C. Alcaraz and I. H. Meskini and J. Lopez, "Digital twin communities: an approach for secure DT data sharing", *International Journal of Information Security*, vol. 24, 2024.
NICS Lab. Publications: https://www.nics.uma.es/publications

Digital Twin Communities: An Approach for Secure DT Data Sharing

Cristina Alcaraz, Iman Hasnaouia Meskini, and Javier Lopez
Computer Science Department, University of Malaga
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz,imanb,javierlopez}@uma.es

Abstract

Digital Twin (DT) technology empowers organizations to create virtual counterparts of their physical assets, thereby magnifying their analytical, optimization and decision-making capabilities. More specifically, the simulation capabilities of a DT generate high-quality data that not only benefit the DT owner organization, but also the potential of similar organizations by leveraging the DT's capabilities when sharing its simulation results. This collaborative sharing boosts the capabilities of each participating organization, fostering a collective intelligence that amplifies their competitive advantage. Nonetheless, data exchange must rigorously safeguard each organization's data confidentiality, and access to this data must be thoroughly controlled. Thus, this paper introduces the novel concept of DT communities and proposes a hybrid access control architecture. This architecture seamlessly integrates the strengths of both Role Based Access Control (RBAC) and Organizational Based Access Control (OrBAC), facilitating secure, authorized intra- and inter-organizational information sharing in the context of Industry 5.0, combining the strengths of local DT communication and other organization's DTs as well. Moreover, in order to show the feasibility of the approach for critical corporate organizations and their systems, in this paper we provide a proof-of-concept implementation of this architecture. To validate its functionality and efficiency, we perform a number of experimental studies showing how various entities can benefit from securely sharing DT models based on the concept of "community".

Keywords: Digital Twin, Access Control, Data Sharing, Communities, Industry 5.0

1 Introduction

Throughout the past decade, Digital Twin (DT) technology has been subject of extensive research in literature, and the business world is now transitioning toward the widespread adoption of DTs as a cornerstone technology [8]. Recent

estimations project that in the coming years, over 40% of major corporations will incorporate DT into their operations, with a corresponding envisioned market expansion of 25% [8]. Thus, DTs serve as an essential technology within the context of Industry 4.0, where the fusion of Industrial Internet of Things (IIoT) and Cyber–Physical Systems (CPSs) takes center stage alongside an array of other technologies, such as virtualization and Artificial Intelligence (AI) [3]. This multifaceted ecosystem demands that DTs have a deep understanding of various communication protocols inherent to each physical device, all the while maintaining compatibility with their corresponding virtual equivalents. This adaptability and cross–protocol competence are essential features that empower DTs to bridge the physical–virtual spaces, facilitating the holistic integration of Industry 4.0 technologies.

The primary advantages of DTs lie in their capacity to deliver valuable information for diagnosis, predictive maintenance, optimization and support for decision-making [4, 30]. This, in turn, underlines the growing importance of real-time communication, further emphasizing its critical role in ensuring the seamless synchronization of physical spaces and their virtual counterparts [3, 33]. The potential of DTs increases substantially when communication and collaboration between different organization's DTs materialize [13]. Organizations with similar expertise and backgrounds have the opportunity to collaborate [4] by sharing predictions and simulation results of their devices. This collaborative effort harnesses collective intelligence, enabling them to efficiently predict equipment failures and identify opportunities to optimize the production process, thereby enhancing operational efficiency and informed decision-making. This collective intelligence holds the potential to bolster threat intelligence, as organizations can conduct attack simulations and share the outcomes with their related peers. Therefore, the focus of this approach also helps safeguard their infrastructures and fortify defenses against potential threats, enhancing overall cybersecurity and infrastructure resilience [18].

We understand the collective capability of DTs as the ability to play a part in an interconnected network where the shared data consists either of DT models themselves, which an organization could clone and integrate into its own DT network; or DT-generated output information such as cyber-attack simulations or predictive maintenance. This output information could be the edge connecting two different DTs without accessing the model, since a DT's output data may be the input data for another one, and minimizing access to the model protects its industrial property as well. We achieve this collective intelligence of DTs through DT communities, which enables secure data sharing and interconnection of DTs in the Industry 5.0 context.

The concept of DT communities applied to multiple organizations facilitates the transition to Industry 5.0. This phase builds upon the principles of Industry 4.0, aiming to deepen the integration of the human workforce with technological advancements in the industrial environment, emphasizing the interaction between humans and technology to achieve enhanced efficiency and productivity. Its core revolves around sustainability, resilience, and human-centricity; and the intra- and inter-organizational communication by DT communities allows for a

transition towards an Industry 5.0-enabled environment. Therefore, DT communities cultivate sustainability by promoting resource reuse through efficient information exchange. All of this enhances the resilience of organizations and their critical systems to counter potential threats, simply by prioritizing security measures, ensuring confidentiality and access control. Likewise, this approach is human-centered and spotlights simplicity and maintainability, recognising the importance of providing sustainable and user-friendly systems.

Nevertheless, there are security and technical aspects that must be considered for a secure and efficient inter-organizational DT data sharing framework, especially for the preservation of intellectual and industrial property of each organization. Namely, some of the main challenges that need to be addressed are privacy, access control, confidentiality, and standardization of these security measures [3, 22]. In this paper we design an architecture that incorporates DT communities for both intra- and inter-organizational data sharing and integrates access control to address these challenges in the Industry 5.0 context, in addition to favoring the trustworthy cooperation, security and resilience of critical systems. Therefore, the **main contributions** of this work are:

- Design of an access control architecture for DT Communities data sharing.
- Alignment of DT communities with Industry 5.0 requirements based on the proposed architecture.
- Definition of a real experiment scenario and evaluation experiments to test the Industry 5.0 requirements of DT communities.

The paper is structured as follows: Section 2 introduces the concept of DT Communities. Section 3 presents the access control architecture for DT Communities data sharing. Section 4 covers DT communities usability in terms of overhead management and adoption by organizations and real-life scenarios.Section 5 defines the Industry 5.0 DT Data Sharing requirements. Section 6 analyzes and compares related work. Section 7 evaluates and tests performance to demonstrate compliance with Industry 5.0 objectives, providing a final discussion. Section 8 discusses remaining challenges and new research chances, while section 9 outlines the conclusions and future work.

2 Digital Twin Communities and Conceptualization

Interoperability and interconnection between DTs are indispensable to take full advantage of their simulation capabilities [3], specifically in a dynamic environment where DTs generate single organization simulation data. By leveraging a DT's previously integrated Machine Learning (ML) and statistical analysis mechanisms, more realistic results can be obtained when different organization's DTs collaborate through data sharing. Moreover, time-sensitive information such as cyber-attack alerts or a predictive device failure alert could be processed earlier by the DT, as another organization may have the data beforehand.

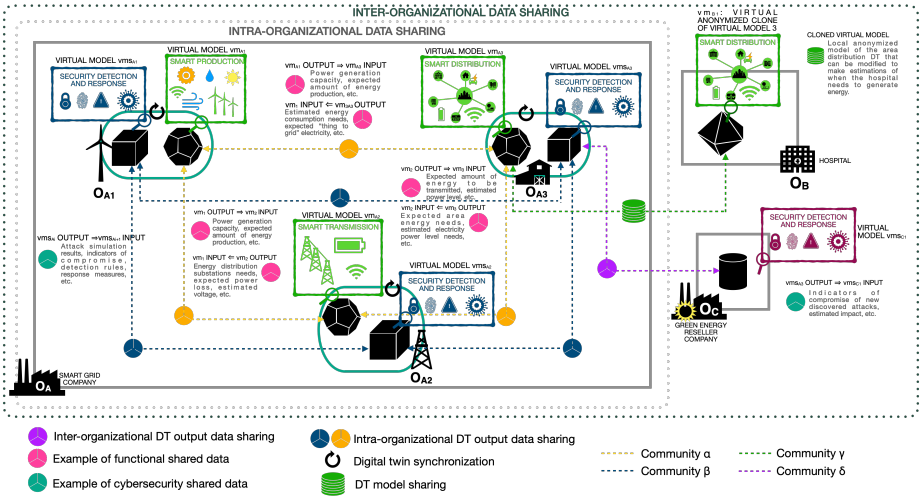

Figure 1: Illustrative figure showcasing the implementation of DT communities

The synergy achieved through the collaboration of different organizations' DTs mirrors the effective sharing of Cyber Threat Intelligence facilitated by CSIRTs (Computer Security Incident Response Teams). Much like how organizations proactively share information about cyber threats with CSIRTs, the collaboration of DTs enables a collective intelligence approach. When an organization experiences a cyber-attack, prompt communication with other organizations through DTs facilitates timely preparation for response to potential threats.

Given the advantages of DT collaboration and collective intelligence arising from data sharing within and across organizations, we introduce the novel concept of "digital twin communities". A DT community is a logical concept that groups several DTs within a cluster, where all communications occur. This interconnection enables interoperable and secure intra- and inter-organizational data sharing between DTs regardless of whether they belong to the same or different organizations, facilitating and fostering cyberintelligence and situational awareness.

The virtues of DT communities extend beyond ensuring secure data sharing: they empower DTs with the capacity to clone and reuse models, fostering efficient model sharing. Moreover, DT communities facilitate the synchronization of multiple twins by harnessing output information from one DT as input for another. This synchronization enhances operational efficiency whilst resulting in substantial resource savings. In other words, when reusing outputs from other organizations' DTs as inputs instead of creating a whole new DT, a significant number of hardware and workforce elements are spared. Similarly, when models are cloned, organizations can leverage other organizations' DT shared models. If a DT model is beneficial for one organization, they can simply clone and tailor it to their requirements, eliminating the need to create a model from scratch.

