J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", *IEEE Wireless Communications*, vol. 28, pp. 48-55, 2021.
http://doi.org/https://doi.org/10.1109/MWC.001.2000336
NICS Lab. Publications: https://www.nics.uma.es/publications

Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid

Javier Lopez, Juan E. Rubio, and Cristina Alcaraz*

January 28, 2022

Abstract

Beyond fifth-generation (B5G) communication networks and computation paradigms in the edge are expected to be integrated into power grids infrastructures over the next years. In this sense, AI technologies will play a fundamental role to efficiently manage dynamic information flows of future applications, which impacts the authorization policies applied in such a complex scenario. This article studies how Digital Twins can evolve their context-awareness capabilities and simulations technologies to anticipate faults or to detect cyber-security issues in real time, and update access control policies accordingly. Our study analyzes the evolution of monitoring platforms and architecture decentralization, including the application of machine learning and blockchain technologies in the Smart Grid, towards the goal of implementing autonomous and self-learning agents in the medium and long term. We conclude this study with future challenges on applying Digital Twins to B5G-based Smart Grid deployments.
Keywords: smart grid, 5G, edge computing, fog computing, intelligence, blockchain, digital twin, authorization.

Introduction

The smart grid (SG) came in the last decade to change the way electricity is consumed in homes and demand is managed in the utilities. As the digitialization of critical infrastructures continues, advancements in telecommunications do not stop either, and the industry is not unaware of this progress. New communication technologies such as 5G and innovative computing paradigms at the edge of the network are on the horizon. Together with them, other disruptive technologies such as the Internet of Things or the blockchain are already being integrated into various industrial sectors (including the Smart Grid), in what is already known as Industry 4.0.

Besides adding more complexity to the SG infrastructure, these technologies can solve several of the problems it faces currently. This ranges from increased

* *The authors are with the University of Malaga*

process automation to secure data handling at all levels, accompanied by almost instantaneous transmission and analysis. Only in this way can we understand future industrial scenarios where data ubiquity is achieved, as well as optimal interaction between all participants in the production chain.

However, these upgrades can only be adopted if a fine-grain control over the data is introduced, along with a continuous assessment of all assets in terms of cyber-security, in order to anticipate risks, generate evidence transparently and ensure the democratization of the available resources. This is attained by advanced authorization policies capable of adapting to lively environments with ever-changing technology and actors. For this mission, virtualization technology is the turning point for the simulation and visualization of changes in the infrastructure while also predicting consequences derived from potential actions, approaching the concept of Digital Twin (DT). This can be defined as a representation of a physical asset in virtual space, enabled by a synchronized data acquisition about its structure, functionality and behavior. By analyzing and simulating virtual states of such entity, it is possible to undertake real-time monitoring and predictions, optimize processes and improve decision making [1]. All in all, they emerge as a forthcoming solution to guide access control, by coordinating all security services within the SG network in a holistic and autonomous manner.

In this work, we carry out an introspection of the future SG architectures to accommodate the upcoming communication and computation technologies, by looking into the evolution of DTs for the ultimate goal of implementing intelligent authorization policies. More specifically, we provide a mid-term and long-term analysis and a concise study on the pending challenges of DTs concerning AI. These are consistent with recent industrial views that suggest that the landscape of DT evolution will fulfill a three-stage process: from mere monitoring systems with limited analysis capabilities nowadays, going through semantic platforms featuring prediction and optimisation over the next few years, until the future implementation of fully semantic, self-learning, socio-technical platforms [2].

The remainder of the article is organized as follows: to begin with, the enabling technologies for the upcoming power grids are highlighted. Then, we present the proposed SG architecture and the analysis of DT advancements in the medium and long term. Based upon this, the main challenges regarding AI and intelligent authorization policies are identified later. Finally, conclusions are drawn to conclude the article.

Enabling technologies

Due to the increasing complexity of power grids architectures, access control is essential to manage the permissions of all users, processes and heterogeneous devices involved. This obliges to continuously study the full range of requirements of this scenario, and redesign new ways to intelligently update authorization policies over time. In this section, we review the emerging technologies that

offer significant innovations to the Smart Grid in the medium and long term.

