Cloud testing in smart grids - A literature review

Anonymous Unknown
Department of Informatics
University of Zurich
Zurich, Switzerland
unknown.anonymous@uzh.ch

***Index Terms*—Smart grid, IoT, Cloud testing, Cloud computing**

***Abstract*—The present document contains a review on the topic of common testing techniques that are applied in the domain of smart grid testing and what role cloud testing plays. Intelligent electrical supply systems are subject to an emerging field of research, especially the related risks of cyber security attacks as well as the challenges of processing high data volumes in real-time and of sustaining flawless interoperability within complex systems. The need of comprehensively testing such systems is obvious. This review collects and elaborates core statements on the current state of research about cloud-based testing IoT, particularly smart grid infrastructure, like communication networks or control systems.**

I. Introduction

In context of the energy transition and by being a substantial part of smart cities, evolving all around the globe, smart grids have gained increased focus in information technology and electrical engineering research during the last years. Smart grids complement traditional power grids with the application of communication and computational techniques [1] i.e. with the incorporation of communication networks, intelligent automation, advanced sensors, and information technologies ([2]). By automatically monitoring, controlling and steering the generation, delivery, and consumption of electricity, the performance of the power grid in terms of reliability, efficiency and resilience can be optimized significantly and costs on the customer side can be reduced. While smart grids open doors to unprecedented possibilities, like many other technological achievements, they have their downsides at the same time. Being part of the highly critical infrastructure of electricity supply, they are exceptionally exposed and vulnerable towards malicious attacks. Furthermore they face high-performance requirements in order to fulfill real-time data processing and seamlessly integrated components ensuring flawless interoperability of the system. Successful cyber attacks or misbehavior due to badly performing systems can cause huge damage to institutions and humans that depend on this infrastructure.

Reliable security and protection layers and perfect interoperability of software and hardware are inevitable to mitigate these risks. Such systems require a high amount of thorough testing, especially with focus on their vulnerabilities. However conventional testing technologies reach their limits when facing the combination of heterogeneous and co-existing smart grids. Smadi et al. stress fidelity to be one of the major factors limiting the effectiveness of existing testbeds because they do not implement sufficient interoperability, by simulating mainly the software and neglecting the physical system parts. Furthermore the physical and cyber layer lack of flexibility and are expensive to configure and finally the equipment is insufficiently diverse and heterogeneous, e.g. by assembling only devices from one vendor or supplier[2]. Elaborate test environments can be key to addressing the weaknesses of smart grids and cloud testing can make extended testing feasible by providing highly scalable test environments and resources. In general, testing should not be done on the real power system, because the deployment and usage of poductive software and hardware for testing purposes is far too expensive. Additionally, simulating disruptive actions like cyber attacks can damage a system considerably - another reason why the employment of testbeds and simulators that mimic productive environments and their components is highly recommended.

This present review study encompasses scientific papers containing research about how safety, interoperability and efficiency of IoT devices - especially smart meters -, and communication networks and data management systems in smart grids, can be tested and how cloud testing might contribute in solving some of the above mentioned problems.

II. Related Work

Many authors investigated on IoT cloud computing and emphasize its potential to improve efficiency and reduce costs in IoT because computing resources can be scaled and virtualized in a flexible manner. Laghari et al. in their *Review and State of Art of Internet of Things* point out the tight interconnection between cloud and IoT and they emphasize advantages that the intermingling of IoT and cloud have. Almolhis et al. attest the beneficial characteristics of cloud computing in IoT technologies in terms of on-demand self-service, resource pooling, broad network, measured service, and rapid elasticity. However, the large part of literature agrees repeatedly on criticalities of the cloud IoT, like security, data ownership, potential crashes and latency and Almolhis et al. recommend to put immediate attention in the research community especially on open security topics.

In the context of smart grids, the term *hybrid-cloud usage* appears frequently and seems to be clearly favoured over ”cloud-only” approaches for several reasons. Talaat et al. for example suggest to integrate data processing hardware devices to a private cloud to overcome security issues in the public

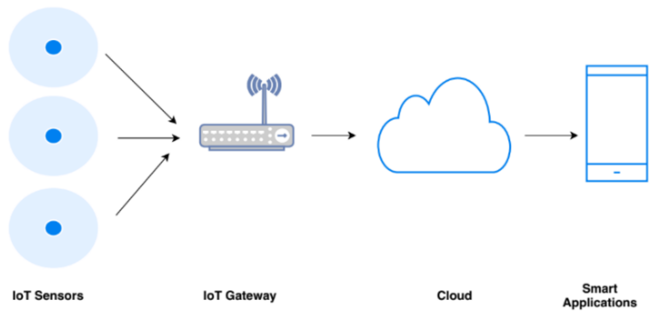

Fig. 1. Sample of IoT cloud application scenario by Almolhis et al.

