C. Alcaraz, and J. Lopez, "Protecting Digital Twin Networks for 6G-enabled Industry 5.0 Ecosystems ", *IEEE Network Magazine*, vol. 37, pp. 302-308, 2023.
http://doi.org/10.1109/MNET.004.2200529
NICS Lab. Publications: https://www.nics.uma.es/publications

Protecting Digital Twin Networks for 6G-enabled Industry 5.0 Ecosystems

Cristina Alcaraz and Javier Lopez

Computer Science Department,University of Malaga,

Campus de Teatinos s/n, 29071, Malaga, Spain

{alcaraz, javierlopez}@uma.es

Abstract

New industrial paradigms, such as the Industrial Internet of Things (IIoT) and Industry 5.0, are emerging in industrial contexts with the aim of fostering quality in operational processes. With the expected launch of 6G in the coming years, IIoT networks in Industry 5.0 ecosystems can leverage 6G technology and its support for training machine learning models using Digital Twins (DTs), embedded in DT Networks (DTNs), to transparently and continuously optimize their communications. Unfortunately, the use of these technologies, in turn, intensifies the attack surface and poses a serious threat to the new goals of Industry 5.0, such as improving the user experience, sustainability and resilience. This paper therefore proposes a layered protection framework for 6G-enabled IIoT environments, where not only DTs and DTNs are fully protected, but also the whole 6G ecosystem, complying with the expected goals of Industry 5.0. To achieve this, the framework identifies for each protection layer a set of security and privacy services to subsequently relate them to existing computing infrastructures (cloud, edge, edge-cloud) and provide the best approach for future IIoT deployments.

Keywords: Digital Twin Network, 6G, Industrial Internet of Things, Industry 5.0, Cybersecurity.

1 Introduction

6G technology aims to expand connections by *space-air-ground-sea* [1] and provide (approximately) zero-latency interactions with energy efficiency guarantees for time-sensitive Industrial Internet of Things (IIoT) applications, such as immersive multimedia, brain-computer interaction, tactile Internet and autonomous driving. This implies working in terms of Terabps and Terahertz with support to create reliable and flexible communication environments [2], especially for those 6G-enabled IIoT networks. In this setting, Artificial Intelligence

(AI) and Machine Learning (ML) become essential for adapting 6G services according to the real demand, the level of mobility and the heterogeneity of the context. However, this support is only ideal as long as ML models are deployed consistently throughout the system. Their training and testing phases can be time- and resource-intensive if executed within IIoT devices, which are critical to real-time operational environments. For that reason, the current trend is to distribute and allocate those phases in computing infrastructures (cloud, edge, cloud-edge) whose servers integrate Digital Twins (DTs) [1,3,4] and are deployed close to the application scenario.

DT is among the most prominent technologies nowadays for its ability to digitally represent and simulate the behavior, statuses and dynamics of a corresponding physical counterpart, which can be a simple object or a complex system. This level of simulation, guided primarily by mathematical principles, conceptual theories and predictive models, is characterized by connections to the real world, allowing DTs to perceive the context for synchronization and make decisions to change the behavior or operation of their physical counterparts [5]. This capability is described in [4] as *Operational DT*, differentiating it from those that only monitor or simulate scenarios in order to gain insights and analysis. Currently, in the particular case of Operational DTs, integrated digital models make it possible to dynamically and autonomously diagnose, forecast and optimize solutions and services such as those expected from 6G networks [6] and for IIoT scenarios. For that reason, operational DTs are of particular interest for our paper (we will refer to them simply as DTs) because they are able to simulate physical IIoT devices to learn [7] about their context and orchestrate their physical connections based on ML model training carried out from the DT, thereby optimizing physical world operations, connectivity through 6G networks, and quality of user experience [3]. Moreover, when individual DTs are interconnected to virtually recreate an IIoT subnetwork, they form a Digital Twin Network (DTN). It is then possible to create a DTN system (composed of several DTNs) and foster mobility among IIoT networks through migration of DTs between DTNs [8]. This way of decentralizing learning across the DTN system to build or improve ML models gives rise to the concept of Federated Learning (FL).