Beginning with the timeline of forthcoming communications technologies, beyond fifth-generation (B5G) networks emerge as the first solution to meet the performance demands and extreme capacity of nowadays applications. Following the principle of "*no latency, gigabit experience*", it will allow to instantaneously and reliably connect million of users in dense areas and trillions of IoT devices, thereby enabling the smart cities and autonomous cars, among other applications. As for industrial environments, 5G enables real-time business decisions driven by data, paving the way for cost savings and long-term growth. In the particular case of the Smart Grid, 5G networks can provide significant advancements to four application scenarios [3]:

- **Intelligent distributed peer-to-peer (P2P) automation:** nowadays, fault isolation and control procedures are conducted by centralized automation, which causes more traffic from the terminals to utilities and high latency. However, B5G enables effective P2P communication between terminals, aggregators and substations, to take the processing logic from primary sites to those distributed devices, in an autonomous way.

- **Millisecond-level load control:** this circumvents the issue of traditional distribution networks, which are not deployed with sufficient communication infrastructure to support precise load control. At this point, 5G offers ultra-low latency and high-reliability communications with high isolation from actual managements assets.

- **Low voltage information retrieval:** electricity usage data is periodically retrieved in intervals of 15 minutes. However, upcoming services impose a quasi-real-time reporting and the coverage of a greater number of terminals in the households and high-end premises. In this sense, B5G copes with such massive access to ensure a high-frequency transmission of data.

- **Distributed power supplies:** over the present and coming years, new types of micro-grids and distributed power supplies are being integrated at the user end, which now becomes user and generator of electricity. These introduce new challenges to deal with massive power and information flows in an efficient manner. Again, 5G emerges as a key technology to enable seamless communication with millions of accesses and low latency.

At present, the standardization bodies behind 5G, the International Telecommunications Union (ITU) and the European Telecommunication Standards Institute (ETSI), have already started its commercial deployment early in 2020. Long after that, 6G technologies, despite they are still in the design phase, are expected to roll out from the 2030s. This process firstly requires a deep effort to physically integrate new equipment into the radio access networks and then implement virtualization technologies that enable the programmability of B5G networks. It is the case of software defined networking (SDN) and network

functions virtualization (NFV), which permit to flexibly migrate components of the network core to the cloud, so that network resources are optimized for particular services.

As part of this offloading of functions to the cloud, mobile edge computing (MEC) appears to address further performance requirements by bringing the cloud closer to the edge of the network, and consequently to the users. For this reason, it is considered as a key technology towards B5G networks to drive demand for its services. It provides a highly distributed environment that can be used to integrate computing, storage and networking resources with the base station, thereby enabling compute and latency-sensitive services in proximity to mobile users. With this computation model, applications are split into small tasks that are executed at the local or regional clouds to achieve ultra-low latency and high bandwidth.

Smart Grid will also benefit from MEC technologies:

- Smart meters can send energy readings, trigger alarms or fire events that can be transmitted to the MEC nodes for data analytics and billing purposes;
- Measuring sensors and actuators from a local region can collect control information that is handled by MEC to perform fine-grain management of energy supply.

Despite the contributions of MEC, some challenges arise when distributing sub-tasks of one of these services across different edge computing nodes. The reason is that we need to coordinate individual edge service providers and allocate shared data between different domains, which is essential in applications with stringent requirements on mobility [4]. Therefore, MEC needs a versatile deployment that allows the optimal management of virtual resources while in operation. Fog computing can also be integrated and leveraged as an alternative in this matter, by orchestrating scalable services between devices that reside at the edge [5].

For the interest of authorization enforcement, the security of data at rest is likewise of paramount importance, as well as the accounting of every single action performed across all devices within the grid. Blockchain solutions barge in at this point to offer the synchronization of immutable but linkable information between all partners within a federated Smart Grid, vouching for the data ownership and provenance. This way, access registers can be securely analyzed by external auditors to submit potential policy updates to devices and components involved, favouring the creation of access control schemes governed by Smart Contracts [6]. Beyond authorization applications, blockchain can be applied to other scenarios, generally to conduct energy trading processes or to establish trusted networks for the operation of intelligent electric vehicles [7].