The electrical flow of the Smart Grid conceptual model proposed by the NIST (National Institute of Standards and Technology) [21] and managed by a conceptual electrical company combined with homologous organizations is a good example to comprehend how the role of DT communities provides interoperability, secure data sharing and resource reuse (model and data reuse). Figure 1 illustrates how intra- and inter-organizational communication clusters are formed through DT communities, where a set of organizations O = $\{O_A, O_B, O_C\}$ consists of three homologous organizations O_A, O_B *and* O_C. Each organization owns its independent DTs, which comprise a set of digital models $vm = \{vm_A, vm_B, vm_C\}$, symbolizing a virtual representation of reality that maintains continuous bidirectional synchronization between physical devices and virtual models. In particular, O_A represents an electricity company that manages the Smart Grid life cycle, which showcases three substations ($O_A = \{O_{A1}, O_{A2}$ *and* $O_{A3}\}$) where intra-organizational communication takes place. These substations represent the electrical flow of the Smart Grid [29], such that: O_{A1} represents the energy production substation, which owns a subset of DTs defined as $\{vm_{A1}, vms_{A1}\} \in vm_A$; O_{A2} corresponds to the electricity transmission substation, which owns another subset of DTs defined as $\{vm_{A2}, vms_{A2}\} \in vm_A$; and O_{A3} is the distribution substation where electricity is distributed and reaches the final customers, its DTs consisting of the subset defined as $\{vm_{A3}, vms_{A3}\} \in vm_A$. O_B is depicted as a hospital equipped with its own dedicated power generator to ensure operational continuity during emergencies, and its own DT, namely $vm_{B1} \in vm_B$. O_C exemplifies a green electricity reseller company, with its corresponding DT $vms_{C1} \in vm_C$ that procures electricity from a distribution company, such as a distribution substation, and subsequently redistributes it to end customers. This configuration establishes an example with four customized communities, each showcasing a potential real-world application.

Given this scenario, we present a formal definition of the concept of community for both intra- and inter-organizational communication: A community that connects DTs among the same organization is defined as a trust relationship ($\leftrightarrow^t$) between them:

1. $\exists O_A \in O,\ \exists O_{A1}, O_{A2}, O_{A3} \in O_A,\ \exists vm_A \in O_A,\ \exists vm_{A1}, vm_{A2}, vm_{A3} \in vm_A$
2. $\forall\, O_{Ai} \in O_A, \forall\, vm_{Aij} \in O_{Ai}, \exists\, vm_{Aij} \leftrightarrow^t vm_{Aij+1},\ vm_{Aij+1} \leftrightarrow^t vm_{Aij+2},\ vm_{Aij+2} \leftrightarrow^t vm_{Aij} \rightarrow vm_{Aij},\ vm_{Aij+1},\ vm_{Aij+2} \in community_{Ai}$

A community that connects DTs across different organizations is defined as a trust relationship ($\leftrightarrow^t$) between them:

1. $\exists O_A, O_B \in O,\ \exists O_{A3} \in O_A,\ \exists vm_A \in O_A,\ \exists vm_{A3} \in vm_A,\ \exists vm_B \in O_B,\ \exists vm_{B1} \in vm_B,\ vm_A \notin O_B,\ vm_B \notin O_A$
2. $\forall\ O_i \in O,\ \forall\ vm_{ij} \in O_i,\ \forall vm_{(i+1)k} \in O_{i+1},\ \exists\ vm_{ij} \leftrightarrow^t vm_{(i+1)k} \rightarrow vm_{ij}, vm_{(i+1)k} \in community_i$

Community α entails an intra-organizational communication link connecting DTs across various substations. In this setup, simulation outputs from each DT model are shared as data inputs for another model. For instance, if vm_{A1} estimates power generation substation's (O_{A1}) electricity generation capacity within its simulation system, this data becomes valuable for the power transmission DT, enhancing the accuracy of its results. Another instance arises when predicting substantial wind power generation due to strong winds. In this scenario, the transmitting substation DT can leverage this data alongside historical data to formulate an optimal transmission plan. Simultaneously, the transmitting substation DT (vm_{A2}) can extract value from simulation data provided by the distribution substation's DT (vm_{A3}). For instance, if simulation results indicate an imminent surge in peak power and energy consumption in a particular region, the transmitting substation DT can incorporate this insight to enhance its energy transmission simulations. In addition, the distribution company's DT (vm_{A3}) can supply consumption estimate data to the generating substation's DT (vm_{A1}). This enables more accurate simulations of energy production, minimizing loss wherever feasible. Another intriguing scenario is smart cities contributing energy to the grid through "Thing-to-Grid" (T2G) technology. As such, while the said concept does not exist, there is the established practice of "Vehicle-to-Grid" (V2G) [7]. In this system, vehicles can supply electricity to the grid as needed, rather than solely charging their batteries. In contrast, surplus energy generated by solar panels, if not utilized, is fed back into the grid. Looking ahead, it is plausible, akin to the evolution seen with the Internet of Things (IoT), that devices in an interconnected ecosystem could autonomously contribute electricity to the grid based on simulation data from DTs. This has the potential to optimize electricity flow to its fullest extent. Thus, the information shared among the three substations' DTs can be leveraged to optimize power flow.

The β community also illustrates an intra-organizational communication link. However, in this context, it serves as a cybersecurity reference for critical environments. Here, DTs dedicated to attack detection and system response communicate exclusively within the community, ensuring that shared information remains confidential among its members. For instance, twins capable of simulating attacks can collaborate by sharing results with counterparts in different substations. This enables the simulation of the progression of an attack, facilitating a chained simulation of malware with lateral movements.

Similarly, the δ community establishes an inter-organizational connection between DTs devoted to cybersecurity defense and response within the energy distribution substation (O_{A3}) and those within the green energy reseller company (O_C). This facilitates the comparison of information such as indicators of compromise or the estimated impact of an attack, enabling the establishment of local cyber intelligence to combat cyber threats. This community illustrates how a single DT can belong to two distinct communities as well (β and δ communities) autonomously sharing or receiving information within each respective channel.

Subsequently, within the γ community, the hospital (O_B), equipped with

its independent power generator, can proactively predict potential power generator activation based on energy distribution data within the area or city. Additionally, the energy distribution substation (O_{A3}) offers the capability to clone previously anonymized models provided by the distribution company, safeguarding intellectual and industrial property rights as well as consumer data. Consequently, the hospital can duplicate the DT model (vm_{A3}) for its own estimations, eliminating the necessity of relying on output data accessibility from other organizations and mitigating the need to allocate resources for DT creation. This particular example can be extended, as the shared models may address analogous scenarios in related contexts.

This illustration served as a practical demonstration on how the novel concept of DT communities contributes to achieving resource optimization and fostering efficient data sharing across organizational boundaries. In the next section, we consolidate the DT community concept by proposing an architecture that implements DT communities integrating access control and confidentiality.

3 DT communities-based access control and accessibility layers

In order to understand the concept of "DT communities" and the relevance of data protection and access thereto that DT communities provide, this section explores the theoretical concept of DT and its architecture in order to integrate the concept of DT communities, data sharing protection and access control with the DT architecture, thus allowing smooth integration with pre-existing twins, minimizing complexity and maximizing efficiency.

We consider that a DT is composed by four abstract layers [3] where, for the scope of this paper, we focus on the last two layers: data modelling and data access. The data modelling layer encompasses the core intelligence of a DT, acting as the central hub for digital model definition, simulations, predictions, and other essential functions. On the other hand, the data access layer serves as the front-line interface for accessing and visualizing processed data from the preceding layer, facilitating interaction with software processes, other DTs, end-users, and various other entities. In other words, the access layer is positioned as the nexus between DT simulation information and the organizational domain, where DT data sharing occurs. In particular, the access layer strongly needs access control methods to serve as the primary security barrier for the DT. In fact, the literature highlights the critical significance and imperative need for robust access control for critical infrastructures, such as digital twins [3, 38, 39]. Hence, we expand the DT access layer and advance the notion of DT communities introduced in the preceding section, offering an architectural framework that prioritizes access control. Currently, a human-centric industrial revolution is underway (Industry 5.0), and security is imperative for an interconnected ecosystem that mainly functions on trust [1, 5, 28], especially when DTs hold important intellectual and industrial property of organizations, thus reinforcing

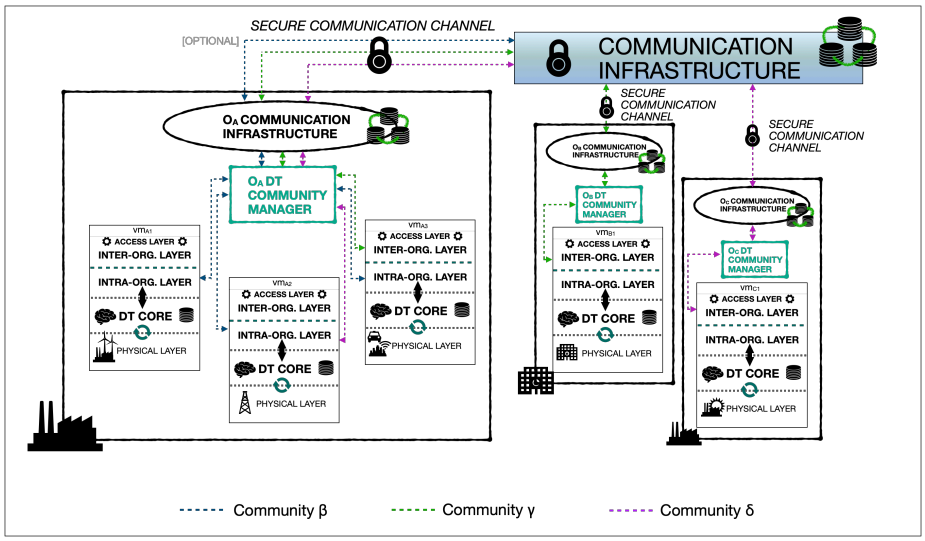

Figure 2: DT Communities data sharing through Pub/Sub Infrastructure

the need of access control as the first defense wall between the interconnected world where DTs are playing a key role and an organization DT which must be protected.

