystem participants and the need to build up their trust and reputation while providing services as expected. The proposed architecture includes both trust by design and computational-based trust. Introducing distributed ledgers will implement the CDT in trust by design, while a proactive trust and security analyser service compute and evaluates the trustworthiness of individual DTs. Distributed ledger features such as immutable records and cryptographic keys based on non-repudiation methods help systematically prevent untrusted activities and make participants accountable for their actions. This can be categorised as control level trust and security as multiple participants are responsible for controlling the ecosystem. At a data level, the trust and security analyser will define individual DT trust and security posture based on the following categories:

- Security
- Resilience
- Reliability
- Dependency and uncertainty
- CDT goals (strategical and operational)

<sup>3</sup><https://www.iso.org/standard/75066.html>.

<sup>4</sup><https://www.digitaltwinconsortium.org/>.

<sup>5</sup><https://industrialdigitaltwin.org/en/>.

<sup>6</sup><https://learn.microsoft.com/en-us/azure/digital-twins/concepts-models>.



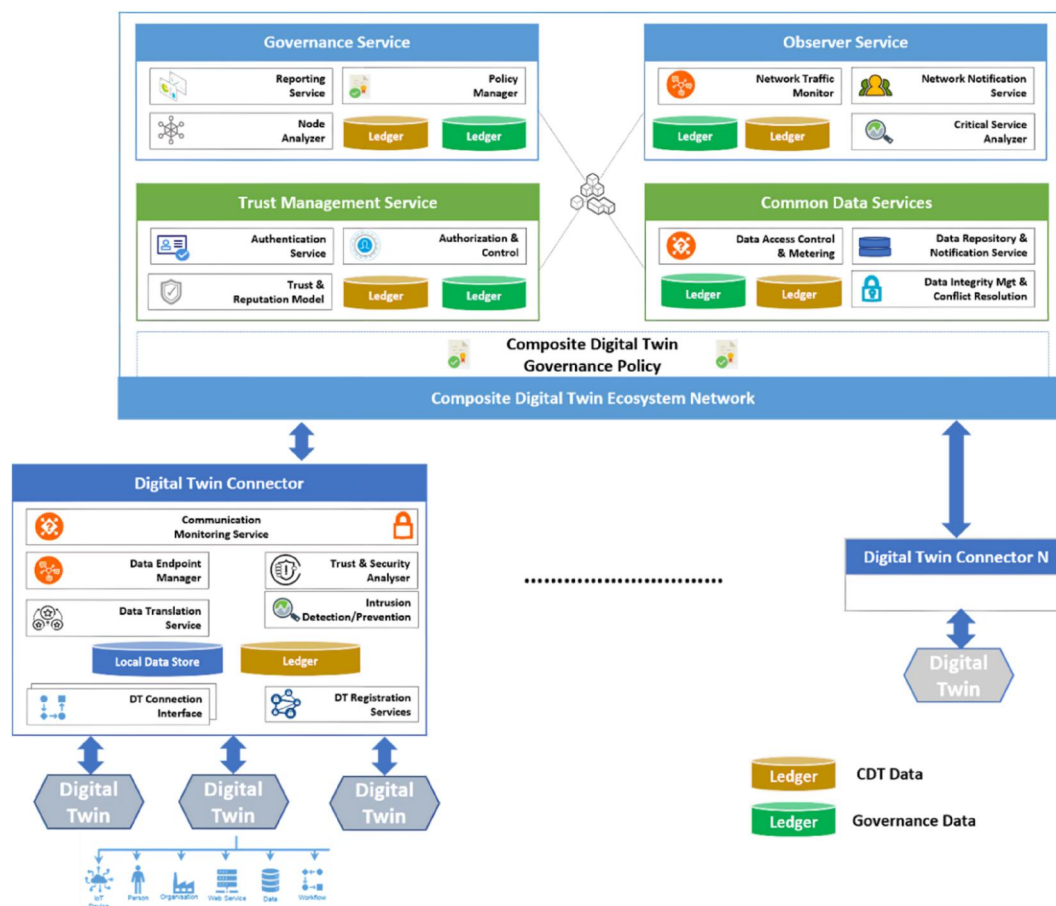


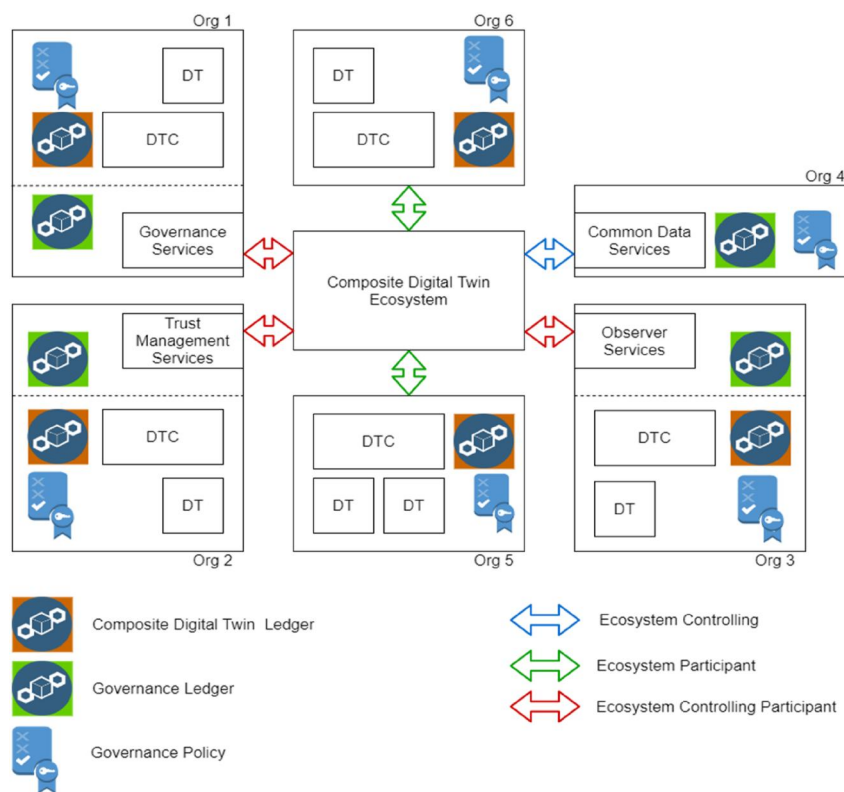
FIGURE 3 Proposed composite digital twin architecture [7].