Altogether, these technologies set the dynamic and mutable application context, where it is fundamental to introduce access control mechanisms that are steadily supported by intelligent monitoring platforms and context-awareness solutions. These pave the way for the development of DTs in the future Smart

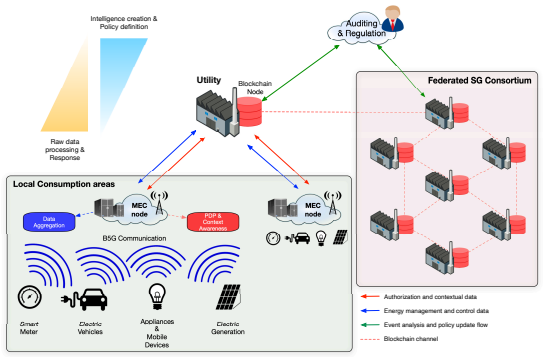


Figure 1: B5G-enabled Smart Grid architecture for accommodating DTs in the medium term

Grid. In the next sections, we take these constraints into account to analyze the evolution of these systems in a medium and long term.

Intelligent monitoring platforms for B5G-based Smart Grids in the medium term

According to the heterogeneity of not only technologies but also stakeholders involved in a SG (i.e., prosumers, governments, utilities, regulators), it becomes mandatory to apply hybrid access control mechanisms. They can be based on RBAC (role-based access control) or ABAC (attribute-based access control), that permit to define fine-grained policies that are easy to maintain. These must subsequently meet the real-time needs of all entities, respond in a timely manner and be subject to dynamic cyber-security rules.

As a consequence, the traditional authorization model in a SG scenario should be redesigned to comply with these requirements. The aforementioned model is commonly based on the introduction of policy enforcement points (PEPs), that emit requests to the policy decision points (PDPs), where they are assessed and access decisions are made depending upon the policy and permissions. Whereas the former points are allocated in households or substations near the consumption areas, the latter are endorsed by aggregators, utilities or data centers in a hierarchical fashion within the grid infrastructure, where analysis and management endpoints are placed. However, despite their location, all of them serve as policy information points (PIPs) to collect contextual information from resources and processes involved in any interaction, as to enrich the evaluation of access requests, conducted by PDPs. This is where context-awareness mechanisms and intelligent monitoring platforms come into play.

By introducing ubiquitous processes that permanently conduct context-aware ness analysis over the entire infrastructure, the authorization components can improve decision making and enhance the established policies [8]. More specif-

ically, these processes act as the PIPs that are assigned with different tasks: firstly, they retrieve contextual information from a layer of devices to be monitored, which includes low-level operational inputs (e.g., energy readings, pricing data), host-based or network-related information (e.g., protocol used, commands issued, bandwidth). Together with cyber-security analysis executed ad-hoc or leveraging external mechanisms (e.g., intrusion detection systems), this information helps to create a virtual representation of the assets in a certain region: a Digital Twin.

Consequently, DTs must be implemented and live in the vicinity of the devices, if not embedded to them, to achieve a total interoperability between virtual and actual assets, without delays. MEC nodes are a solution to introduce intermediate computational nodes, alongside with regular energy management procedures, near the consumption areas. In particular, these can transparently implement the PDP components in charge of autonomously apply authorization at a regional level, and the context-awareness processes described before. Both services are deployed on different edge applications that are coordinated by the respective utility, which ultimately behaves as a global PDP when exchanging data between different regional domains.

The new infrastructure would also allow the utilities to store aggregated transactions that belong to a local business network in the blockchain. Thus, there would be a distributed ledger across a set of peers involved in a SG consortium, which guarantees consistent updates to a chronologically sorted database. It can contain tamper-proof access and context-awareness registers from all participants using a consortium-based platform with an efficient consensus algorithm. This information is regularly accessed and validated by external auditors and regulators (e.g., federal comissions, energy market operators) to assess the policy enforcement and detect possible tamperings. As a result, they may also contribute to the new authorization life-cycle by proposing potential updates to the different utility PDPs.