As mentioned, the aim of this work is to design an access control-based secure DT data sharing architecture which supports both inter- and intra-organizational communication. We achieve this through a dual-layer approach for the access layer abstraction of a DT and a publish/subscribe architecture. As depicted in Figure 2, firstly, we separate the accessibility layer into two sub-layers: the intra-organizational, and the inter-organizational accessibility layer. This way, an organization gains the capability to precisely configure the data flow from the simulation layer to each accessibility sub-layer, effectively isolating critical data that may only be accessed within the organization's perimeter. The intra-organizational layer comprises the data exchange among the same organization's DTs, while the inter-organizational layer provides a dimension where interconnections between different organizations occur. This dual-sub-layer approach not only facilitates efficient data sharing, but also ensures data privacy, since the information managed within one layer remains concealed from the other layer (as already proved in other scenarios [36, 37]). More specifically, the logical division in the access sub-layers of DTs is attained through a combination of the use of topics, which are the channels that handle pub/sub messages, with access control. This orchestration ensures that communication pipelines are distinctly compartmentalized into various topics, all the while adhering to standardized communication protocols. Secondly, we consider pub/sub architecture as the communication architectural basis for our DT communities' model, where all communications occur within a communication infrastructure designed

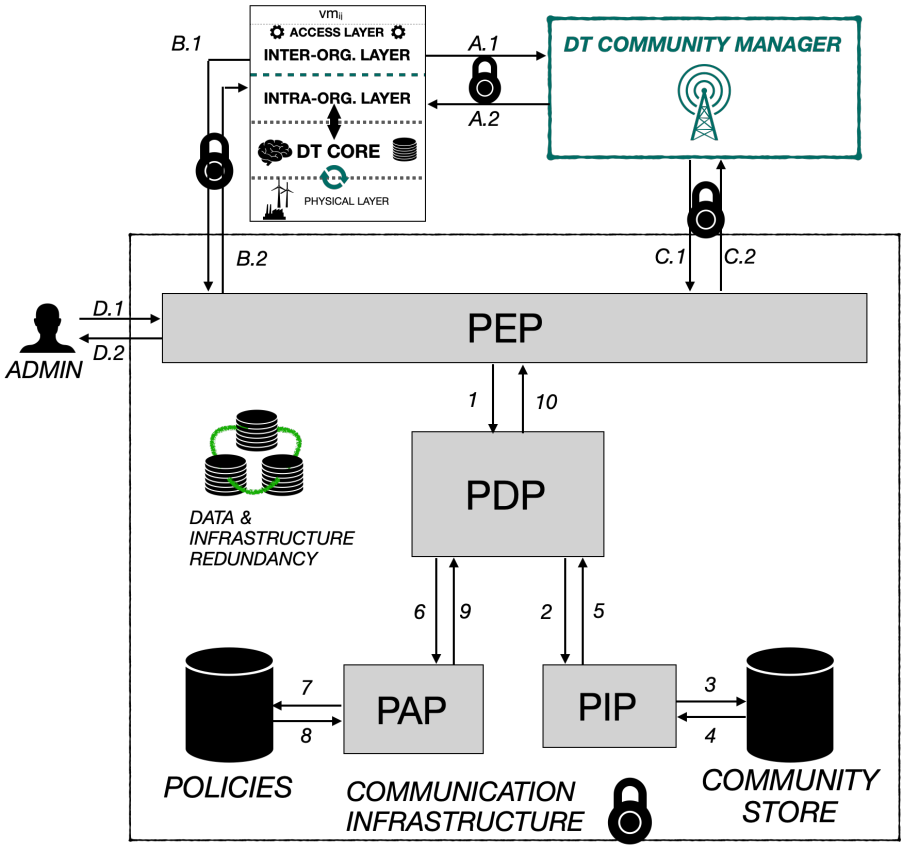

Figure 3: DT Communities Data Sharing through Access Control Architecture

to manage shared data. One notable advantage of this type of communication is that the entity sharing data remains unaware of the data recipients; however, trust relationships established by DT communities facilitate secure data sharing while preserving data privacy. The widespread adoption of pub/sub architecture as a solution for facilitating effective communication among collaborative CPSs [2, 16, 23] serves as a validation of its relevance within the scope of this paper.

Delving deeper into access control of the architecture proposed in this paper, Figure 3 illustrates the resulting access control architecture integrated into the communication infrastructure of the pub/sub architecture. This architecture combines the classical Role-Based Access Control (RBAC) with the modern Organizational-Based Access Control (OrBAC) models [27]. The incorporation of RBAC facilitates streamlined policy management, harnessing its simplicity, while the integration of OrBAC extends the architecture's capabilities into the scope of inter-organizational access control. In order to achieve a more standard-

ized approach and fine-grained access control, we refined our DT Communities concept to align with the standardized XACML (eXtensible Control Markup Language) architecture [43]. XACML is an access control standard that defines a reference architecture for Attribute Based Access Control (ABAC) and provides a language for its implementation. Given that ABAC extends the capabilities of RBAC [27], it presents itself as a fitting choice for adapting our architecture to meet our specific requirements. Therefore, we take the main functions of access control, such as Policy Decision Point (PDP), Policy Enforcement Point (PEP), Policy Administration Point (PAP), and Policy Information Point (PIP), and integrate them into the communication infrastructure of our pub/sub architecture, thereby assembling a holistic representation of our approach within the framework of a reference architecture. In addition, we introduce a novel component termed the *CommunityManager*, which acts as an intermediary between the DTs and the communication infrastructure and is responsible for dynamically overseeing access control management, such as user creation, deletion, and modification, among other tasks. Its primary utility is its adaptability to dynamically generated DTs.

Following the depicted figure, the flow of access control within DT communities unfolds as follows:

1. The process is initiated by a publish or subscribe request (steps B.1, C.1 or D.1) directed towards the communication infrastructure. This initial step could be triggered by one of the following events: automatic user creation, deletion or change request, which is sent by the DT Community Manager; some action by the administrator, which could include actions such as manual configuration; or a request to publish or subscribe request to a DT community action by a pre-existing DT user with a previously assigned role. For instance, Algorithm 1 formalizes how a DT could start the access control process. Assuming a set of pre-defined and pre-configured users $RequestUsers = \{u_{admin}, u_1, u_2, u_3, u_4\}$ with unique permissions enabling them to request the dynamic-creation of DT users for data sharing in DT communities, $u_1 \in RequestUsers$ is used in this example to request a user for a DT, whose permissions will also be assigned dynamically according to the organization's specific data sharing needs. The objective is to request the credentials for a new DT user that has some permissions assigned to a certain role and belongs to a specified community. A set of request and response topics, controlled by the *DT Community Manager*, is also established.

2. The process of dynamic user creation management is exemplified in Algorithm 2. Given a pre-existing set of users, where $RequestUsers \in ExistingUsers \wedge cm_A \in ExistingUsers$, cm_A is the designated user to manage O_A's DT *CommunityManager* module. cm_A is configured with a specialized role facilitating user management within the context of DT communities. In this case, the *CommunityManager* module's user creation management process is exemplified. Firstly, cm_A subscribes to the request

Algorithm 1 DT New Community User Request

Require: $u_1 \in RequestUsers, u_1 \in O_A$
  procedure REQUESTUSER(req_topic, $resp\_topic$, u_1)
    for vm_{Ai} in vm_A **do**
      $role \leftarrow vm_{Ai}.role$
      $community \leftarrow vm_{Ai}.community$
      $u_1.subscribe(resp\_topic)$
      $u_1.request\_user(req\_topic, community, role)$
      enc_msg$\leftarrow u_1.receive_messages()$
      $msg \leftarrow decrypt(enc\_meg)$
      if $ERROR \in msg$ **then**
        $u_1.notifyCommunityManager()$
      else
        $vm_{Ai}.setCredentials(msg.credentials,$
        $community)$
      end if
    end for
  end procedure

topic and waits for a DTs request. After receiving requests, new credentials are issued and transmitted to the PDP, along with the requested community and role. Subsequently, upon receiving the PDP's response, the community manager assesses whether the request was accepted or rejected and publishes the corresponding response to the requester DT on the response topic.

3. It is essential to emphasize that the PDP manages all predefined users and roles in a conventional approach, adhering to the RBAC model. The organizational aspect truly stands out for its dynamic management of users and DT communities, facilitated by the DT *CommunityManager*. Consequently, when cm_A or any pre-defined user tries to publish or subscribe, it generates an event that is intercepted by the PEP, which then proceeds to transform and transmit it (step 1) to the PDP. Afterwards, the PDP requests information (step 2) from the PIP, which consults the *Community Store* database for information about the community to which the requester belongs to (steps 3 and 4). The *Community Store* is a module that checks, if the request implies communication across organizations, the community or communities in which the DT participates, and forwards the information to the PDP (step 5). Once the PDP has obtained all the information needed, it asks the PAP if any of the policies are met by the request (step 6). Then, the PAP checks if the requester has privileges (read/write) over the topics (steps 7 and 8) and sends the results to the PDP (step 9). Finally, the PDP sends the final decision to the PEP (step 10), and it transforms and forwards it to the requester (steps B.2, C.2, D.2). Algorithm 3 specifies the procedure followed by the PDP to

Algorithm 2 CommunityManager dynamic user and role management

Require: $cm_A \in ExistingUsers \wedge cm_A \in O_A$
  procedure ManageCommunity(req_topic, $resp\_topic$, cm_A)
    $cm_A.subscribe(req\_topic)$
    enc_req_msg $\leftarrow cm_A.receive\_messages()$
    $req\_msg \leftarrow decrypt(enc\_req\_msg)$
    for rm_{Ai} in req_msg **do**
      $new\_cred \leftarrow cm_A.create\_secure\_credentials()$
      $req\_id \leftarrow send\_PDP(rm_{Ai}.DT, rm_{Ai}.community,$
      $rm_{Ai}.role, new\_cred)$
      pdp_enc_response $\leftarrow cm_A.wait\_response(req\_id)$
      $pdp\_response \leftarrow decrypt(pdp\_enc\_response)$
      if $ACCEPT \in pdp\_response$ **then**
        $cm_A.publish$(encrypt(new_cred), $resp\_topic$)
      else
        $msg \leftarrow$ '*Request denied*'
        $cm_A.publish$(encrypt(msg), $resp\_topic$)
      end if
    end for
  end procedure

either accept or reject a request. When a request is received, the PDP firs verifies the role by forwarding it to the PAP. The PAP then queries the database for existing roles and permissions; if the role does not exist, it is automatically created. Subsequently, the PDP queries the PIP to determine whether the vm_i DT is affiliated with the requested community. The PIP, in turn, refers to the *CommunityStore* to retrieve this information. The PIP itself incorporates trust mechanisms to establish the trust link, thereby determining membership in a specific community. However, delving into the specifics of these trust mechanisms falls beyond the scope of this paper. At the final stage, the PDP validates the data obtained from both the PAP and the PIP. Based on this assessment, it proceeds to issue either a grant or reject message.