Zero trust is another concept that some of the current systems use to achieve trusted behaviour. The fundamental idea of zero trust is not trusting any actor while always using verification methods such as authentication, authorisation, and access control to grant permission to perform actions in the system. However, considering CDT collaborative ecosystem, it is essential to build trust over time to improve communication. This is one of the reasons to periodically evaluate trust and security in DTs to detect untrusted behaviours. However, some zero trust concepts, such as comprehensive logging, secure communication channels, access requests to data owners etc., are considered in the proposed architecture further to strengthen the trust and security of the CDT. Another zero-trust security strategy is micro-segmenting the network [54]. This will shrink the attack surface and isolate the threat to minimise the damage to other systems. Micro-segmenting proves it can reduce network exposure and improve robustness from 60% to 90%. Considering this concept, the proposed architecture already segments the CDT into two sections, DTC and CDTEN. This will enable CDT to isolate infected DTs via DTC and limit the attackers' reach to other DTs. Most micro-segmenting trust evaluations are based on the dependency of different systems, such as identifying the essential nodes and their connections with others. This evaluation mainly tries to analyse how easy it is to attack connected

nodes and then get access to the essential nodes. Using dependency graphs, this evaluation is captured in the proposed trust and security analyser.

The SMM presented by IIC has three domains: governance, enablement, and hardening and is used by organisations to identify and target advancing the level of security maturity over time. The proposed architecture incorporates all these domains. Considering SMM governance practices, the proposed architecture uses CDTGP to inform all participants regarding rules, responsibilities, and requirements that need to be fulfilled by all the participants. The trust and security analyser will address the SMM subdomain dependency management using DT dependency graphs to understand dependencies between DTs in the CDT ecosystem. The proposed architecture also addresses SMM enablement domain considerations such as data protection, access control, and protection model for data etc., under the common data service component. SMM hardening domain is addressed in the trust management component consisting of security checks such as vulnerability assessment, security monitoring, recovery, and continuity of operations. The observer service component also provides functionality to support SMM continuity of operations by checking all the essential services are up and running to operate within the CDT securely. The proposed architecture is designed to be modular, following a micro-service design





**FIGURE 4** Example architecture implementation

pattern. These services can be updated or revised without interrupting the core CDT operations. This agility is required in modern systems due to the rapidly evolving nature of technology and potential threats.

Figure 4 provides an example of the proposed architecture implementation. In this example, six organisations will take part in the ecosystem. There are three types of roles, controlling, participant, and controlling participant. Ecosystem controlling means only engaging in the ecosystem controlling tasks such as how to implement new policies, requirements to join CDT, conflict resolutions, etc. As the name suggests, participants only connect to CDT and provide the required inputs and outputs. The controlling participant will play both roles in the ecosystem. As shown in the figure, all participants will have a copy of the GP because it is the primary agreement between participants to operate the ecosystem. Another highlight is the different ledgers that store different levels of information. As mentioned previously, this will prevent data privacy issues and allow access only to required information to participants.

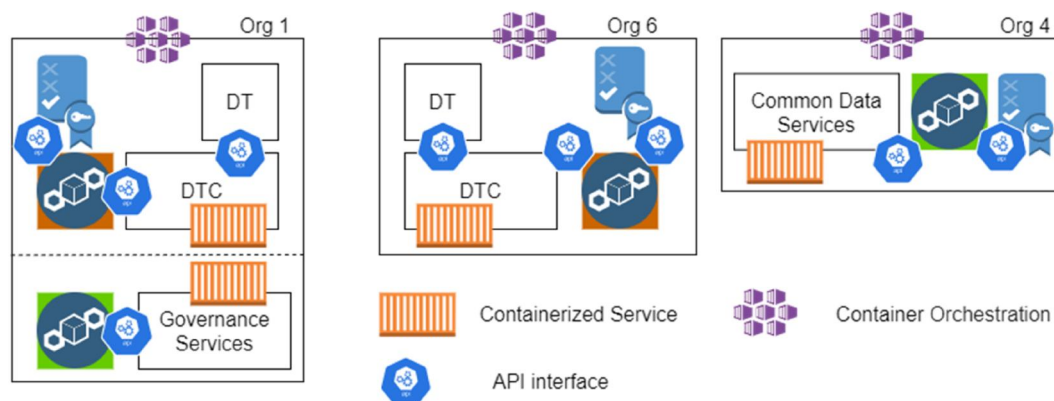
## 4 | PROPOSED ARCHITECTURE IMPLEMENTATION

Containerisation will play a major role in realising the deployment and distribution of services across ecosystem participants. Once the controlling organisations decide and distribute the responsibilities, customised containers will be

created for each organisation. As shown in Figure 5, the architecture will be implemented as a collection of microservices. Individual organisations will have their own container orchestration services to manage multiple containers. As an example, organisation 1 will have DTC and GS containers. Container orchestration will help to scale the application as well as redeploy if the current instance is interrupted. This will increase the availability of the services, especially in the CDTEN. All the main containers will be connected using respective application programming interfaces (APIs). In Figure 5, only DTC and CDTEN represent containerised applications as individual DTs can be either containerised applications or generic hosted applications. Regardless of the hosting environment, all DTs will connect to the DTC using a **secure API**.