The resulting B5G-enabled architecture appears depicted in Figure 1. The current network infrastructure may converge on this model in the coming years, taking into account the direction of the new communication and computing paradigms. However, this vision still has some drawbacks: on the one hand, there is still a dependence on centralized entities for the staggered governance of resources, which can lead to bottlenecks and latency problems. By the same token, non-federated environments could simply benefit from a domain-focused monitoring, without trusted and third-party auditing procedures based on Blockchain. For these reasons, there is no distributed intelligence that allows for autonomous and holistic decision-making, nor do DTs control the productive process. In this case, the use of AI is reduced to threat analysis in localized areas, and policy redesign is mostly a manual procedure in the hands of auditors. Consequently, these aspects are expected to be tackled with a highly decentralised architecture, where DTs play a key role in adapting authorisation to the dynamic environment instantly. This one is addressed in the next section.

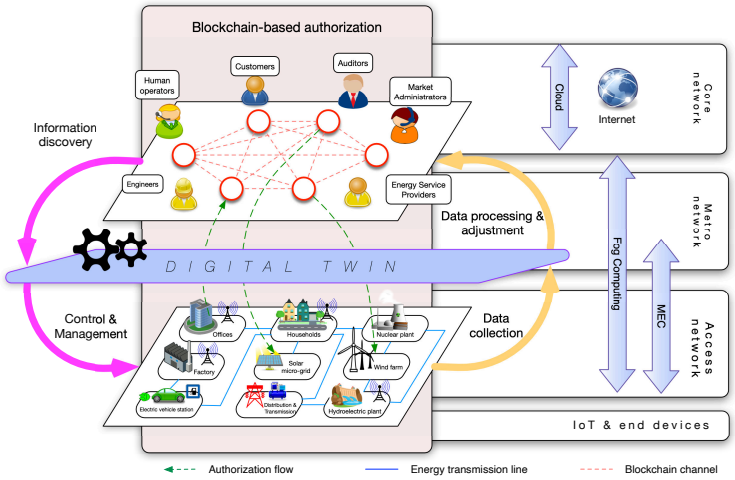


Figure 2: B5G-enabled Smart Grid architecture for accommodating DTs in the long term

Autonomous and reliant Digital Twins for long-term grid deployments

As the electric sector is embracing the digital age, the SG infrastructures are more influenced by value-added technologies to analyze data, carry out simulations and ultimately optimise the energy management systems. This evolution will lead to a full hybridization of grids at an international/regional level with local substation micro-grids and focusing on consumer empowerment, which demands a more resilient, reliable and efficient architecture. For this goal, while intelligent monitoring systems provide a first semantic representation of the grid assets, DTs are needed to convey a more holistic socio-technical and process-oriented characterisation of the environment by means of a total synchronicity of the cyber-physical bi-directional data flows.

In order to present the characterization of DTs in the upcoming SG model, we firstly present its architecture, shown in Figure 2. This hyper-connected and totally decentralized model assumes that the barrier between energy generation, transmission and distribution assets are blurred, and all processes coexist with micro-grids and EV infrastructures. Based on any application scenario, these resources are collaboratively used and the information is compartmentalized and securely accessed by the corresponding stakeholders, who have flexible control over the legislation, energy management and data acquisition. This is achieved with NFV- and SDN-based techniques, with little or no change to the physical infrastructure.

In a higher layer of abstraction over these physical devices, a blockchain-based authorization system handles the access to information and resource trading in communities, thereby avoiding the need for additional and coupled PDP

computation nodes. The provisioning of the DLT nodes can be done by stakeholders on-premises (e.g., micro-grid owners, resident operators, utility administrators) or leveraging blockchain-as-a-service (BaaS) providers, hence cutting costs and increasing the scalability of resources.