Undoubtedly, these technological advancements, including FL, can bring innovative and important business opportunities for stakeholders, especially within the new Industry 5.0 paradigm [9]. This paradigm is increasingly relevant in many of today's automation applications because of the creation of intelligent, hyper-connected and technologically enriched industrial ecosystems [5], and is characterized by three main goals [9]: *human-centricity* (G1) to improve the user experience and its integration and interaction with the real world; *sustainability* (G2) to ensure reliable operation and communication over a long period of time as well as energy saving; and *resilience* (G3) to prevent unforeseen threats, ensuring business continuity at all times.

Due to the novelty of these technologies and paradigms, there is still a lack of research on the benefits of integrating DTNs and 6G in the context of Industry 5.0, though we can envision some immediate examples. For instance, FL

and the use of advanced visualization interfaces (e.g. mixed and extended reality) with explanatory dashboards may enable human operators to make much more efficient decisions, hence fulfilling G1, probably under the premise of coworking. Also, FL can help to allocate functional capabilities of IIoT devices as covered by G2, whereas the combined use of DTN with computing infrastructures (as discussed throughout this paper) may benefit 6G protection, thus meeting G3. Regarding the last example, this type of support can indeed enable the integration of specialized prevention approaches, with the additional ability to avoid anomalies or intrusions. However, and most probably, because of the heterogeneity of the technologies in the Industry 5.0 arena, G3 is the most challenging to fully achieve, and for this reason it forms the core of this paper. There are already several studies on this issue warning about the security risks in 6G technology ([2, 10]), while a taxonomy of threats to DTs along with their attack surface is comprehensively addressed in [5]. The main problem is that when, additionally, DTs are used in 6G ecosystems, which already have their own particular weaknesses ([2, 10]), the DT attack surface becomes very unmanageable.

To date, there have been very few attempts to address these security issues. Some works have focused on protecting 6G technology [2,10] and DTs [5], though separately. Also, we can find in the literature several works ([2, 4]) on DTNs, where a blockchain network is used as a common repository for trained ML models, and several more focusing on the need for privacy of DT data ([1, 5, 11]). However, beyond these, there are no technical approaches or frameworks based on specific Security and Privacy (hereinafter S&P) servicesaddressing the particular problems of DTNs. In fact, as noted in [12], there are only some initial recommendations and standards for DTs (e.g. ISO-23247-2 [13] and IRTF-DTN [11]). Most of them cover preliminary concepts and essential functions such as synchronization and data management, as well as a generic view of security that does not cover the main protection measures that any typical Industry 5.0 scenario demands (G1, G2 and G3). To fill this gap, this paper thus presents a specific protection framework for 6G-enabled IIoT networks where DTs are integrated into complex DTN networks to support FL and enhance 6G services. This protection framework is based on layers in order to better approach the implicit technological complexity involved in implementing a FL process supported by DTs. Each of the layers integrates a set of particular S&P services and related technologies, which makes it possible to protect not only individual DT models but also the rest of the components that make up a DTN system. To meet the expectations of Industry 5.0, we further analyze how the S&P services can benefit G3, and highlight how the design of the framework additionally benefits G1 and G2. For that reason, we examine the integration of the framework in different computing infrastructures in order to identify which is the most suitable to be applied in the near future.

The paper is organized as follows. Section 2 presents the protection framework, whose S&P services and supporting technologies are established in Section 3. Section 4 discusses the integration of the framework in computing infrastructures, and Section 5 outlines the final remarks and future work.