Tools such as Docker Compose<sup>7</sup> provide the flexibility to configure and deploy services at scale across the CDT ecosystem. In a manufacturing environment, it allows system integrators to deploy computing hosts (or virtual servers at enterprise tier or cloud) and leverage Docker Compose to deploy isolated environments that execute the architecture services. For example, the GS will have a docker image to support a smart-contract-based ledger and associated API gateway (e.g. NodeJS). Utilising Docker, this will not interfere with existing systems, but rather acts as an overlay to add new capabilities.

<sup>7</sup><https://docs.docker.com/compose/>.



**FIGURE 5** Implementation approach for composite digital twin

Considering the proposed architecture, there are some implementation choices that need to be considered to ensure robust delivery of a CDT; these include:

- **Service availability** decentralisation of services running across boundaries of multiple organisations can hinder management of the risk of failure. Some services have a higher impact, for example, common data and trust management services (TMS). If either service is unavailable, other organisations will have difficulty communicating. Therefore, it is important to allow for redundancy and ensure multiple organisations can host these services to maintain availability and minimise risk.
- **Performance** is another issue when the system is distributed among various participants. While this can minimise the risk of a single point of failure, latency and delay can be introduced based on the location services hosted and accessed. Instead of hosting services on-premises, an immediate solution is to move to the cloud and enable replications of the data based on the accessing locations (similar to content delivery networks). This can make the ecosystem operations highly available and high performance based on service level agreements etc. However, some concerns regarding data commercial sensitivity require additional support for the industry to migrate to the cloud. On one hand, the operation and scalability of a discrete DT falls outside the scope of the proposed architecture. It is expected that local integration will facilitate scalability for data inputs. The focus is on providing a secure and trusted mechanism to exchange data between DTs. This does require consideration of aspects for managing big data, that is, the four 'V's volume, velocity, variety, and veracity. For non-time critical and commonly shared data approaches akin to content delivery networks could help in staging data near the DT for easy access. Alternative approaches such as the InterPlanetary File System (IPFS) protocol, for data sharing across peer-to-peer networks could be considered (also to maintain privacy and maximise distributed approach).
- **The use of distributed ledgers** could impact overall performance and management overhead (i.e. hosting and supporting a ledger infrastructure), as such the implementation design must take great care to ensure efficient deployment and

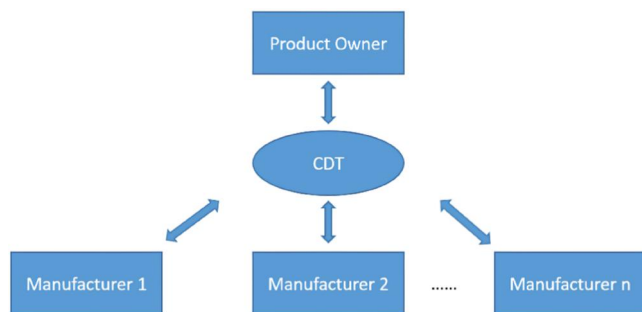
integration of DLT technology into DT systems. Industrial ecosystems are generally against public BCs (Ethereum) due to the higher transaction costs (price fluctuations), data privacy issues (sharing a common ledger to hold data), and limited control over the ledger. As such private Blockchains/ DLT networks are more attractive from an industrial perspective. Solutions such as Hyperledger Fabric, R3 Corda, Quorum, IoTA all provide enterprise grade solutions that can be deployed as a service or managed privately. To facilitate different governance structures and governance policies, Hyperledger Fabric is the preferable candidate for the proposed architecture. It offers significant flexibility from application implementation perspective and a growing support community to facilitate sustainability of the solution. There is also a lot of solutions available within the broader Hyperledger Foundation, that support the deployment and management of large networks, for example, additional supports for specific needs (e.g. digital identity, interoperability, development kits, reusable APIs). It is envisaged that the architecture would support an interledger protocol in the future to allow for abstraction of underlying ledger layer that may be used across different ecosystems.

## 5 | EXAMPLE SCENARIOS IN THE MANUFACTURING CONTEXT

As mentioned in Section 1, manufacturing is one of the key industries, developing and maximising the use of DTs. To highlight architectural components and its operations, this section will present three example use case scenarios in the collaborative manufacturing domain to emphasise the proposed architecture's suitability and potential, particular focus is placed on implementing the proposed governance schemes.

### 5.1 | Centralised governance CDT use case

To showcase centralised governance, a single owner additive manufacturing use case is presented in Figure 6. In this scenario, there will be a product owner, and parts of the product



**FIGURE 6** Use case example for centralised governance. One Product owner (Centralised) with multiple support manufacturers.

will be distributed among several manufacturers. To get a holistic view of the product manufacturing, the product owner creates a collaborative CDT manufacturing ecosystem where all the stakeholders who need to produce this product will connect to the CDT ecosystem. The value of participation includes the product owner achieving a complete view of the manufacturing process. At the same time, other participants can share product-related information to manufacture quality products. Based on the states of other manufacturers, individual manufacturing capabilities can be optimised. For example, if one manufacturer is facing difficulties, others can change their manufacturing process to produce something else to optimise their production lines, avoid downtime, and reduce costs.

The centralised governance structure will help the product owners to control who can join the CDT collaborative ecosystem and other aspects such as what information CDT participants need to share, synchronisation intervals etc. In this governance type, there is little to no control over the CDT for other participants who may or may not have direct benefits from joining the CDT.