Transversely to the end devices and the blockchain infrastructure deployed over the future grid, the presence of DTs must be holistic to achieve a symbiosis between physical assets and their virtualized entities. This means the authorization and the energy management processes must be integrated around the DT agents to implement a fully distributed automation. This way, they play the proactive role of controlling resources over the grid, compared to the passive behavior (i.e., monitoring) presented earlier. This functionality is enabled by orchestrating MEC, fog and cloud services at multiple architecture layers, which enables sensing of the physical and to have full interaction with the blockchain and the production line. The functionality loop between both worlds is provided by the data that connects them, so that the DT agents act as transparent but operational proxies in this duality, as represented in Figure 2. It comprises four phases that are executed permanently in high-frequency intervals:

1. **Data collection:** energy usage data and control information is retrieved in the proximity of IoT and end devices, leveraging the B5G infrastructure to carry out context-awareness procedures.

2. **Data processing and adjustment:** as data is aggregated, further analysis and detection is performed, to subsequently store such information in the ledger and execute additional maintenance tasks to inform potentially affected stakeholders.

3. **Information discovery:** the DT subscribes to events on the blockchain that are related to its monitoring area (e.g., pricing information, demand response) in order to accelerate decision-making and anticipate potential security issues that may render changes in the access to resources.

4. **Control and management:** as aforementioned, the DT agents that are hierarchically spread over the SG infrastructure have full autonomy to manage its corresponding assets, without the need of a vertical and centralized control.

Aside from sensors information and control commands, authorization requests and responses pass through intermediate DT agents located in the edge, as depicted in Figure 2. These submit transactions to the ledger and relay the outputs back to the field devices using B5G communication, based on the existing policy and the cyber-security state assessed by the agents. Likewise, they can propose amendments to the access control scheme based on repetitive behaviors and past perceptions, as explained in the next section.

So far, we have presented the architectural side of the B5G-based Smart Grid for the future accommodation of DTs as the enabling factor of the distributed automation of processes. However, despite the emergent interest around this

concept, the research within this field is still immature: many simulation applications have been used and re-branded as DTs, while some others lack precision for tailored environments or cannot escalate to potential nation-wide agents [1]. Moreover, the core AI algorithms have a long road ahead until the completion of self-reliant and self-learning agents. In the following, we review these challenges and provide useful insights for future R&D milestones in this area.

Challenges and optimizations using AI technologies: Self-upda-table authorization policies

Numerous challenges remain to drive the sophistication of DTs and enable application scenarios where the AI will play the leading role [9]. Particularly, in the context of this article, we stress on challenges belonging to four categories: technology integration, modeling, usability, and security & safety. These are summarized in Table 1. We close this analysis by discussing the intelligent authorization policies.

Beginning with the commissioning of modern technologies, the main concerns revolve around the coordinated deployment of applications in the edge or fog to ensure data sharing between geographically dispersed environments (and incidentally avoid handover), and the need to speed up transaction processing in DLT structures to reduce the impact on the control performance. The latter depend on upcoming advancements such as the concept of lightning networks (i.e., an extra layer to process private transactions between parties in a P2P fashion) or sidechains (i.e., secondary blockchains to offload bulky processing from the main one), besides lightweight consensus algorithms. Another issue consists in the privacy of customer data, which has also been addressed by using blockchain approaches, including private channels between peers [10]. Also, as a consequence of the deep transition from legacy tools, this integration process must be supported by a gradual standardisation effort. Telecommunication bodies, industrial committees, government entities, e-mobility investors and cyber-security institutions are expected to join forces to the sustainable development and harmonisation of these technologies in society at an international level. In brief, Table 2 summarizes the advantages and constraints of every discussed technology in the scenario considered.