2 Layered protection for Industry 5.0

Our protection framework for 6G-enabled IIoT networks is focused on two functional spaces of a DT: the physical space comprising IIoT devices, and the digital space with DTN servers hosting the corresponding digital counterparts. The two spaces are connected to allow DTs to: (i) synchronize their DT models; (ii) simulate the QoS of connections of the IIoT devices, (iii) train the ML models based on the context of these devices, and (iv) update these ML models on the IIoT devices in order to optimize their QoS. Unfortunately, this process involves multiple technologies and connections, and therefore intensifies the attack surface, requiring a protection solution based on layers, ranging from DT-level security to DTN system-level security. Therefore, our framework extends the current reference architectures [4, 11, 13] by adding layered protection services that ensure prevention at different levels.

The selection of those protection services is critical. The complex nature of some security services – such as situational awareness (including software agents, AI/ML, consensus and correlation models [5]) for traceability and response to attacks in real time – can affect the operation of DTs and DTNs. One practical way to avoid this situation within our approach is to decouple the functions (divide and conquer) and offload the global protection services to an external dedicated S&P server (or, eventually, more than one), leaving the lighter but essential security services as part of the DTN servers. In this way, the dedicated server can provide a clearer view of the real status of the entire system and respond to adverse (probably distributed and concurrent) situations in optimal time. For an effective response, it must collaborate with DTN servers not only to perceive the local status of each DTN, but also to transmit corrective actions in the event of a threat.

In short, the protection framework is based on the following Protection Layers (hereinafter PL):

- *PL1: local protection in DT.* PL1 protects each virtual IIoT device and its models. Simulations must be error-free and without risk of illicit access that could lead to deviations in the fidelity and accuracy [5] of the trained ML models. This protection comprises all connections involved in the simulation process, including the data storage interface in the Local Repository (LRep) of PL2, common for all DTs.

- *PL2: local protection in DTN/s.* PL2 covers the security of a DTN server and the connection to its neighborhood. This includes secure access to each DT instance hosted on that server (via PL1) and secure access to LRep. The use of this repository, recommended in [11], stores various data, such as trained ML models, DT models as well as security configurations, alarms and logs. Since DTN servers are connected to each other, PL2 also encompasses the secure migration of DTs between neighboring DTNs in order to promote mobility in the physical space.

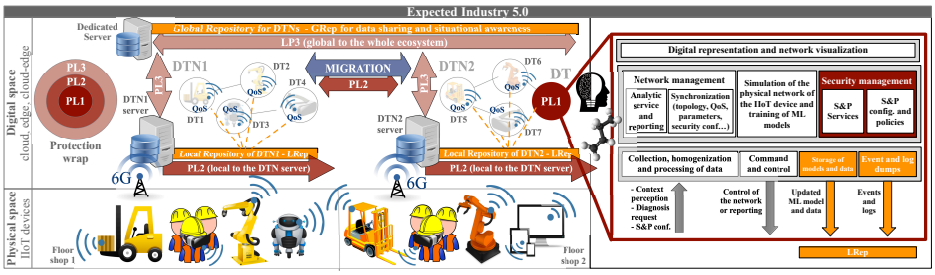

Figure 1: Protection layers for DT-enabled 6G industrial networks – PL1, PL2 and PL3

- *PL3: global protection in the DTN system.* Dedicated servers can dynamically diagnose health status, both locally (within a DT or a DTN/s) and globally (in the DTN system), through situational awareness techniques [14] and a common Global Repository (GRep) (fed back with local information from RepL). In turn, these statuses allow dedicated servers to predict, locate and track advanced threats, and take corrective actions with the help of DTN servers.

To consistently define the protection services for each PL, it is also necessary to establish the functional requirements of the whole framework so that it meets the Industry 5.0 and 6G targets. The requirements are as follows:

- *Uncoupling (1) and lightweight services (2).* Multi-layer protection and S&P services should not add significant overhead and delays to operational tasks. Thus, system decoupling and the selection of "green" S&P solutions become mandatory for operational performance (G1), energy savings (G2), and protection (G3).