In a CDT, the GP is the foundation for building the collaborative ecosystem. The workflow of defining this policy is shown in Figure 7, the product owner will start the initiation process by creating the CDTGP. The GP will then make all the essential services in the CDT, such as CDS, Observer Services, TMS, and GS. As shown in the DT joining, organisation 1 will first send a joining request to GP to get permission to connect its DT to CDT. GP is an executable contract between all the participants that enforce rules, responsibilities, and CDT information management. Based on the product owner's GP, permission will be granted to join the CDT. If permission is granted, DTC needs to conduct an initial trust and security analysis (TSA). After finishing the TSA, results will return to TMS in the CDT. Based on the results, TMS will record the DT initial trust index and start doing TSA periodically. After submitting the initial TSA, DTC will then submit all the data points that DT will share with CDT. Since this is centralised governance, the product owner specified GP would manage what type of information needs to be shared, frequency, and format. After submitting, DTC can also request to get available services for subscription. The communication between DTs will be a highly influential activity based on the GP. This level

of CDT ecosystem control allows the CDT creator to manage CDT as required based on the use case objectives.

The proposed architecture has multiple data flow patterns, and Figure 7 demonstrates the publisher-subscriber data flow. In this method, DT will send its data to DTC to pass it to the CDS. In this use case, organisation 2 sends data to CDS, and then CDS distributes that new data to all subscribers. In this CDT, organisation 1 and organisation  $n$  (represent  $n$  number of organisations) will get this new data update. Since it is a centralised governance structure, the product owner will also get this update. In that way, the product owner can have control and visibility over the CDT. In addition, all the transactions will be recorded in the distributed ledger to support conflict resolution and traceability of actions carried out by each organisation. However, these distributed ledger writing parts are not specified in Figure 7 to reduce the complexity of the figure. Another data flow method will be discussed in the next Section 5.2.

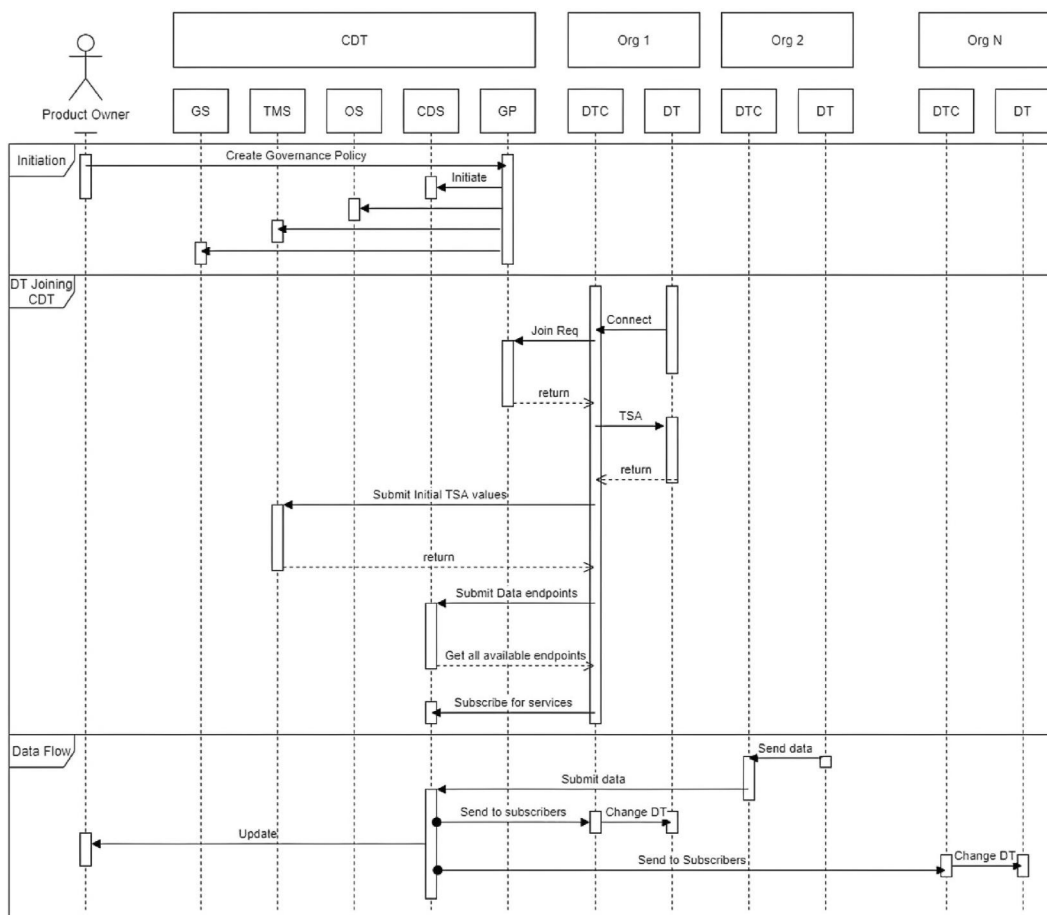
Figure 8 demonstrates the sequence of activities for TSA and Policy change. As mentioned previously, in Section 3, the trust and security analyser will be activated periodically to update the trust and security index for active DTs. This is a mandatory step when a new DT joins. TMS will initiate a trust analysis of all the DTCs in the CDT, and then DTCs will submit the trust and security indexes. There are five categories in the trust and security index, and only some of them will be provided by the respective DTCs. At the same time, the TMS itself will evaluate some categories. Security, Reliability, Resilience, dependency, uncertainty, and goals are the five trust and security index categories. DTC will only analyse security and resilience, while TMS will analyse dependency and uncertainty with the help of CDS DT data subscriptions and goals. The individual DTCs will evaluate each other's reliability using QoS metrics, such as throughput, response time, and failure rate. However, reliability calculations are based on GP because if CDT operates in a publisher-subscriber data flow, there are no direct communications between DTs. A centralised authority can decide what kind of data communication is allowed; based on that, TSA can be adapted.

As shown in Figure 8, the product owner can submit policy changes to GS, and those changes will get updated directly in the GP. In this use case, soon after GP changes, it will re-evaluate CDT and terminate organisation 2 from the CDT. However, policy change is different in the decentralised CDT governance structure, which will be discussed in detail in the next section.