Algorithm 3 How PDP handles requests

  procedure PDP(vm_i, $community$, $role$, $credentials$)
    $role\_data \leftarrow check\_PAP(role)$
    $isMember \leftarrow check\_PIP(vm_i, community)$
    if $role\_data \notin \emptyset \wedge isMember$ **then**
      $send\_request\_granted()$
    else
      $send\_request\_rejected()$
    end if
  end procedure

The implementation of access control integrated in a pub/sub architecture guarantees that communication, whether confined within a community of local DTs or DTs owned by different organizations, is restricted to authorized data sharing. The preservation of confidentiality is further reinforced by employing encryption mechanisms for local communication and establishing secure authenticated and encrypted communication channels for inter-organizational communication. These communication channels are overseen by organizations functioning as community administrators. Additionally, resilience in communication within communities is reinforced by implementing redundancy and clustering mechanisms within the architecture. This ensures high availability, even in the event of communication infrastructure failure. By scaling up the number of infrastructure instances and implementing automatic fail-over mechanisms, uninterrupted communication is maintained. This approach enables effective communication management across multiple organizations. Nevertheless, alternative strategies for securing connections between communication infrastructures in different organizations are viable. One such approach involves the implementation of a semi-automatic central communication infrastructure that functions as a DT community administrator responsible for overseeing all communities, incorporating perimeter protection measures, and administering access control.

This architecture tenders the concept of communities that are both manageable and tangible for any organization utilizing DTs, leveraging its existing resources to make the implementation and integration of DT communities practical and accessible. This is achieved through the simplicity and standardization of the proposed architecture.

Once the communities architecture has been defined, it is critical to highlight how the proposed DT communities scheme relates to Zero Trust Architecture (ZTA), especially in a diversified, multi-organizational context where communities are primarily focused. Therefore, ZTA prioritizes resource protection and continuous trust evaluation. It takes a holistic approach to securing enterprise resources and data, emphasizing identity, access management, and infrastructure integrity [41]. The main points of ZTA were extracted [41], introduced and discussed below:

1. **Continuous authentication**: It entails continuously checking the user or device's identity rather than just once at the start of the procedure, assuring correct identification before proceeding with the authorization process. The proposed DT Communities architecture centers around access control. Consequently, the integration of innovative lightweight continuous authentication mechanisms into the communication infrastructure is recognized as a future work, as the scope of this research does not encompass authentication mechanisms.

2. **Least privilege principles**: Through risk minimization, implementing separation of duties, and employing dynamic access control that considers contextual factors, ZTA provides a means to reduce attack surfaces and

prevent lateral movements within networks. In the context of DT communities, simplicity appears as the key to developing a secure data-sharing environment while keeping communication infrastructure agnostic to each organization. The isolation of this infrastructure, which cannot access the organization's network, ensures a streamlined approach while avoiding the introduction of unwanted technological complications in terms of access control, depending only on the community and role management associated with DTs. Henceforth, our DT communities approach follows the principle of least privilege by using isolation and role-based access to ensure continuous data flow without being constrained by context-based access rules like location or resource consumption. However, it may be desirable to add lightweight resource consumption monitoring combined with trust mechanisms to detect instances of excessive data transfer, thereby enabling mechanisms to eject errant DTs from the communities they belong to.

3. **Encryption**: The ZTA principle goes beyond defining access to resources and hardening network perimeters; it also prioritizes data security through the use of encryption mechanisms that protect information both in transit and at rest. Encryption prevents sensitive data from illegal access, interception, or modification. In harmony with this notion, DT communities enforce encryption for every data transfer. However, given that the communication infrastructure acts as a conduit across communities, establishing trust in its reliability requires robust trust mechanisms, which remains a challenge.

4. **Continuous monitoring**: Continuous monitoring and comprehensive logging of network activities can strengthen security capabilities when implemented. This proactive approach facilitates the implementation of advanced mechanisms like anomaly detection and recognition of suspicious behaviors, enabling real-time identification of potential security threats. DT communities can include continuous monitoring into their communication infrastructure, depending on specific implementations. Despite these monitoring capabilities, the integration of threat, anomaly, and intrusion detection mechanisms remains an interesting challenge, especially in multi-organizational and interconnected scenarios.

This section defined an access control architecture for DT communities and delved into the relationship between ZTA and DT communities architecture, uncovering intriguing prospects for future exploration and highlighting unresolved challenges. These will be elaborated on further in a dedicated section. Moving forward, the subsequent section will focus on examining the usability and governance of communities, addressing potential adoption barriers in real-world scenarios.

4 Usability and real-life scenarios of DT communities

Following the detailed specification of the architecture and its practical adaptation to a specific example in the preceding sections, in this section we delve into the core usability and governance challenges that naturally accompany the implementation of DT Communities across diverse industries and organizations of all sizes.

To facilitate the widespread adoption of DT communities without overburdening organizations with excessive management overhead, it is utmost important to prioritise usability and user experience. This involves designing user interfaces that streamline the management of the platform, ensuring smooth navigation and intuitive controls for both administrators and users. In order to prove the usability of the proposed architecture and the feasibility of DT communities, Figure 4 illustrates a simple GUI for organizations to manage their own DTs in the context of DT communities. Since the proposed architecture stands out for its inherent automation in data sharing and access control, most management responsibilities will be concentrated during the initial implementation phase of the communication infrastructure component. Subsequently, the focus for each organization shifts towards managing its individual DTs, encompassing tasks such as community assignment and specifying data subscriptions or publications. While these tasks could potentially be automated, their execution remains contingent upon the unique requirements of each organization. Therefore, facilitating this management process could involve implementing a user-friendly GUI interface. This interface should present information in a comprehensible manner, accessible to non-technical individuals with expertise in the organization's specific domain (i.e., industrial engineers). It would allow for the management of non-automated elements within the DT communities framework, such as assigning a community to a previously created DT within the organization's trusted network or monitoring the status of DT users.

For a deeper grasp of the usability of the implemented architecture, Figure 5 illustrates the operational flow of communities in two scenarios: when an organization creates a new DT and when another organization activates a preconfigured DT, subscribing to and publishing previously defined information. In an environment with a functioning communication infrastructure, Organization O_A initiates the creation of a new DT. Initially unassigned to any community and lacking access to inter-organizational data sharing, this DT undergoes configuration, specifying the community or communities it will join. Subsequently, it integrates with the communication infrastructure, which then orchestrates user creation and automatically assigns necessary permissions based on preestablished data sharing topics.

Despite the architecture's reduction in management overhead and user-friendly interface facilitating organizational adoption of DT communities, the innovation in technological solutions alone is not sufficient. Indeed, while advancements in data security and privacy are fundamental, they must be complemented by the