- *Maintainability (3) and usability (4).* Modularity of the framework improves the user experience (G1) by facilitating its own management and maintenance and, consequently, its sustainability in terms of operation and protection (G2 and G3). Likewise, the protection framework and its embedded services should facilitate decision-making (G1), and enable the end user to interpret and react accordingly (G2 and G3).

- *Mobility (5) and adaptability (6).* Industry 5.0 expects hyper-connected environments to be created with high mobility guarantees. This means that the framework must manage migration techniques of DTs between DTNs, and adapt them to integrate DTs to the new application context, containing their own security policies. In other words, DTs must adapt transparently to the new security conditions (G1) to ensure not only continuous operation (G2), but also resilience (G3).

To summarize, Figure 1 illustrates the protection framework. The services associated with each PL (and corresponding servers) are defined in the next

section, taking into account support from emergent technologies to meet the requirements (1-6) of the protection framework.

3 Matching services to protection layers

PLs establish the primary lines of defense, to which S&P services and supporting technologies are matched based on the type of asset to be protected, the level of access to repositories (LRep/GRep), and communication with other assets and actors in the system.

3.1 PL1: first-line defense and technologies

PL1 comprises all the essential S&P services that safeguard the DT and its data (at all times), giving full guarantees of the integrity and fidelity of the final results, whose simulations must not clash with the operational requirements of the industrial environment. To achieve this, PL1 is required to comply with requirements (1-3), establishing this first line of defense based on lightweight, independent and modular solutions following the principles of zero-trust and least privilege. Security policies have to be managed by simple Authentication, Authorization and Accounting (AAA) mechanisms (even from PL2) [2] in which every action within a DT (with unique identifiers) must be logged. As shown in Figure 1, the export of records to LRep is vital to foster local monitoring of all DTs and improve context awareness in PL2.

If, additionally, DTs are connected to other entities (including other DTs and LRep), measures related to hardening and malware control must be considered. Integrity techniques (e.g. through hashes) and automated diagnostics are needed to prevent the spread of infections that compromise the granularity and fidelity of DT data [5]. Software agents, under lightweight ML-powered detection techniques, can also check if processes embedded in DTs are working as they should and, if necessary, notify PL3. Priority must also be given to protection at the communications level and in relation to Confidentiality, Integrity and Availability (CIA), authentication and key management. The authors in [2] already identified a set of prospective technologies for 6G, where quantum looks set to jeopardize some of the existing security protocols (SSH, IPSec, TLS). Everything points to a need to reconsider traditional hash functions and symmetric encryption algorithms endowed with suitable keys, and to specify new quantum-resistant public-key cryptographic approaches based, for example, on lattice. On the other hand, simple trust and reputation models (to orchestrate interactions DT-DT, DT-IIoT device, DT-LRep) and location privacy techniques (to protect the location of DTs within a DTN and avoid observation) can also play a relevant role. However, the use of certificates for trust, and random routing and obfuscation for location protection may no longer be sufficient. ML capabilities can be leveraged to automate and guide the process.

3.2 PL2: second-line defense and technologies

As DTN servers have a strong software connotation within their systems with multiple inter-DT and inter-DTN connections, their attack surface is greatly expanded. Thus, PL2 must incorporate more specialized security services into server protection, such as the inclusion of hardware security modules (e.g. Trusted Platform Module (TPM) or Hardware Security Module (HSM)) in line with advances in quantum security cryptography. Also, segmentation under a controlled administration (requirement (4)) is essential, where configurations must be subject to strict security policies and controls. Any event occurring within PL2 and PL1 (as mentioned above) must be logged for local diagnostics and context awareness.