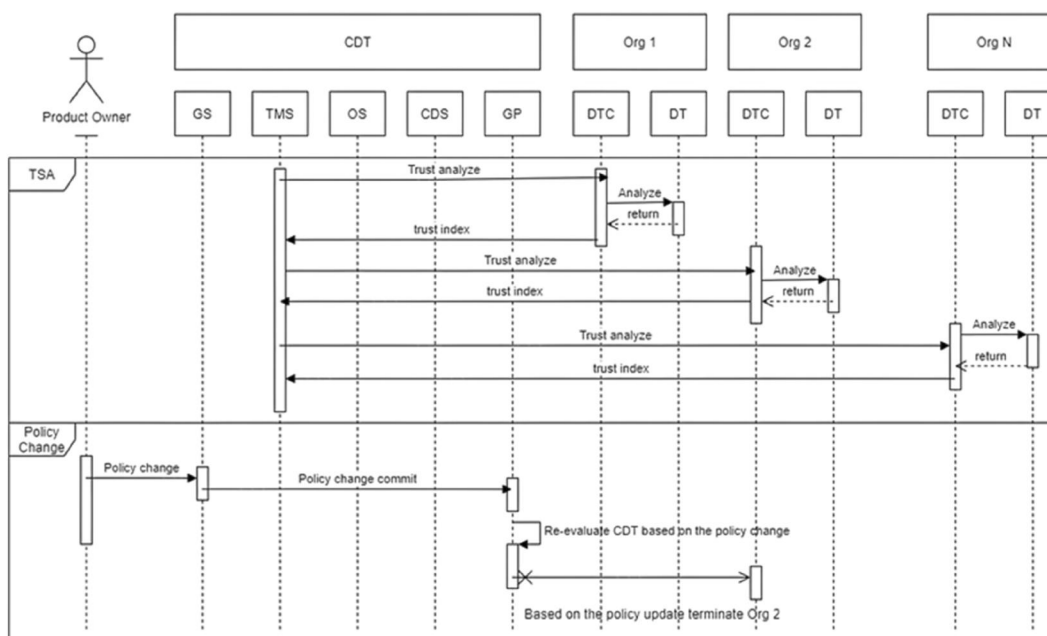
## 5.2 | Decentralised governance CDT use case

In this scenario, there is a mutual or direct benefit for all the participants of this governance type. This means everyone has equal authority over the CDT.

As shown in Figure 9, the producer-supplier scenario is an example of a decentralised governance structure. This is a classic CDT implementation between two parties, and both



**FIGURE 7** Centralised CDT Sequence diagram for initiation, DT joining, and data flow. CDS, common data services; CDT, composite digital twin; DT, digital twin; DTC, digital twin connector; GP, governance policy; GS, governance service; OS, observer service; TMS, trust management service



**FIGURE 8** Centralised CDT Sequence diagram for policy change, trust and security analysis. CDS, common data services; CDT, composite digital twin; DT, digital twin; DTC, digital twin connector; GP, governance policy; GS, governance service; OS, observer service; TMS, trust management service



want to share some information that can benefit both. For example, a producer DT can update CDT with its future productions, and a supplier DT can absorb this information and ramp up or slow down its production. The same can be considered when producers see an increase in production from the suppliers' side. It will be beneficial to stock up or ramp up production to match it for maximising profits.

Since control over CDT is distributed among all participants, they can decide who can join the CDT and what requirements need to be fulfilled to join the CDT. For example, suppose an institution needs to see all the communications between participants to ensure fair trade. In that case, distributed governance will allow such participants and expose distributed ledger with extra transparency. If another party wants to join CDT, a majority of participants must agree on that joining request.

Decentralised CDT initiation is shown in Figure 10. All the founding stakeholders will submit their policy suggestions to the GS. Then, GS will send the policy agreement to all the founding stakeholders. Once it receives all the stakeholders'



**FIGURE 9** Use case example for decentralised governance. Producer and supplier working together to address each other's demands

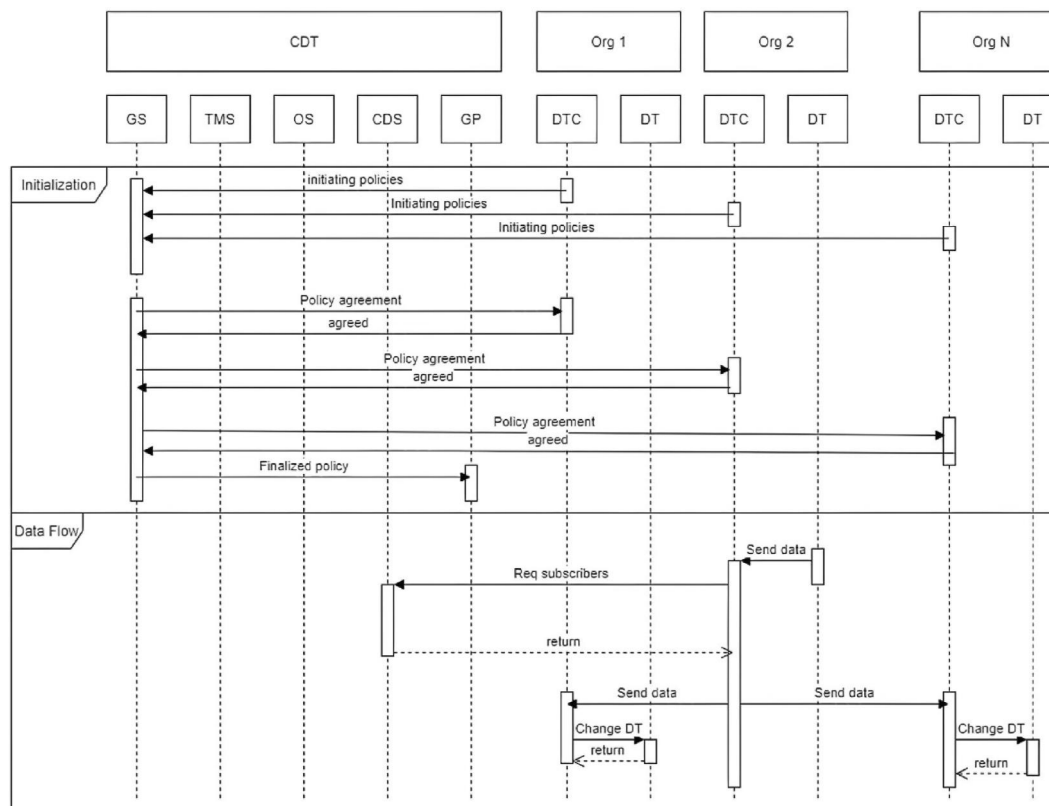
agreement on the policy, it will then state it as the GP of the CDT. This will be the same process for policy changes; other stakeholders will accept or reject the policy amendments.