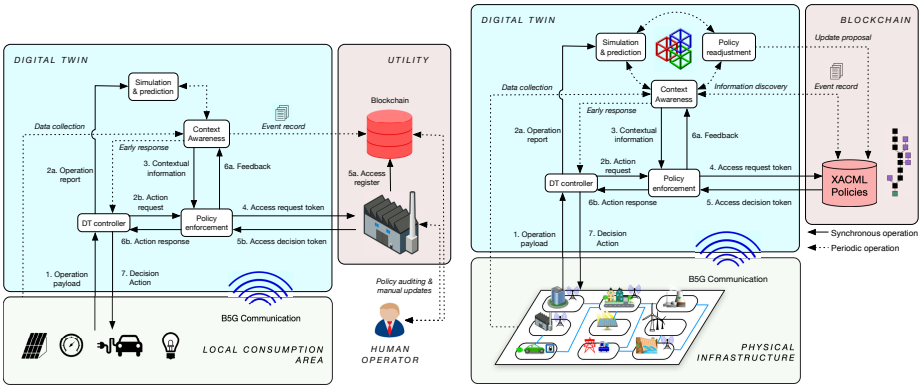
With respect to implementation, modeling DTs imposes several improvements over well established simulation procedures in the industry. Despite the many approaches investigated in other fields, the SG requires an increased degree of precision in its business logic, ranging from small measurement and control elements to buildings, aggregators and power plants at national levels. The main challenges to maintain synchronization between the physical resources and the DT representation are twofold. Firstly, the variety, volume and velocity of data to be processed online from multiple sources, in order to create an accurate model. Secondly, the maintenance of virtual models as the actual equipment evolves in time. Enabling technologies to address these issues include data com-

pression in B5G networks, hybrid techniques that combine physics-based modeling approaches (experimental and numerical), and data-driven approaches (by using readily available open resources), into reduced order models that can be efficiently handled at a greater computational speed [1]. In these environments, the use of open, cross-platform communication protocols (e.g., OPC UA) is crucial for the acquisition of observations from heterogeneous devices and hence estimate the state of the physical system given a predefined model (i.e., data assimilation). This process can be accomplished by means of Big Data analytics and Machine Learning solutions allocated in the cloud or fog (e.g., compressed sensing and symbolic regression).

As for usability requirements, the interaction of the twin with the physical infrastructure can imply autonomous decisions taken by the agent that must be interpretable by humans in a transparent way. This is ensured by means of explainable artificial intelligence, providing users with timely and actionable information to manage the SG resources efficiently, and complying with legal and regulatory requirements. A fast interaction with augmented reality (AR) and virtual reality (VR) is also key to support decision-making, which can be aided by enhanced probabilistic and predictive recommender systems. Besides top-notch human-machine interfaces, voice communication and web-apps are needed to provide the operators with holistic access and a detailed visualization of assets.

The solutions outlined above assume that information security and safety is guaranteed in all scenarios. This requirement is met by various conditions: firstly, that all grid operations are supervised by context-awareness agents in the proximity of the affected devices (e.g., by leveraging apps deployed in the edge). Various distributed detection techniques can evaluate the security state of resources and accurately trace persistent attacks throughout the infrastructure. One of the most promising approaches is Opinion Dynamics [11], a multi-agent algorithm that holistically correlates anomalies to report different alert indicators in real time. Secondly, the privacy of users and the security of data in transit and at rest. As mentioned above, this must be addressed by means of privacy-preserving techniques to collect and aggregate consumption information, coupled with cryptographic measures when this data is accessed and exchanged in the blockchain of a federated environment [10]. Thirdly, the grid is envisaged to effectively manage demand response to hold the power supply and anticipate high peaks to avoid potential blackouts. For this goal, the adoption of time series forecasting models or deep neural networks has been successful to forecast residential load demand [12].

Lastly, and returning to the starting point, the access control and authorization systems will acquire a greater influence from artificial intelligence in the new DT prototypes for the Smart Grid. The provisioning of traditional policy schemes in industrial sectors require an initial static procedure to analyse the regulations applied, engineer the roles involved, establish permissions and define rules for accessing resources or performing actions, considering precise constraints and relationships between assets. At the same time, these rules should be consistently declared to avoid conflicts, using an interoperable pol-



(a) (b)

Figure 3: DT authorization workflow: a) Medium term; b) Long term

icy language such as XACML. However, such mechanisms will have to face an unsteady environment where a huge set of actors fluctuate and the information flow is massive. In consequence, policies will have to be continuously assessed for the entire set of domains in order to readjust them in real time depending on a wide range of social, economic, and security conditions to guarantee the continuity of the network [13]. Additionally, although decentralised authorization systems are more flexible than centralized decision points in terms of efficiency, they are harder to manage.