ML-based prediction and agent-driven diagnostics in specific security containers (for decoupling) could locally compute the contextual statuses of each virtual instance. This process, which normally involves combining techniques such as ML, consensus (e.g. Opinion Dynamic) and correlation, can help to trace statuses in real time [5]. Moreover, this method of bringing security to containers can also facilitate co-simulation. Security-specific DTs (*twins of twins*) could monitor, validate and certify compliance with regulatory frameworks, predict deviations and respond when necessary – all for the benefit of G3. In any case, events and diagnostic results from PL2 should also be reported to PL3 and recorded in GRep for situational awareness, which goes beyond context awareness as stated in [14] – thus GRep > LRep. The latter repository, LRep, is critical in nature as it contains DTs, ML models, and configuration and security data. This also means that LRep should remain shielded using encryption techniques (e.g. homomorphic, identity-based, attribution-based, adaptation-based) under quantum-resistant schemes to prevent leaks that threaten device tracking and industrial secrets [5]. This is relevant, because if in the future DTs are expected to render their simulations with quantum advances, quantum+IA may be the perfect Molotov cocktail to corrupt the S&P principles ([2, 5]), and thus presents a future research challenge. Likewise, the availability of this type of repository becomes essential to guarantee the simulation of DTs. In this case, constant monitoring by agents (e.g. in containers for decoupling) in charge of controlling the proper use of these resources and their statuses is essential, and even for context awareness (in PL2) and situational awareness (in PL3).

Beyond secure access to DTs (via PL1), it is also essential to ensure secure access to external entities such as dedicated servers (PL3) and other DTN servers. Indeed, if DTNs can transfer information for situational awareness (PL3) or mobility in order to meet requirement (5), then it is mandatory to protect their communication channels as indicated in Section 3.1, and their positions, so as to avoid possible penetrations that go against FL services. To ensure QoS during mobility processes, incentives to reward the migration process between DTNs (as indicated in [8]) and reputation models could be a good approach.

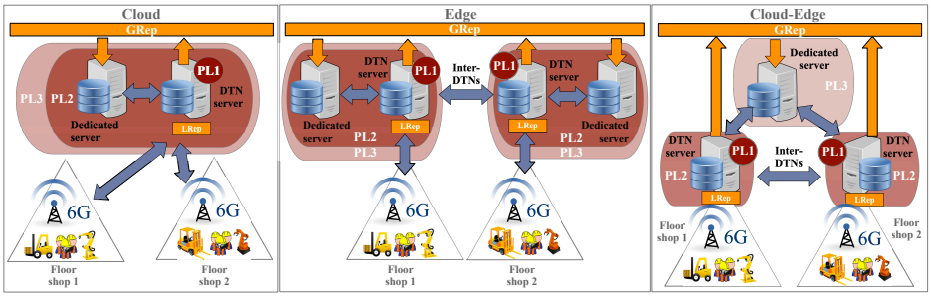

Figure 2: Three possible architectures for the secure deployment of DT-enabled 6G industrial networks

3.3 PL3: third-line defense and technologies

PL3 allows complex security services to be deployed on dedicated servers. To protect these servers, many of the measures discussed in Section 3.2 (e.g. hardware and perimeter security, access control, diagnostics, detection, trust and privacy) can be adopted to subsequently ensure situational awareness and resilience. The goal is to manage dynamically, and from PL3, all the contextual statuses provided by each DTN, making it possible to establish a more comprehensive and complete diagnosis that helps to explain and track what is happening within a DT, a DTN or across multiple DTNs. Therefore, cooperation between PL2 and PL3 is important, as is the use of anomaly-based detection systems. These systems can be designed under collaborative criteria (supported by embedded agents in DTN servers) or based on simulation technologies (in dedicated servers) to estimate anomalies or risks. Indeed, through simulation it is possible to predict variations in the semantic behavior of observed objects, security breaches or non-compliance with regulatory frameworks.

Moreover, future DTN servers in PL2 could leverage the computational capabilities of dedicated servers in order to deploy their own digital twins and optimize their local detection models through FL (for security). Regardless of how detection is managed, its outcome can feed back into other essential security components, such as: risk managers (to predict risks in DTs and DTNs), policy managers to automate PL2 configurations, response systems to prevent risks in advance, or reconfiguration systems to restore statuses, configurations or policies. Similarly, remote attestation can also intensify the protection by verifying (from PL3) the correct operational functioning of the DTN servers in PL2.