DT joining and TSA will be the same as the centralised CDT, the only difference is how GP is defined to accommodate new CDT participants and TSA operations. Figure 10 will demonstrate another version of publisher-subscriber data flow. In this method, DTC will request an updated subscriber list, send the update directly to all the subscribed DTCs, and apply the changes to the DT. Another supported data flow method is request-response, and in that case, DTC will directly request data from the respective responsible DTC.

### 5.3 | Hybrid governance CDT use case

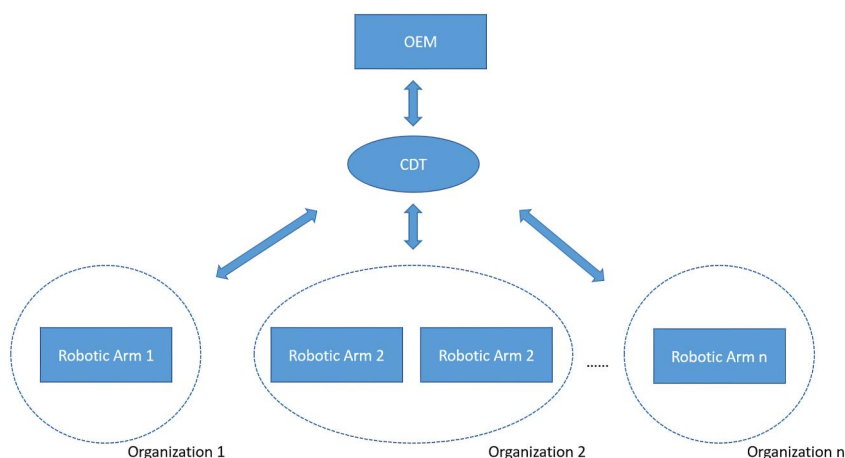
In this structure, all the participants may or may not get benefits because participants will join the CDT based on the governance structure.

Figure 11 illustrates an example of a hybrid governance structure. In this scenario, an original equipment manufacturer (OEM) acts as a centralised control party, and organisations join as participants. All the organisations connected to this CDT purchase a robotic arm from the OEM and join this CDT to learn new robotic capabilities and optimisations. In this way, robotic arms can share their learnings with the CDT and distribute them to other robotic arms to improve their



**FIGURE 10** Decentralised CDT sequence diagram for initialisation and data flow. CDS, common data services; CDT, composite digital twin; DT, digital twin; DTC, digital twin connector; GP, governance policy; GS, governance service; OS, observer service; TMS, trust management service

**FIGURE 11** Use case example for hybrid governance. OEM controlling the similar types of equipment owned by multiple organisations. OEM, original equipment manufacturer



operations. This is a collective learning effort that benefits all the organisations that have these robotic arms. This is also beneficial to prevent unplanned interruptions by sharing error reports, and OEM can distribute patches to fix the problems in advance for other robotic arms.

In this use case, OEM is partly controlling the CDT by enabling those who can join the CDT ecosystem, such as specific models of robotic arms. Meanwhile, any organisation purchasing this robotic arm can join the CDT and benefit from it with minimum friction from other parties. In that sense, it incorporates some distributed governance structure characteristics. This use case can also be implemented in a fully decentralised way and allow robotic arm DTs to communicate with each other directly. However, instead of implementing complete decentralised governance, it is better to have some control in the data value chain as the OEM can control the data flow. Otherwise, bad actors could potentially inject malicious behaviours into other robotic arms. Even in that case, the proposed trust and security analyser will provide protection via a trust index for participating DTs. The receiving party can then decide whether to accept or reject the new information. In hybrid governance, OEMs have some control over the information sharing and validate the optimisations that other robotic arm DTs are proposing. This will make the whole operation more secure and robust.

## 6 | CONCLUSION

Section 5 discusses three collaborative CDT ecosystems to highlight the need for multiple governance structures. The key feature of the proposed architecture is the ability to support all three governance structures while strengthening trust and security. The example scenarios demonstrate initialisation, data flow, TSA, and policy changes in the proposed architecture. The GP is the core of all governance types and specifies all the required rules and responsibilities that participants must follow. Distributed ledgers, TMS, and TSA will help to re-enforce transparency and trust among CDT participants. All the use cases discussed are in the manufacturing domain, but CDS and translation services in the proposed architecture will help adapt

to any domain. Hence, the proposed architecture addresses the key architectural requirements (trust, interoperability, and governance) identified in the state-of-the-art analysis. The next step is the implementation of the proposed architecture and its evaluation within real-world operating conditions, such as distributing the DTs geographically and connecting DTs from various domains.

## AUTHOR CONTRIBUTIONS

**Pasindu Kuruppuarachchi:** Conceptualization (equal); writing - original draft (lead); Methodology (lead); writing-review and editing (supporting). **Alan McGibney:** Conceptualization (equal); Supervision (lead); Methodology (supporting); Writing-review and editing (equal). **Susan Rea:** Conceptualization (equal); Supervision (supporting); Writing-review and editing (equal)

## ACKNOWLEDGEMENT

This research work is supported by Science Foundation Ireland Centre for Research Training focused on Future Networks and the Internet of Things (AdvanceCRT), under Grant number 18/CRT/6222.