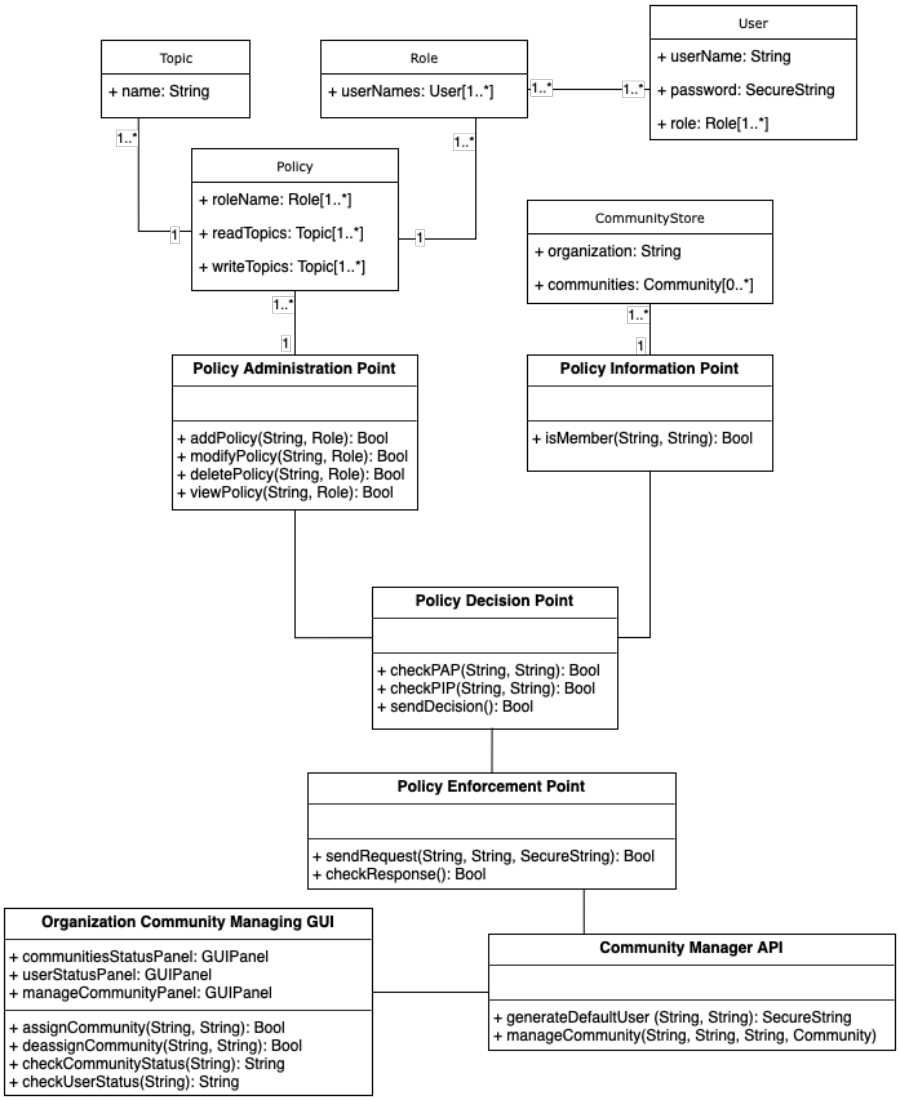

Figure 4: DT communities management class diagram

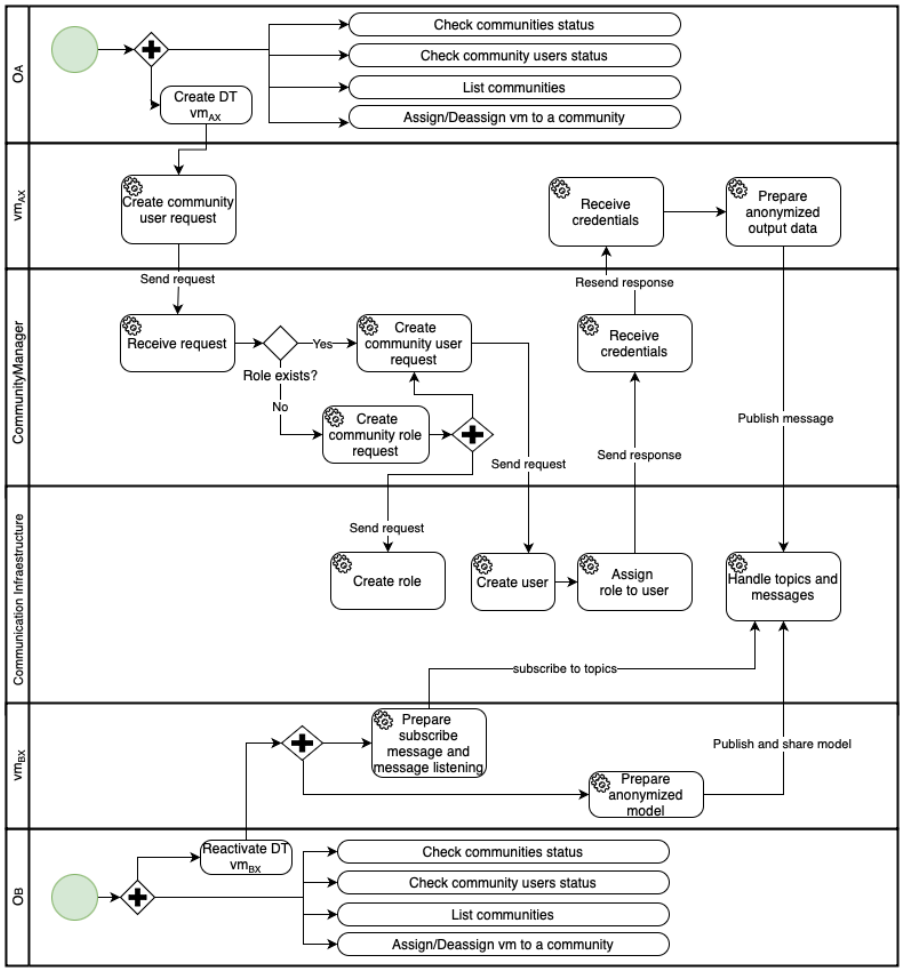

Figure 5: DT communities management usage

establishment of a solid legal framework. Such a framework is indispensable for fostering secure ecosystems for data exchange, whether confined by national borders or across a transnational alliance such as the European Union (EU). EU is a pioneer in this respect, spearheading legislative efforts to harmonize cybersecurity practices across diverse companies and nations. Particularly, two main initiatives surface, set to strengthen inter-organizational collaboration in the years ahead:

- **EU Cyber Resilience Act**: In light of the prevailing deficiency in cybersecurity across numerous products, particularly in the context of IoT devices, the Cyber Resilience Act [10] aims to strengthen cybersecurity on these devices by requiring strict cybersecurity measures for products and software with digital components in order to be marketed. Since sensors and actuators serve as the initial nodes in the DT chain, which are presently vulnerable when connected to the Internet, improving cybersecurity in these devices through widespread adherence to this act holds the potential to significantly boost the foundation of trust among organizations within the EU regarding collaborative DT data sharing through DT Communities.

- **EU Cyber Solidarity Act** [15]: In a context marked by a relentless surge in cyber attacks, supply chain attacks, and cyber espionage, compounded by a growing frequency of assaults on critical infrastructure, the need for collective defense in multi-organizational cyber defense has never been more pressing. Of particular concern are attacks targeting public infrastructure, numerous of which have constrained resources to deal with such attacks. Given the resource constraints faced by many organizations, whether public or private, joint efforts and collaboration aimed at strengthening our collective cyber defenses are critical. Through cohesive partnerships spanning all sectors and sizes, we can bolster resilience and enhance cybersecurity capabilities, thereby strengthening the digital resilience of organizations at all levels [15]. This act generates a robust legislative framework aimed at forging trusted partnerships not only between nations but also between organizations in the cybersecurity environment. It also paves the way for the exchange of cybersecurity data facilitated by DTs through predictive cyber intelligence, for instance. With trust firmly established as a foundation, it lays the groundwork for greater collaboration between organizations from diverse backgrounds and industries, leveraging DT communities to reduce the efforts in obtaining real data sources and DT models.

Although inter-organizational trust for collaboration still remains a challenge, we regard these two recent initiatives as essential steps towards fostering a more collaborative future, particularly within the realm of cybersecurity. In the face of escalating cyber attacks and cyber warfare, this coming together is necessary to address and mitigate the ever-evolving threats that threaten our digital reality.

Figure 6: Industry 5.0-enabled requirements for DT Communities

5 DT-assisted data sharing requirements in Industry 5.0 communities

After establishing the DT communities architecture, the subsequent phase involves delineating the requirements of Industry 5.0 DT communities and evaluating the proposed solution against these benchmarks. This process serves to validate the assertion that DT Communities are indeed instrumental in fostering data exchange within the context of an interconnected Industry 5.0 ecosystem where numerous organizations benefit from sharing data between its DTs.

In 2021, the European Commission defined the concept of Industry 5.0 based on the concept Society 5.0 introduced by the Japanese government [14]. Society 5.0 seeks to harmonize economic growth with the resolution of societal and environmental issues, extending its scope beyond the manufacturing sector to tackle broader social challenges through the convergence of physical and virtual realms. Therefore, Industry 5.0 represents a paradigm shift, redirecting its focus towards creating a human-centric, resilient, and sustainable industrial landscape. All this while maintaining Industry 4.0 objectives, since Industry 5.0 builds upon the foundations of Industry 4.0, which primarily focuses on enhancing production efficiency and flexibility through digitization and AI.

Given the definition of Industry 5.0, we define a set of data sharing requirements for DT communities rooted in the principles of productivity, sustainability, resilience, and human-centricity. **Productivity** [R1] establishes a direct correlation between resource utilization and the outcome of the production process. In the context of Industry 5.0, the overarching objective is to enhance production efficiency, with a key emphasis on the importance of human leadership and participation in the process. Our approach centres on two fundamental aspects: interoperability/coexistence [R1.1] of DTs, and performance [R1.2] as the backbone for enhancing productivity within the organization. These elements are deemed essential for the effective operation of DTs [3]. Furthermore, interoperability is evaluated based on the compatibility of technologies used to integrate DTs for data sharing, as well as standardization and compatibility of data formats. This compatibility ensures the sharing of diverse types of information, including performance metrics, simulations, models, and others. Ultimately, this fosters a collaborative ecosystem where DTs can coexist and facilitate data exchange within their communities. Performance stands as a fundamental requirement, requiring that the architecture design for inter and intra-organizational secure data sharing have a minimal impact on the performance of existing DTs. Moreover, the intrinsic traits of interoperability and coexistence among DTs are intimately intertwined with the sustainability imperative of Industry 5.0.

Sustainability [R2] is a principle that is inspiring the changes taking place

in the current industrial revolution, particularly in the context of Industry 5.0. Its significance is highlighted by the United Nation's formulation of Sustainable Development Goals (SDGs) as part of the 2030 Agenda [12], which seeks to foster a worldwide partnership aimed at achieving a more sustainable global ecosystem. Among the 17 established SDGs, the focus on innovation, infrastructure, and manufacturing is a testament to the central role sustainability plays in shaping the future of industry and society [25]. Enhancing the sustainability of the DTs inter-organizational data sharing process hinges on prioritizing two core requirements: long-lasting maintainability [R2.1] and efficient resource reuse [R2.2]. These requirements are fundamental in realizing the objective of sustainable data sharing. Effective maintainability is primarily characterized by a design that embodies low complexity [R2.1.1], extensibility [R2.1.2], and scalability [R2.1.3]. By prioritizing a simplified architectural design, we mitigate the risk of introducing unnecessary complexity to existing DTs, reducing the potential for deviations in results that require real-time communication [3]. Furthermore, the modular architectural design enables the incorporation of new features and software components to the existing access control and data sharing model (i.e. an agent that monitors communication for cybersecurity intrusion detection), achieving extensibility. Additionally, data scalability is of vital importance, as the volume of shared data in the process can expand significantly. Employing an approach that emphasizes decoupling, reducing complexity, and enhancing extensibility and data scalability streamlines the process of maintaining the system. This, in turn, results in a reduced investment of human time, allowing for more efficient resource allocation and alignment with a more human-centric and organization-centric approach to problem-solving.