Therefore, the administration of complex authorization systems is expected to progress towards more automated processes with scarce manual intervention. This fact is visible in our analysis of the transition from the medium to long-term DTs regarding the authorization workflow, as Figure 3 shows. Whereas the auditor has the last decision to manage the policies in the earlier approach, the latter does not need any human interaction. In this trend, we can classify the use of AI for intelligent authorization into two research lines:

- **Automatic policy alteration:** the aim is to gain insight from previous access requests and the overall behavior of the system, in order to refine existing rules. Data mining and classification algorithms are useful to identify discrepancies in policy specifications and infer new properties. Also, such evaluation can be combined with time-constrained delegation models and domain-specific rules to derive authorizations in unforeseen scenarios [14]. Altogether, they can help to automate conflict resolution and role assignment, as well as to support implicit authorizations (i.e., accesses that are not explicitly specified or granted) [15]. Simultaneously, the complexity of the explicit authorization set is reduced.

  The logic behind the analysis and improvement of security policies could ideally be implemented through smart contracts in the architecture proposed in the long-term analysis. This way, the DT agents distributed over

the architecture would be in charge of auditing the policy correctness, so that they would be able to submit transactions to propose upgrades to certain access control functions, which would be then approved by the consortium after being contrasted with other peer agents concerned.

- **Rule learning:** in this case, algorithms are trained to learn from data and infer policies rules from scratch. The most significant solutions here are about reinforcement learning. The traffic and events generated during the standard operation of the grid are studied to identify target resources and infer trust relationships between users and assets, based on the anomalies encountered [13]. Their counter-side is that the system is exposed to potential security threats, as the learning process takes place progressively while accesses are made and optimal policy rules are barely applied. As such, these solutions are more appropriate in later stages of the authorization life-cycle, when a base authorization model is enforced. Other alternatives to guide the reinforcement learning consists in probabilistic policy reuse, which balances among the application of the dynamically learnt policy, the exploration of random actions and the use of past policies.

Due to the differences between automatic alteration and rule learning, a dynamic authorization system that is collaboratively maintained and upgraded by a decentralized architecture of DTs must find a balance between these two approaches. Generally, the most common rationale will be to apply rule learning over a minimal set of policy regulations defined in the organization, to subsequently polish them with automatic alteration methods. Therefore, this process must be coupled with context awareness and auditing procedures to feedback the learning mechanisms and be fully integrated with the DT functionality loop of the previous section.

Conclusions and future challenges

In this article, we have carried out a prospective analysis of the future Smart Grid through the evolution of the Digital Twins, and we have pointed out the most relevant challenges they have to go through. Due to the aspirations of artificial intelligence and the role of recent computer and B5G communication technologies in this sector, these mechanisms are postulated as the guiding thread to drive the progress of the electricity grid towards a fully decentralised and autonomous model, governed by intelligent authorisation systems. Ahead lies an arduous path that involves various efforts in terms of standardization and information security, in conjunction with deep research into machine learning specifically applied to critical infrastructures and smart cities.

Acknowledgments

This work has been partially supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu), the EU H2020-MSCA-RISE-2017 Project No. 777996 (SealedGRID), and by a 2019 Leonardo Grant for Researchers and Cultural Creators of the BBVA Foundation. The second author has been partially financed by the Spanish Ministry of Education under the FPU program (FPU15/03213).

References

[1] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *IEEE Access*, vol. 8, pp. 21 980–22 012, 2020.

[2] C. Boje, A. Guerriero, S. Kubicki, and Y. Rezgui, "Towards a semantic construction digital twin: Directions for future research," *Automation in Construction*, vol. 114, p. 103179, 2020.

[3] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5g network-based internet of things for demand response in smart grid: A survey on application potential," *Applied Energy*, vol. 257, p. 113972, 2020.

[4] W. Hou, Y. Jiang, W. Lei, A. Xu, H. Wen, and S. Chen, "A p2p network based edge computing smart grid model for efficient resources coordination," *Peer-to-Peer Networking and Applications*, pp. 1–12, 2020.

[5] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. Rodrigues, "Fog computing for smart grid systems in the 5g environment: Challenges and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 47–53, 2019.

[6] C. Alcaraz, J. E. Rubio, and J. Lopez, "Blockchain-assisted access for federated smart grid domains: Coupling and features," *Journal of Parallel and Distributed Computing*, vol. 144, pp. 124–135, 06/2020 2020.