As with LRep, GRep is a repository that requires comprehensive protection and availability. Multiple stakeholders can gain access to it to enhance cyber intelligence for data sharing and, consequently, situational awareness. One of the technologies that may be relevant to this management would be permissioned

blockchain networks to promote decentralization, immutability, transparency and auditing, and even secure migration of DTs between DTNs and their rapid adaptation in the new application scenario (complying with requirements (5 and 6)). That is, DTNs only need to access the blockchain to download the DTs, not needing to receive them via the inter-DTNs channels. However, blockchain is still in its infancy and presents weaknesses that need to be noted, particularly in terms of data scalability and privacy [5].

4 Matching protection layers to architectures

As illustrated in Figure 2, the deployment of (S&P and DTN) servers can be centralized on the cloud, distributed at the edge or hybrid, as also stated in [4]. In contrast to [4], we examine the role of these infrastructures from a security standpoint and in accordance with the six requirements of the protection framework detailed in Section 2.

4.1 PL1-3 in the cloud

One of the main issues faced by this architecture is precisely the management of the digital space in the cloud with DTN and dedicated servers working at the same level, in addition to other issues related to the nature of the application scenario and the design of the protection framework. That is, while the scalability, heterogeneity and mobility of the entire IIoT ecosystem may require frequent updating of trained ML models to satisfy expected QoS constraints in the physical space, the centralization of the simulations and the protection framework in the cloud (assuming a limited number of servers) may result in significant bottlenecks. Moreover, in this type of infrastructure, the concept of local learning for each application scenario (related to FL) is completely lost and the tendency would be to create centralized platforms based on the traditional concept of ML as a Service (MLaaS) instead of FL as a Service (FLaaS) [15]. All this can consequently impact the user experience, access and maintenance of S&P services, impacting requirements (3-5) − note that requirement (6) does not apply due to the very centrality of the cloud.

Likewise, since the DTN and dedicated servers work at the same level, security controls from the cloud without the means to manage context awareness by zones can complicate resilience actions, such as real-time health status traceability by area/s. Thus, this type of architecture can lead to significant false positive and false negative rates.

4.2 PL1-3 at the edge

Unlike the cloud, this deployment brings multiple benefits, such as agile communication between spaces, migration and adaptation of DTs along with their corresponding security policies (as long as GRep is considered, e.g. via a blockchain), and diagnostics in local terms. However, while it is true that all these advantages

contribute to satisfying requirements (1-6), the last one points to a significant drawback. The simple fact that dedicated servers operate at the same level as DTN servers makes it difficult to manage situational awareness and subsequent actions that require a global view of the system for decision making, such as maintenance or response for resilience. For instance, if situational awareness is implemented by allowing DTN servers to periodically share their contextual status with other DTN servers. so that they all collaboratively learn from their respective health status, the communication cost around the edge becomes significant. The bandwidth overload increases significantly, degrading migration tasks for mobility (requirement (5)). If, on the other hand, situational awareness is calculated from information stored in GRep and locally in each dedicated server, the processing time of tracing the repository and the complexity of the solution itself would severely penalize requirement (2). Therefore, the effect of both approaches is rather negative to meet the requirements of the framework.

In addition, although the edge promotes gradual maintenance for business continuity and the inclusion of servers by DTN improves the decoupling of functions, the duplication of servers carries an economic penalty and energy cost.