Resilience [R3] embodies the capacity of a system to maintain stable operation and rapidly recover in the face of adversity [25]. When crafting the architecture for data sharing, we prioritize three key elements to ensure resilience: security [R3.1], safeguarding against threats and vulnerabilities and preserving the confidentiality of sensitive information; and redundancy [R3.2], by establishing mechanisms for continuity and robustness in data sharing across multiple organizations. In the context of the inter-organizational data sharing for DT communities architectural design, our primary focus in respect to the security aspects to be addressed revolves around communication security to preserve the utmost confidentiality of information. Additionally, we underscore the significance of access control, as it plays a fundamental role in safeguarding data privacy by ensuring only authorized entities have access to the shared data. The literature highlights the critical significance and imperative need for robust access control for critical systems, such as DTs [3, 38, 39]. Within our DT communities data sharing approach focused on interconnected organizations in Industry 5.0, the construction and integration of an access control architecture are deemed essential. Undeniably, access control is a crucial component of ZTA since it restricts access to resources in a trust zone, and access control is also the fundamental requirement for DT communities Industry 5.0 security requirements. Hence, we identify the extraction of access control [R3.1.1] for both intra- and inter-organizational data sharing as a fundamental requirement. In

Table 1: Comparison of related work

Metrics \ Ref.		[34]	[44]	[9]	[32]	[40]	[17]	[20]	[24]	[11]	Our Work
Access Control	Intra-org.	+	+	++	++	-	+	-	+	+	++
	Inter-org.	-	-	+	+	-	+	-	+	-	++
Data Sharing	Intra-org.	+	+	++	++	++	+	+	+	+	++
	Inter-org.	-	-	+	+	++	+	-	+	-	++
Industry 5.0	R1	+	+	++	+	-	+	-	+	++	++
	R2	-	-	-	-	+	-	-	-	-	++
	R3	+	+	+	+	-	-	-	+	-	++
	R4	-	-	-	-	-	-	-	-	-	++

++: Covered +: Slightly covered -: Not covered

addition, redundancy holds a significant role in bolstering resilience by ensuring the continuity and reliability of data sharing systems. We consider two types of redundancy: communication infrastructure redundancy and communication link redundancy. The communication infrastructure in our DT communities pub/sub architecture is fortified with redundancy mechanisms. In practice, this is achieved through replication of the communication infrastructure server and implementation of fail-safe configurations. Besides, communication link redundancy is maintained through Quality of Service (QoS) mechanisms that reduce packet loss and ensure their reception by re-sending the message in the event of communication failure.

Human-centricity [R4] is a fundamental pillar in Industry 5.0 that encapsulates and harmonizes all the R1, R2 and R3 requirements, weaving them together to create a data sharing framework based on DT communities that places human well-being and efficiency at its core. Besides, DT communities usability covered in Figure 4 and Figure 5 enables organizations to adopt our approach more widely. As noted in Section 4 regulatory frameworks for cybersecurity increasingly stress inter-organizational collaboration; now is the time for human-centric approaches such as DT communities. This transition will benefit and empower numerous individuals who rely on timely and reliable data in their daily operations.

6 Related work and Matching Data Sharing Requirements for Industry 5.0

Several recent studies have provided solutions for DTs' data sharing, each contributing unique solutions and insights. To facilitate a clear and concise understanding of the current state of the art, we have curated the principal findings

and contributions of these studies, organizing them in Table 1 based on their alignment with the criteria outlined in the preceding section. A notable proportion of the corpus of related works is dedicated to the integration of blockchain technology for DT secure data sharing with access control in this context. Consequently, our analysis commences with an examination of blockchain technology approaches, followed by an exploration of alternative methodologies to culminate our search.

Qi *et al.* propose a blockchain-based rollbackable data access control for a secure access control scheme for DT data sharing [34]. However, this solution only focuses on data sharing between sensors and external sources for DT data and does not consider data sharing between intra- and inter-organizational DTs. Although this solution performs well, one of its limitations is the lack of interoperability, and therefore only partially meets R1. Moreover, the issues of scalability and complexity of the blockchain are not addressed, not meeting R2. The inherent secure and redundant nature of blockchain, combined with the proposed approach for privacy, allows this solution to meet R3. On the other hand, Wei *et al.* present a blockchain-based DT data sharing scheme in the context of IIoT [44]. This solution supports both intra-organizational data sharing and access control. Although sharing DT data is addressed, data sharing among DTs is not covered. Besides, the main drawback of this work is that secure data sharing relies on a trusted platform hardware; hence, this solution lacks interoperability and scalability. The performance test demonstrates its degree of efficiency, not meeting R2 and partially meeting productivity criteria (R1). Security and privacy are addressed, fully meeting R3.

Cao *et al.* provide a life-cycle management for DTs using blockchain technology which includes a fine-grained hierarchical access control that combines RBAC and ABAC architectures policy to enable secure data sharing among stakeholders [9]. This work meets both intra- and inter-organizational access control and data sharing requirements, since in the DT lifecycle it contemplates all related stakeholders, such as manufacturers or maintainers. Nonetheless, the data shared among stakeholders does not contemplate data sharing between DTs owned by different organizations. In contrast with previous related works, this approach considers the interoperability problems and includes an interoperability module consisting of a limited set of technologies that interact with the blockchain, meeting R1. Resilience (R3) aspects are addressed as well, while R2 is not met due to lack of maintainability, more specifically due to the need to update the interoperability module and the complexity of the solution. Similarly, Putz *et al.* present a solution for decentralized data sharing of DT and propose a formal access control model to address the security aspects of DT [32]. This study offers strengths and weaknesses similar to [9] but does not solve the problem of interoperability within different blockchain technologies and other technologies. Moreover, Shen *et al.* address the issues of data security and trust among stakeholders in DT data sharing, integrating cloud and blockchain technology [40]. This approach broadly covers data sharing among the same organization and different organization stakeholders. However, access control mechanisms are not covered. Likewise, Dietz *et al.* propose a framework

for secure DT data sharing based on Distributed Ledger Technology (DLT) to overcome the infrastructural challenges of DT data sharing [17]. This work supports data sharing among DTs that belong to the same or different organizations with integrated access control mechanisms. However, the scope of inter-organizational sharing is limited by the DT life-cycle stakeholders in respect to the requirements, none is met because of its complexity and lack of performance testing due to the absence of implementation.

Subsequent to our examination of blockchain-enabled solutions, we delved into a comprehensive exploration of alternative technological approaches, expanding our research to encompass a broader spectrum of possibilities. However, there is little work that addresses both the challenges of inter- and intra-organizational data sharing with integrated access control. This is the case of Gehrmann and Gunnarsson [20], who provide a security framework for secure DT data synchronization. This architecture covers secure information sharing between physical and virtual space but does not cover information sharing across DTs nor covers Industry 5.0 requirements. Lau *et al.* also presented a security and privacy scheme which combines cloud technology and ABAC for DT-based traffic control authenticity and reliability of data sources [24]. The proposed model covers both access control and data sharing requirements. Conversely, this approach only focuses on traffic control DTs. Hence, the use case is very specific and only works for this type of DT. The restricted type of DT impacts interoperability and data scalability, partially meeting R1 and not meeting R2. This solution addresses confidentiality, but not redundancy, thus partially meeting R3. Moreover, Cathey *et al.* propose the use of multiple DTs for one object supported by edge devices to boost performance and reduce latency for DT real-time data sharing [11]. This approach serves as a solution for secure data sharing among DTs, and its design includes an access control solution. However, inter-organizational data sharing and access control are not addressed.

In contrast to the prevalent trend in the literature that explores the integration of blockchain technology for various applications, the approach presented in this paper adopts a simpler yet highly practical approach based on a pub/sub architecture. It is worth noting that while blockchain presents a viable solution for resource sharing among multiple parties, its application is less practical for a single company seeking to share resources exclusively among its own DTs or substations. In such centralized scenarios, deploying an alternative solution is necessary due to the inherent cost of blockchain technology. Consequently, our DT communities approach prioritizes efficiency and maintainability with an organizational-centric nature while enabling both inter- and intra-organizational data sharing. DT communities are particularly beneficial when organizations lack resources for blockchain deployment or prefer classical approaches to avoid complexities, especially those that provide the blockchain networks in critical scenarios [6, 28]. To conclude, by prioritizing the security and redundancy of blockchain technology, our solution addresses the challenge of inter- and intra-organizational data sharing in a non-complex manner.

7 Experimental design and evaluation results

This section provides a Proof of Concept (PoC) to show the feasibility of the proposed approach. To do so, we consider the Community Manager (see Section 3) to dynamically generate and launch DTs with pre-assigned roles. For the intra- or inter-organizational communication in O_A we consider a broker pattern [42] as the communication infrastructure. In particular, the MQTT (Message Queuing Telemetry Transport) protocol is used so as to simplify the data exchange process under the control of a broker implemented with mosquitto [26] with integrated support for RBAC [19].

As mentioned, a set of four primary pre-defined roles pdRoles = {instanceManager, entityManager, simulationManager, viewer} has been defined (also refer to Table 2). This categorization is constructed considering that DTs within a community encompass both instances and entities. Specifically, a DT instance corresponds to the DT itself, while entities represent the elemental components, such as devices, which collaboratively constitute the DT. Henceforth, we articulate the defined Use Cases (UCs) for data sharing and the related roles as follows:

Table 2: Definition of roles and topics

Role \ Privilege	Read	Write
instanceManager	/comm_name/entities_info/+/#	/comm_name/entities_info/+\#
entityManager	/comm_name/inst_name/entities/+/outputs /comm_name/inst_name/manage/entities/entity_name/inputs /comm_name/inst_name/manage/entities/entity_name/vars	/comm_name/inst_name/entities/entity_name/outputs
simulationManager	/comm_name/+/manage/entities/#	/comm_name/+/manage/entities/#
viewer	/community_name/entities_info/+/#	X

- **Use case 1 (UC-1)**: An instance is required to share its specifications (DT model sharing) and access the specifications of other instances within a community. To facilitate this, a designated topic has been specified, entailing both read and write permissions which are assigned to an "instanceManager" role.