[7] K. Valtanen, J. Backman, and S. Yrjölä, "Blockchain-powered value creation in the 5g and smart grid use cases," *IEEE Access*, vol. 7, pp. 25 690–25 707, 2019.

[8] C. Choi, C. Esposito, H. Wang, Z. Liu, and J. Choi, "Intelligent power equipment management based on distributed context-aware inference in smart cities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 212–217, 2018.

[9] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications*, 2020.

[10] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[11] J. E. Rubio, R. Roman, C. Alcaraz, and Y. Zhang, "Tracking apts in industrial ecosystems: A proof of concept," *Journal of Computer Security*, vol. 27, pp. 521–546, 09/2019 2019.

[12] X. Xie, A. K. Parlikad, and R. S. Puri, "A neural ordinary differential equations based approach for demand forecasting within power grid digital twins," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–6.

[13] A. Outchakoucht, E. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *Int. J. Adv. Comput. Sci. Appl*, vol. 8, no. 7, pp. 417–424, 2017.

[14] R. A. Shaikh, K. Adi, and L. Logrippo, "A data classification method for inconsistency and incompleteness detection in access control policy sets," *International Journal of Information Security*, vol. 16, no. 1, pp. 91–113, 2017.

[15] L. Zhou, C. Su, Z. Li, Z. Liu, and G. P. Hancke, "Automatic fine-grained access control in scada by machine learning," *Future Generation Computer Systems*, vol. 93, pp. 548–559, 2019.

Category	Challenge	Enabling technologies and solutions
Technology integration and real-time performance	Coordination of edge-distributed DT agents	Multi-cloud application delivery using fog/cloud services, hand-over prediction
	Low transaction processing rate in blockchain	Lightweight consensus algorithms, lightning networks, sidechains
Modeling and physical/ virtual synchronization	Real-time modeling and data processing	Hybrid analysis and modeling, reduced order modeling, multivariate data-driven models
	Consistent and continuous model updates	Data assimilation, Big Data analytics, compressed sensing and symbolic regression
Usability	Transparency and interpretability	Hybrid analysis and modeling, explainable artificial intelligence, DLT accounting
	Interaction with physical asset	Aided decision-making with bayesian recommender systems, natural language processing, Enhanced human-machine interfaces (augmented reality and virtual reality), holistic web-based integration
Security and safety	Global intrusion detection	Distributed detection frameworks, Opinion Dynamics
	Data privacy	Cryptography and blockchain private channels, group signatures, zero-knowledge protocols
	Demand forecasting and fault prediction	time series forecasting models like ARIMA (autoregressive integrated moving average) or deep learning architectures such as deep neural networks (DNN), deep belief networks (DBN) and recurrent neural networks (RNN)
	Authorization policy readjustment	Automatic alteration (classification, time-contrained delegation models, implicit authorization) and rule learning (reinforcement learning, probabilistic policy reuse)

Table 1: AI-related challenges for the future Digital Twins in the Smart Grid

Technology	Medium term	Long term	Advantages	Drawbacks
B5G communication	✓	✓	Distributed and Intelligent P2P automation, ultra-low latency, high-frequency data retrieval	Slow international roll-out and integration in the industry
Mobile Edge Computing	∼	✓	Accelerated context-awareness services by means of computation offloading in the proximity to end users	Service allocation for multiple computing nodes, coordination of distributed DT agents
Fog computing	∼	✓	Orchestration of scalable services at a regional or national level, synchronization of physical/virtual entities across multiple domains, privacy control	Complex data management and maintenance
Cloud computing	✓	✓	Advanced data processing and policy readjustment, provisioning of Blockchain nodes	Privacy implications due to ineffective data governance, availability and high-latency issues
Blockchain	∼	✓	Tamper-proof database across between SG domains to store context-awareness and access registers, decentralized authorization schemes, P2P energy trading	Low transaction speed rates, computation overhead

✓ *technology in use;* ∼ *partially applied or with limited functionality*

Table 2: Advantages and constraints of the future DT enabling technologies in the Smart Grid