## CONFLICT OF INTEREST

The authors have declared no conflicts of interest. All co-authors have read and approved the article, and there are no financial conflicts to disclose. We certify that the contribution is unique and that it is not currently under consideration by another publisher.


## DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

## PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

## ORCID

Pasindu Manisha Kuruppuarachchi  <https://orcid.org/0000-0003-2343-8227>

## REFERENCES

- Tao, F., et al.: Digital twins and cyber-physical systems toward smart manufacturing and industry 4.0: correlation and comparison. *Engineering* 5(4), 653–661 (2019). <https://doi.org/10.1016/j.eng.2019.01.014>
- Grievens, M.: Digital twin: manufacturing excellence through virtual factory replication (2015)
- Padovano, A., et al.: A digital twin based service oriented application for a 4.0 knowledge navigation in the smart factory. *IFAC-PapersOnLine* 51(11), 631–636 (2018). <https://doi.org/10.1016/j.ifacol.2018.08.389>
- Ayani, M., Ganebäck, M., Ng, A.H.C.: Digital twin: applying emulation for machine reconditioning. *Procedia CIRP* 72, 243–248 (2018). <https://doi.org/10.1016/j.procir.2018.03.139>
- Malakuti, S., et al.: Digital twins for industrial applications. *IIC Journal of Innovation*. [Online]. [https://www.iiconsortium.org/pdf/IIC\\_Digital\\_Twins\\_Industrial\\_Apps\\_White\\_Paper\\_2020-02-18.pdf](https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf) (2020). Accessed 13 Aug 2022
- Kritzinger, W., et al.: Digital twin in manufacturing: a categorical literature review and classification. *IFAC-PapersOnLine* 51(11), 1016–1022 (2018). <https://doi.org/10.1016/j.ifacol.2018.08.474>
- Kuruppuarachchi, P., Rea, S., McGibney, A.: An architecture for composite digital twin enabling collaborative digital ecosystems. In: 2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 980–985 (2022)
- Rasheed, A., San, O., and Kvamsdal, T.: Digital twin: values, challenges and enablers, pp. 1–31 (2019)
- Chaturvedi, K., Kolbe, T.H.: Towards establishing cross-platform interoperability for sensors in smart cities. *Sensors* 19(3), 562 (2019). <https://doi.org/10.3390/s19030562>
- Electric, G.: Digital twins debunking the myths. [Online]. <https://www.ge.com/digital/blog/digital-twins-debunking-myths>. Accessed 08 Jul 2020
- Laaki, H., Miche, Y., Tammi, K.: Prototyping a digital twin for real time remote control over mobile networks: application of remote surgery. *IEEE Access* 7, 20235–20336 (2019). <https://doi.org/10.1109/access.2019.2897018>
- Lockheed Martin Digital Twin Maturity Model. [Online]. <https://www.lockheedmartin.com/en-us/news/features/2021/visualizing-the-digital-thread-and-digital-twins.html>. Accessed 04 Jun 2022
- Song, E.Y., et al.: IEEE 1451 smart sensor digital twin federation for IoT/CPS research. In: SAS 2019 - 2019 IEEE Sensors Applications Symposium Conference Proceedings (2019)
- Sun, W., et al.: Adaptive federated learning and digital twin for industrial internet of things. *IEEE Trans. Industr. Inform.* 3203, (2020). <https://doi.org/10.1109/tii.2020.3034674>
- Adams, M., et al.: Flexible integration of Blockchain with business process automation: a federated architecture. In: *Advanced Information Systems Engineering*, pp. 1–13 (2020)
- Lu, Y., et al.: Communication-efficient federated learning and permissioned Blockchain for digital twin edge networks. *IEEE Internet Things J.* 8(4), 2276–2288 (2021). <https://doi.org/10.1109/jiot.2020.3015772>
- Sun, W., et al.: Dynamic digital twin and federated learning with incentives for air-ground networks. *IEEE Trans. Netw. Sci. Eng.* 4697(c), 1–13 (2020). <https://doi.org/10.1109/tnse.2020.3048137>
- Lu, Y., et al.: Low-latency federated learning and Blockchain for edge association in digital twin empowered 6G networks. *IEEE Trans. Ind. Inf.* 17(7), 5098–5107 (2021). <https://doi.org/10.1109/tii.2020.3017668>
- Autiosalo, J., et al.: Towards integrated digital twins for industrial products: case study on an overhead crane. *Appl. Sci.* 11(2), 1–35 (2021). <https://doi.org/10.3390/app11020683>
- Mi, S., et al.: Prediction maintenance integrated decision-making approach supported by digital twin-driven cooperative awareness and interconnection framework. *J. Manuf. Syst.* 58(PB), 329–345 (2021). <https://doi.org/10.1016/j.jmsy.2020.08.001>
- Borth, M., Verriet, J., Muller, G.: Digital twin strategies for SoS. In: 2019 Annual Conference System of Systems Engineering, pp. 164–169 (2019)
- Maier, M.W.: Architecting principles for systems-of-systems. *Syst. Eng.* 1(4), 267–284 (1999). [https://doi.org/10.1002/\(sici\)1520-6858\(1998\)1:4<267::aid-sys3>3.0.co;2-d](https://doi.org/10.1002/(sici)1520-6858(1998)1:4<267::aid-sys3>3.0.co;2-d)
- Ganguli, R., Adhikari, S.: The digital twin of discrete dynamic systems: initial approaches and future challenges. *Appl. Math. Model.* 77, 1110–1128 (2020). <https://doi.org/10.1016/j.apm.2019.09.036>
- Wang, J., et al.: A collaborative architecture of the industrial internet platform for manufacturing systems. *Robot. Comput. Integrated Manuf.* 61, 101854 (2020). <https://doi.org/10.1016/j.rcim.2019.101854>
- Jammes, F., et al.: *Orchestration of service-oriented*, vol. 1, pp. 617–624 (2005)
- Sahal, R., et al.: Blockchain-empowered digital twins collaboration: smart transportation use case. *Machines* 9, 1–33 (2021). <https://doi.org/10.3390/machines90901939>
- Rasor, R., et al.: Towards collaborative life cycle specification of digital twins in manufacturing value chains. *Procedia CIRP* 98, 229–234 (2021). <https://doi.org/10.1016/j.procir.2021.01.035>
- Rouhani, S., et al.: Distributed attribute-based access control system using a permissioned Blockchain. *arXiv* (2020)
- Cioroica, E., Kuhn, T., Buhnova, B.: (Do not) trust in ecosystems. In: *Proceedings - 2019 IEEE/ACM 41st International Conference on Software Engineering New Ideas Emerging Results, ICSE-NIER 2019*, pp. 9–12 (2019)
- “Meet The Digital Wind Farm.” [Online]. <https://www.ge.com/renewableenergy/stories/meet-the-digital-wind-farm>. Accessed 20 Jul 2022
- Porté-Agel, F., Bastankhah, M., Shamsoddin, S.: Wind-turbine and wind-farm flows: a review. *Boundary-Layer Meteorol.* 174(1), 1–59 (2020). <https://doi.org/10.1007/s10546-019-00473-0>
- van Pelt, R., et al.: Defining Blockchain governance: a framework for analysis and comparison. *Inf. Syst. Manag.* 38(1), 21–41 (2020). <https://doi.org/10.1080/10580530.2020.1720046>
- Putz, B., et al.: EtherTwin: blockchain-based secure digital twin information management. *Inf. Process. Manag.* 58(1), 102425 (2021). <https://doi.org/10.1016/j.ipm.2020.102425>
- Dietz, M., Putz, B., Pernul, G.: A distributed ledger approach to digital twin secure data sharing. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11559, pp. 281–300. LNCS (2019)
- Hasan, H.R., et al.: A blockchain-based approach for the creation of digital twins. *IEEE Access* 8, 34113–34126 (2020). <https://doi.org/10.1109/access.2020.2974810>
- Cioroica, E., et al.: Reference architecture for trust-based digital ecosystems. In: *Proceedings - 2020 IEEE Int. Conf. Softw. Archit. Companion, ICSA-C 2020*, pp. 266–273 (2020)
- Zong, B., et al.: A broker-assisting trust and reputation system based on artificial neural network. In: *Conference Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp. 4710–4715 (2009)
- Cioroica, E., et al.: Towards creation of a reference architecture for trust-based digital ecosystems. In: *ACM International Conference Proceeding Series*, vol. 2, 273–276 (2019)
- Qureshi, B., Min, G., Kouvatsos, D.: Collusion detection and prevention with FIRE+ trust and reputation model. In: *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software Systems ICES-2010, ScalCom-2010*, pp. 2548–2555 (2010)
- Schmittner, C., et al.: Security application of failure mode and effect analysis (FMEA). In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8666, pp. 310–325. LNCS (2014)
- Raspotnig, C., et al.: Enhancing CHASSIS: a method for combining safety and security. In: *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 766–773 (2013)
- Young, W., Porada, R.: System-theoretic process analysis for security (STPA-SEC): cyber security and STPA (2017)
- Cioroica, E., Kar, S.R., Sorokos, I.: Comparison of safety and security analysis techniques, pp. 234–242 (2022)
- Carielli, S., et al.: IoT security maturity model: practitioner’s guide, pp. 8–86 (2019)