- **Use case 2 (UC-2)**: An entity is needed to share the results of its computations or simulations and simultaneously read information regarding the output values of other entities within the same instance inside a community to be used as an input for its own computations. Additionally, it must have the capacity to access input values and simulation variables. To achieve these specifications, four distinct topics have been delineated—three for reading and one for writing. Correspondingly, an "entityManager" role name has been established to govern these privileges.

- **Use case 3 (UC-3)**: Considering the simulation capabilities inherent in the DT, another role name, "simulationManager", is needed. This role is designed to dispatch input data to entities, facilitating the simulation of specific simulation needs within the organization. To cater to this requirement, a series of topics have been defined under the common root "/comm_name/+/manage/entities/", where the simulator possesses both reading and writing permissions. Various use cases illustrate the significance of this role, such as simulating a system attack to assess its response and performance. In such scenarios, the simulator is empowered to transmit inputs and receive the corresponding simulation output information.

- **Use case 4 (UC-4)**: Lastly, there is a crucial requirement to replicate other DTs for utilization and integration with distinct instances within the organization. To address this need, the "viewer" role has been established, granting the capability to read all twin instances within the same community. This role facilitates the essential function of cloning DTs, ensuring their seamless deployment and connection to various instances within the inter- and intra-organizational context.

The implementation was evaluated based on the impact of our PoC on the performance of the computer where the solution was deployed during the creation and simultaneous connection of an increasing number of users. The computer used for the deployment was running Windows 10 Pro x64 with 32 GB of RAM and an Intel(R) Core (TM) i7-9700K processor with 8 CPUs and an Intel(R) Ethernet Connection (7) I219-V network card. The tests were deployed and executed in a docker container with 24GB of RAM and 218GB of disk assigned.

Figure 7 provides a visual representation of the metrics acquired during the user creation process. This procedure involves initiating a request for user creation through the *CommunityManager*, which oversees the creation and subsequently supplies the requester with the necessary credentials. The evaluation of device performance encompasses the utilization percentage of the CPU, disk,

Figure 7: Device and network performance test of user creation using the implemented architecture

Figure 8: Device and network performance test of user connection and activity

and RAM, while network efficiency is determined by the volume of bytes transmitted and received.

Analysis of the evaluation results reveals that the user creation process exerts minimal impact on device performance, as evidenced in the negligible alterations in CPU, memory, and disk usage percentages. The parity in the quantity of bytes transmitted and received is consistent, exhibiting a direct correlation with the number of users created. This observation aligns with the intended architecture, as shown by the correspondence between each user creation request message and the subsequent response message from the *CommunityManager*. The designed system operates in such a way that each inquiry for user creation triggers a corresponding and timely response.

Figure 8 offers an additional graphical depiction of the metrics collected throughout the user connection and message exchange processes. This sequence encompasses connecting each generated user to the broker by leveraging credentials obtained in the preceding step. Subsequently, users engage in the publication and subscription to predefined topics outlined in Table 2. The evaluation of both device and network performance adheres to the identical metrics and methodology employed in the preceding test. An examination of the assess-

ment outcomes reveals that the user connection process has a negligible impact on device performance concerning CPU and disk usage, demonstrating minimal fluctuations throughout the test. However, RAM usage exhibits a gradual ascent, reaching full capacity at 100% when 1500 users are concurrently connected. This indicates a practical constraint of around 1000 users on a singular machine, with optimal connection levels ranging between 800 and 1200 users, contingent upon the chosen usage threshold (60-80% for this instance). While this may seem restrictive, it is crucial to note that the machine designated for testing is not anticipated to sustain an extensive number of simultaneous users. The primary point for message transmission and reception is anticipated to be the client itself, with probable deployment in a separate environment. Even in a worst-case scenario where all components are co-located, this solution exhibits substantial capacity to manage a considerable volume of simultaneous connections without overburdening the equipment, since the (broker) communication infrastructure should be deployed in a different server. In respect to network performance, the volume of bytes transmitted and received is similar to the previous test, converging on the plotted figure. It is essential to highlight that, in both the current and previous tests, synchronization mechanisms have been employed. These mechanisms introduce pauses to await for message arrival upon publication, enhancing control over message flow and guaranteeing the prevention of any loss. Consequently, the near parity in the counts of sent and received messages is an anticipated outcome.

Regarding the evaluation results, these findings underscore the solution's remarkable capacity to exert minimal influence on RAM, CPU, and disk usage, simultaneously fostering a normative level of network usage. This fortifies resource reuse (R2.2), as the solution seamlessly integrates into any pre-existing server infrastructure with nominal performance impact. In contrast to reviewed blockchain alternatives in the literature, this solution stands out by sidestepping the exigent resource requirements associated with deploying a blockchain infrastructure. In addition, note that the main limitations of our work include the absence of authentication and trust mechanisms, which, if included, would make our approach completely compliant with ZTA principles. Additionally, there are performance challenges as well, in particular concerning RAM usage when a substantial volume of users engage in message exchange within a single machine. It is essential to emphasize that RAM-related issues arise during the implementation phase, specifically within PoC implementation. Substantial enhancements in performance can be achieved through RAM optimization strategies. These limitations are to be addressed in future work.

8 Remaining challenges and new chances

Throughout the presented research, several constraints have been discovered that present fascinating challenges in the field of inter-organizational communication, particularly amongst DTs. Primarily, fostering trust among diverse organizations is critical to materializing cohesive DT communities. The EU

has spearheaded initiatives to formalize a trust ecosystem through the Cyber-Solidarity Act and the Cyber-Resilience Act, which together foster a favorable ecosystem. Yet, advancing beyond legislative measures that take time to implement, there's a pressing need for automatic trust mechanisms. These techniques should enable DTs across organizations to discern trusted DT communities autonomously, eliminating the dependency on designated individuals for trust assessment. Despite progress, current trust mechanisms are still in their early stages, with few effective solutions.

Privacy, on the other hand, presents yet another fundamental barrier to inter-organizational trusted data sharing. In the age of collaborative data sharing, respecting privacy necessitates more than just anonymization and encryption. With the ongoing and upcoming disruptions caused by AI, there is a need to explore deeper. Exploring mechanisms such as differential privacy, multi-party security, and federated learning becomes critical for real-time data sharing situations that allow for the use of AI tools while protecting privacy.

Moreover, addressing both scalability and security concerns in infrastructure, this study explores the implementation of a redundant communication infrastructure to ensure availability, scalability, and real-time communication capabilities. Yet, to fully exploit the potential of DT communities, it is essential to explore inter-organizational communication infrastructures that go beyond reliance on particular organizational resources, opting instead for distributed and decentralized systems. Here, blockchain emerges as a promising avenue, offering potential regardless of the scale or complexity of data-sharing networks. Such infrastructures must encompass solid mechanisms for trust, privacy, and confidentiality while also prioritizing efficiency in terms of green cybersecurity, which is becoming an increasingly important concern. Given that sustainability lies at the core of Industry 5.0, green cybersecurity becomes critical, underscoring the need for data sharing mechanisms that are both resilient and environmentally conscious. Consequently, establishing an infrastructure that is not only resilient, sustainable, and organization-centric but also optimal poses a strong challenge.

An additional complex issue is data sovereignty when shared. This entails not only the capacity for organizations to share data but also to retain control over its usage and the ability to retract access. To realize this, exploring trust and reward-based mechanisms in the context of inter-organizational data sharing might be intriguing. Exploring lightweight access control solutions becomes vital to regulating data usage effectively, with approaches like UCON (Usage Control) [31] demonstrating potential, particularly in the field of inter-organizational communication among DTs. Additionally, ensuring the comprehensive protection of DTs is indispensable for enabling a secure model within DT communities. While safeguarding individual DT components like virtualization and networks is feasible, protecting DTs as a whole remains a complex challenge and the scientific community is repeatedly calling for a definitive solution to this important issue [3, 4]. The introduction of new attack surfaces associated with DTs adds complexity to this task, requiring novel strategies to mitigate potential vulnerabilities effectively.

Finally, as exemplified in Section 2, interoperability is required in a smart

grid scenario in which multiple and diverse stakeholders collaborate through DT communities. However, while our DT community approach provides communication interoperability, data interoperability remains a motivating challenge because incorporating large outcomes from various DTs and organizations necessitates the use of current technologies such as big data, AI, or machine learning (ML), all of which have privacy issues that, as previously stated, are demanding [35].

9 Conclusion and future work

When appropriately shared, the information encapsulated within digital twins, and particularly simulation data possesses the potential to significantly enhance the analytical, decision-making, and operational capacities of organizations. The multiple advantages of digital twins combined with the appropriate data sharing between organizations or between sub-entities within an organization, significantly increases their advantages. Moreover, aligning with the contemporary context of Industry 5.0, DTs empower organizations not just with knowledge acquisition, but also with the practical application of the three inherent goals of Industry 5.0, achieving a resilient, sustainable and human-centric data-sharing method. The combination of the advantages of Industry 5.0 digital twin-based inter- and intra-organizational data-sharing motivated us to establish Industry 5.0 requirements, create the concept of DT communities and integrate this concept in an access control architecture that encapsulates all the functionality of data-sharing with integrated security and meeting Industry 5.0 requirements. A practical application of the designed architecture and implementation was also proposed, and a performance evaluation was performed to test Industry 5.0 requirements. In addition to proposing an application of the devised architecture and its subsequent implementation, a comprehensive performance evaluation was conducted to assess its adherence to the requirements of Industry 5.0. The next steps for our research will include extending of the proposed architecture with privacy, trust, authentication mechanisms, and threat detection, thus addressing the security limitations of the proposed solution. In addition, RAM performance in scenarios where a large amount of connected and active users will be improved by optimizing the architecture and applying memory management in the implementation phase, to address the scalability issues detected in the experiments phase. Consequently, experiments will be extended to include diverse scenarios with more sophisticated DTs to test the Industry 5.0 requirements within the extended architecture.