4.3 PL1-2 at the edge and PL3 in the cloud

Hybrid solutions bring together the advantages of the two previous architectures, ensuring consistent distribution of S&P solutions. Essential services can be deployed at the edge for local diagnostics (context awareness), and complex services are developed in the cloud for global diagnostics (situational awareness). In fact, this way of collaboratively deploying services at different levels reduces complexities (requirements (1-2)), benefits maintenance of the DTN system (requirement (3)), makes it possible to have a clearer view of the situation to react accordingly (requirement (4)), and favors the mobility and adaptation of DTs during the migration phase between DTNs at the edge (requirements (5-6)). But even so, cloud centrality remains a serious problem that leads to denial-of-service issues, affecting requirements (3-6). Therefore, server replication is still recommended, and more specifically for critical 6G-enabled IIoT scenarios.

5 Conclusions and future work

This paper proposes a protection framework to guide the deployment of 6G-enabled IIoT systems supported by DTNs to achieve the QoS expected in 6G networks and the objectives of Industry 5.0. The framework has been analyzed from different perspectives, considering the types of protection services to be

Table 1: S&P Services for the protection of DT-enabled 6G industrial networks

Assets		PL1		PL2		PL3	Prospective technologies
Devices	DTs	Hardening Integrity Local diagnosis Detection Alert and reporting	DTN servers	Security hardware Hardening and admin. AAA Local diagnosis Context awareness Detection Alert and reporting Response Certification Privacy and anonymity	dedicated server/s	Security hardware Hardening and admin. AAA Global/local diagnosis Situational awareness (Collaborative) detection Alert and reporting Risk management Policy management Response Restoration Auditing and traceability Certification Remote attestation Privacy and anonymity	Multi-agent systems (*) Consensus and correlat. (2,3) Quantum-safe crypto. (*) Artificial intelligence (*) Virtualiz./containerization (*) Digital twins (2,3) Federated learning (2,3)
Repository	-	-	LRep	Confidentiality Integrity Availability Local data sharing Privacy and anonymity	GRep	Confidentiality Integrity Availability Privacy and anonymity Global data sharing Cyber intelligence	Quantum-safe crypt (*) Blockchain (3) Multi-agent systems (*) Virtualiz./containerization (*)
Interfaces	DT-DT DT-device DT-LRep	Confidentiality Integrity Availability Authentication Key management Location privacy Trust management	DTN-DTN DTN-S&P DTN-GRep	Confidentiality Integrity Availability Authentication Key management Location privacy Trust management	S&P-DTN S&P-users	Confidentiality Integrity Availability Authentication Key management Location privacy Trust management	Quantum-safe crypto. (*) Artificial intelligence (*) Visualization tech. (3)

(sequence): states which layer it impacts (PL1, PL2, PL3 or all with *)

Table 2: Association of the requirements of the protection framework to PL1-3

PL	Uncoupling	Lightweight services	Maintainability	Usability	Mobility	Adaptability
PL1	+	+				
PL2	+	*	+	+	+	
PL3	+	*	+	+	+	+

+: positively affects
+: negatively affects
*: depends on the services implemented

Table 3: Association of the requirements of the protection framework to computing infrastructures

PL1-2	PL3	Uncoupling	Lightweight services	Maintainability	Usability	Mobility	Adaptability	G1	G2	G3
Cloud	Cloud	-	*	-	-	-		-	-	-
Edge	Edge	+	*	+	+	*	*	*	-	*
Edge	Cloud	+	+	*	*	*	*	+	+	*

+: positively affects
+: negatively affects
*: depends on the services or the situation

associated with each layer, and the type of computing infrastructures required to deploy security services.

From the analysis, we draw two relevant conclusions. First, we note from Tables 1 and 2 that layered protection favors G3 both locally (context-aware) and globally (situation-aware), and the requirements of the protection framework are fully met as one moves between PLs: in PL1 (requirements (1-3)), PL2 (1-5) and in PL3 (1-6). This is partly due not only to security solutions (e.g. hardening for decoupling) but also to prospective technologies (e.g. virtualization for decoupling, blockchain for mobility and adaptation). Second, we observe from Table 3 that the use of computing infrastructures is also critical to meet the requirements of the protection framework. In this case, hybrid solutions have proven to be the perfect candidate to cover the expected needs for 6G-enabled IIoT ecosystems under Industry 5.0. The level of decoupling, not only in terms of PLs but also in terms of infrastructure, is key to benefit security management by area/s but also to create end-user-centric protection solutions, further facilitating the maintenance of such solutions and the mobility of devices in the physical space.