45. Suhail, S., et al.: Trustworthy digital twins in the industrial internet of Things with Blockchain. *IEEE Internet Comput.* 7801(c), 1–8 (2021)
46. Buck, C., et al.: Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. *Comput. Secur.* 110, 102436 (2021). <https://doi.org/10.1016/j.cose.2021.102436>
47. Mayoral, A., et al.: Control orchestration protocol: unified transport API for distributed cloud and network orchestration. *J. Opt. Commun. Netw.* 9(2), A216–A222 (2017). <https://doi.org/10.1364/jocn.9.00a216>
48. Ma, W., et al.: Machine learning empowered trust evaluation method for IoT devices. *IEEE Access* 9, 65066–65077 (2021). <https://doi.org/10.1109/access.2021.3076118>
49. Dessì, N., Pes, B., Fugini, M.G.: A distributed trust and reputation framework for scientific grids. In: *Proceedings of 2009 Third International Conference on Research Challenges in Information Science RCIS 2009*, pp. 265–274 (2009)
50. Albuquerque, R.D.O., et al.: Analysis of a trust and reputation model applied to a computational grid using software agents. In: *Proceedings of 2008 Conference on Convergence and Hybrid Information Technology ICHIT 2008*, pp. 196–203 (2008)
51. Barrane, F. Z., et al.: Building trust in multi-stakeholder collaborations for new product development in the digital transformation era. *Benchmarking*. (2020). <https://doi.org/10.1108/BIJ-04-2020-0164>
52. ISO/DIS 23247-1: Automation systems and integration — digital twin framework for manufacturing — Part 1: overview and general principles. [Online]. <https://www.iso.org/standard/75066.html>. Accessed 08 Jul 2020
53. Dib, O., et al.: Consortium blockchains: overview, applications and challenges. *Int. J. Adv. Telecommun.* 11(1&2), 51–64 (2018)
54. Basta, N., et al.: Towards a zero-trust micro-segmentation network security strategy: an evaluation framework (2021)

**How to cite this article:** Kuruppuarachchi, P.M., Rea, S., McGibney, A.: Trusted and secure composite digital twin architecture for collaborative ecosystems. *IET Collab. Intell. Manuf.* e12070 (2023). <https://doi.org/10.1049/cim2.12070>