10 Acknowledgements

Authors would like to thank the company S2Grupo for providing useful comments and feedback for improvements of the paper. The work has been partially supported by the project SEGRES (EXP-00131359/MIG-20201041) funded by

the CDTI as part of the Ministerio de Ciencia, Innovaciación y Universidades; by the project SecTwin 5.0 (TED2021-129830B-I00), funded by MCIN/AEI/10.13039/501100011033 and by the European Union "NextGenerationEU"/PRTR; and by the project DUCA (101086308) funded by the European Union under HORIZON-TMA-MSCA-SE.

References

[1] Adel A (2022) Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. Journal of Cloud Computing 11(1):1–15

[2] Al-Jaroodi J, Mohamed N (2018) Pscps: A distributed platform for cloud and fog integrated smart cyber-physical systems. IEEE Access 6:41,432–41,449, DOI 10.1109/ACCESS.2018.2856509

[3] Alcaraz C, Lopez J (2022) Digital twin: A comprehensive survey of security threats. IEEE Communications Surveys & Tutorials 24(3):1475–1503, DOI 10.1109/COMST.2022.3171465

[4] Alcaraz C, Lopez J (2023) Protecting Digital Twin Networks for 6G-enabled Industry 5.0 Ecosystems. IEEE Network Magazine 37(2):302–308, DOI 10.1109/MNET.004.2200529

[5] Alcaraz C, Fernandez-Gago C, Lopez J (2011) An early warning system based on reputation for energy control systems. IEEE Transactions on Smart Grid 2(4):827–834, DOI 10.1109/TSG.2011.2161498

[6] Alcaraz C, Rubio JE, Lopez J (2020) Blockchain-assisted access for federated smart grid domains: Coupling and features. Journal of Parallel and Distributed Computing 144:124–135, DOI https://doi.org/10.1016/j.jpdc.2020.05.012

[7] Ali M, Kaddoum G, Li WT, Yuen C, Tariq M, Poor HV (2023) A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems. IEEE Transactions on Information Forensics and Security

[8] Attaran M, Celik BG (2023) Digital twin: Benefits, use cases, challenges, and opportunities. Decision Analytics Journal 6:100,165, DOI https://doi.org/10.1016/j.dajour.2023.100165

[9] Cao X, Li X, Xiao Y, Yao Y, Tan S, Wang P (2022) Bdtwins: Blockchain-based digital twins lifecycle management. In: 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), IEEE, pp 2003–2010

[10] Car P, De Luca S (2022) Eu cyber resilience act. EPRS, European Parliament

[11] Cathey G, Benson J, Gupta M, Sandhu R (2021) Edge centric secure data sharing with digital twins in smart ecosystems. In: 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), IEEE, pp 70–79

[12] Cf O (2015) Transforming our world: the 2030 agenda for sustainable development. United Nations: New York, NY, USA

[13] Chen Z, Huang L (2021) Digital twins for information-sharing in remanufacturing supply chain: A review. Energy 220:119,712, DOI https://doi.org/10.1016/j.energy.2020.119712

[14] Commission E, for Research DG, Innovation, Breque M, De Nul L, Petridis A (2021) Industry 5.0 – Towards a sustainable, human-centric and resilient European industry. Publications Office of the European Union, DOI doi/10.2777/308407

[15] Council of European Union (2024) Cyber solidarity act, text of the provisional agreement, 20 march 2024. https://www.consilium.europa.eu/media/70805/ st08047-en24.pdf

[16] Crnkovic I, Malavolta I, Muccini H, Sharaf M (2016) On the use of component-based principles and practices for architecting cyber-physical systems. In: 2016 19th International ACM SIGSOFT Symposium on Component-Based Software Engineering (CBSE), pp 23–32, DOI 10.1109/CBSE.2016.9

[17] Dietz M, Putz B, Pernul G (2019) A distributed ledger approach to digital twin secure data sharing. In: Data and Applications Security and Privacy XXXIII: 33rd Annual IFIP WG 11.3 Conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, Proceedings 33, Springer, pp 281–300

[18] Dietz M, Schlette D, Pernul G (2022) Harnessing digital twin security simulations for systematic cyber threat intelligence. In: 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), pp 789–797, DOI 10.1109/COMPSAC54236.2022.00129

[19] Eclipse Foundation (2021) Dynamic security plugin. URL https://mosquitto.org/documentation/dynamic-security/

[20] Gehrmann C, Gunnarsson M (2019) A digital twin based industrial automation and control system security architecture. IEEE Transactions on Industrial Informatics 16(1):669–680

[21] Gopstein A, Nguyen C, O'Fallon C, Hastings N, Wollman D, et al (2021) NIST framework and roadmap for smart grid interoperability standards, release 4.0. Department of Commerce. National Institute of Standards and Technology ...

[22] Hellmeier M, Pampus J, Qarawlus H, Howar F (2023) Implementing data sovereignty: Requirements & challenges from practice. In: Proceedings of the 18th International Conference on Availability, Reliability and Security, Association for Computing Machinery, New York, NY, USA, ARES '23, DOI 10.1145/3600160.3604995

[23] Karsai G, Balasubramanian D, Dubey A, Otte WR (2014) Distributed and managed: Research challenges and opportunities of the next generation cyber-physical systems. In: 2014 IEEE 17th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing, pp 1–8, DOI 10.1109/ISORC.2014.36

[24] Lai C, Wang M, Zheng D (2022) Spdt: Secure and privacy-preserving scheme for digital twin-based traffic control. In: 2022 IEEE/CIC International Conference on Communications in China (ICCC), IEEE, pp 144–149

[25] Leng J, Sha W, Wang B, Zheng P, Zhuang C, Liu Q, Wuest T, Mourtzis D, Wang L (2022) Industry 5.0: Prospect and retrospect. Journal of Manufacturing Systems 65:279–295, DOI https://doi.org/10.1016/j.jmsy.2022.09.017

[26] Light RA (2017) Mosquitto: server and client implementation of the mqtt protocol. Journal of Open Source Software 2(13):265

[27] Lopez J, Rubio JE (2018) Access control for cyber-physical systems interconnected to the cloud. Computer Networks 134:46–54, DOI https://doi.org/10.1016/j.comnet.2018.01.037

[28] Lopez J, Alcaraz C, Roman R (2013) Smart control of operational threats in control substations. Computers & Security 38:14–27, DOI 10.1016/j.cose.2013.03.013

[29] Lopez J, Rubio JE, Alcaraz C (2018) A resilient architecture for the smart grid. IEEE Transactions on Industrial Informatics 14:3745–3753, DOI 10.1109/TII.2018.2826226

[30] Lopez J, Rubio JE, Alcaraz C (2021) Digital twins for intelligent authorization in the b5g-enabled smart grid. IEEE Wireless Communications 28:48–55, DOI 10.1109/MWC.001.2000336

[31] Park J, Sandhu R (2004) The uconabc usage control model. ACM transactions on information and system security (TISSEC) 7(1):128–174

[32] Putz B, Dietz M, Empl P, Pernul G (2021) Ethertwin: Blockchain-based secure digital twin information management. Information Processing & Management 58(1):102,425

[33] Qi Q, Tao F, Hu T, Anwer N, Liu A, Wei Y, Wang L, Nee A (2021) Enabling technologies and tools for digital twin. Journal of Manufacturing Systems 58:3–21, DOI https://doi.org/10.1016/j.jmsy.2019.10.001, digital Twin towards Smart Manufacturing and Industry 4.0

[34] Qi S, Yang X, Yu J, Qi Y (2023) Blockchain-aware rollbackable data access control for iot-enabled digital twin. IEEE Journal on Selected Areas in Communications

[35] Rahman A, Hasan K, Kundu D, Islam MJ, Debnath T, Band SS, Kumar N (2023) On the icn-iot with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems 138:61–88

[36] Rios R, Lopez J (2011) Analysis of location privacy solutions in wireless sensor networks. IET Communications 5:2518 – 2532, DOI 10.1049/iet-com.2010.0825

[37] Rios R, Lopez J (2011) Exploiting context-awareness to enhance source-location privacy in wireless sensor networks. The Computer Journal 54:1603–1615, DOI 10.1093/comjnl/bxr055

[38] Rubio JE, Alcaraz C, Roman R, Lopez J (2019) Current cyber-defense trends in industrial control systems. Computers & Security 87:101,561

[39] Schroeder GN, Steinmetz C, Rodrigues RN, Henriques RVB, Rettberg A, Pereira CE (2020) A methodology for digital twin modeling and deployment for industry 4.0. Proceedings of the IEEE 109(4):556–567

[40] Shen W, Hu T, Zhang C, Ma S (2021) Secure sharing of big digital twin data for smart manufacturing based on blockchain. Journal of Manufacturing Systems 61:338–350

[41] Stafford V (2020) Zero trust architecture. NIST special publication 800:207

[42] Stal M (1995) The broker architectural framework. In: Workshop on Concurrent, Parallel and Distributed Patterns of Objects Oriented Programming, held at OOPSLA, Citeseer, vol 95, pp 1–19

[43] Standard O (2013) extensible access control markup language (xacml) version 3.0. A:(22 January 2013) URl: http://docs oasis-open org/xacml/30/xacml-30-core-spec-os-en html

[44] Wei W, An B, Qiao K, Shen J (2023) A blockchain-based multi-users oblivious data sharing scheme for digital twin system in industrial internet of things. IEEE Journal on Selected Areas in Communications