As future work, we intend to demonstrate these findings from a practical point of view, focusing on the development of adaptive FL techniques for advanced detection systems supported by DTNs.

Acknowledgments

This work has been partially supported by SecTwin 5.0 (TED2021-129830B-I00) funded by the Ministry of Science and Innovation (Agencia Estatal de Investigación (AEI)/10.13039/501100011033) and by the the European Union "NextGenerationEU"/Plan de Recuperación, Transformación y Resiliencia; as well as by SecureEdge also funded by the Ministry of Science and Innovation (AEI/10.13039/501100011033/) under Grant PID2019-110565RB-I00.

References

[1] Z. Yin, T. H. Luan, N. Cheng, Y. Hui, and W. Wang, "Cybertwin-enabled 6G Space-air-ground Integrated Networks: Architecture, Open Issue, and Challenges," *arXiv preprint arXiv:2204.12153*, 2022.

[2] V.-L. Nguyen, P.-C., Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384-2428, 2021.

[3] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani and C. S. Hong, "Digital Twin of Wireless Systems: Overview, Taxonomy, Challenges, and Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2230-2254, Fourthquarter 2022.

[4] L. U. Khan, W. Saad, D. Niyato, Z. Han and C. S. Hong, "Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions," *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74-80, 2022.

[5] C. Alcaraz and J. Lopez, "Digital Twin: A Comprehensive Survey of Security Threats," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1475-1503, thirdquarter 2022.

[6] S. Shahzadi, M. Iqbal and N. R. Chaudhry, "6G Vision: Toward Future Collaborative Cognitive Communication (3C) Systems," *IEEE Communications Standards Magazine*, vol. 5, no. 2, pp. 60-67, 2021.

[7] W. Sun, S. Lei, L. Wang, Z. Liu and Y. Zhang, "Adaptive Federated Learning and Digital Twin for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5605-5614, 2021.

[8] Y. Lu, S. Maharjan and Y. Zhang, "Adaptive Edge Association for Wireless Digital Twin Networks in 6G," *IEEE Internet of Things Journal*, vol. 8, no. 22, pp. 16219-16230, 2021.

[9] M. Breque, L. De Nul, and A. Petridis, "Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry,", European Commission, 2021. [Online]. Available: https://data.europa.eu/doi/10.2777/308407.

[10] D. Je, J. Jung and S. Choi, "Toward 6G Security: Technology Trends, Threats, and Solutions," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 64-71, 2021.

[11] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor, Q. Wu, and M. Boucadair, "Digital Twin Network: Concepts and Reference Architecture," Internet Research Task Force, IETF, draft version, 2022. [Online]. Available: https://www.ietf.org/id/draft-irtf-nmrg-network-digital-twin-arch-01.html.

[12] G. Shao, "Use Case Scenarios for Digital Twin Implementation based on ISO 23247," National Institute of Standards and Technology Advanced Manufacturing Series 400-2, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.400-2.pdf.

[13] ISO, "Automation Systems and Integration - A Digital Twin manufacturing framework - Part 2: Reference architecture,", ISO/DIS 23247-2:2020(E), ISO TC 184/SC 4/WG 15, 2020. [Online]. Available: https://www.iso.org/standard/78743.html.

[14] C. Alcaraz and J. Lopez, "Wide-Area Situational Awareness for Critical Infrastructure Protection," *IEEE Computer*, vol. 46, no. 4, pp. 30-37, 2013.

[15] N. Kourtellis, K. Katevas, and D. Perino, "FLaaS: Federated Learning as a Service," *1st Workshop on Distributed Machine Learning*, DistributedML, New York, NY, USA: ACM, 2020, p 7–13.