cloud. Zahoor et al. recommend cloud-fog-based smart grid model for efficient resource management [5] and utilization [6]. They explain how the amount of transmitted data and data transmission time can be significantly reduced because the fog approach reduces the amounts of data transmitted to the cloud by performing decentralized data processing. It means that some of the processing units and storage is placed closer to where data is actually being sourced from. It can furthermore address security issues and certain regulations (e.g. in relation to data ownership).

Nastic et al. investigate in how IoT systems' governance can be improved in terms of uncertainty in the system infrastructure. Uncertainty can be caused by many reasons, e.g. probe failures, network issues or human error and puts a lot of burden on the developers and operation mangagers (users) when managing runtime governance in IoT cloud systems [7]. But it is a big challenge to include uncertainties in the development of proper governance strategies. Nastic et al. introduce the U-GovOps framework for *dynamic, on-demand governance of elastic IoT cloud systems under uncertainty*. It consists of a declarative policy language that basically allows the developers to model uncertainties for their governance strategies and mechanisms that support the execution of the strategies taking the modeled uncertainties into account.

Bornhöft et al. showed with a simulation model of a smart grid integration into an office building how much energy costs could be saved if the energy consumption was steered by taking a hypothetical dynamic price model into account. Depending on the current supply and demand of electricity, they reduced consumption or increased the amount energy stored in thermal energy storages. In their model, they could economize up to 31% of their usual energy costs by optimizing the energy consumption depending on the current price of electricity.

Zurich has a test area called *Greencity*, where the electricity utility of Zurich (ewz) maintains a pilot project in form of an integral energy infrastructure with intelligent power regulation mechanisms. Baumgartner et al. summarize findings about the *monitoring concept suitable for utilising flexibilities in the low-voltage distribution grid in Greencity*. Their main focus was to gain experience with cloud architecture in terms of processing data collected by sensors. In the case of *Greencity*, field data is streamed into a Microsoft Azure cloud computing environment for processing. They also seize on security and data protection issues in the context of using a cloud provider for hosting their services, but state that for their use case the Azure cloud architecture fulfils the information security requirements and for data protection they set up individual load profiles.

Testbeds represent a common experimentation platform where (prototypical) IoT devices or applications can be deployed and verified. According to Cintuglu and Mohammed, traditional testbeds tend to cover a limited project frame, while complex IoT systems, like smart grids, due to their interdisciplinary structure, require multiple heterogeneous test environments with different capabilities to interconnect in real-time. They therefore claim on more complete test platforms for comprehensive system testing and propose to include cloud communication for testbed implementation. They design a cloud-enabled architecture, where they outline the most relevant aspects how this can be achieved. Their proposal of a cloud enabled remote access smart grid testbed platform was implemented by the Energy Systems Research Laboratory, Florida International University.

III. Research Methodology

The research procedure consisted of three phases: review planning, conduction and reporting the results. This process was inspired by the recommendation of the guidelines in Kitchenham et. Al's *Procedures for Performing Systematic Reviews* [11]. Even though this is not a *systematic* review, the fundamental principle of the approach is still adequate and useful.

A. Review planning

The research question is about how cloud testing can be employed to test IoT systems like smart grids comprehensively. It gives an overview of the most important non-functional requirements, like cyber security, efficiency, reliability, and interoperability. It summarizes research findings about how cloud computing helps to solve but also aggravates some of these critical aspects.

To get a solid overview of the context, literature about vulnerabilities of smart grids and in general about risks posed in IoT development was examined. Smart grids are actually nothing else than a type of IoT ecosystem. They utilize sensors that collect data, streaming it on a central platform, which itself, processes and stores the data and implements APIs for devices and applications to enable interaction with the system.

Next, it was investigated, if and how cloud replicas can help preventing system lacks in one of the above mentioned risk aspects. The section IV provides an overview of findings and discusses core statements regarding chances and difficulties as well as existing or proposed solutions.

B. Review conduction

The search for the literature review included manual document retrieval from three popular web libraries: IEEE eXplore, Google Scholar, and ACM Digital Library. The documents have been retrieved by using a search term combined of the keywords *smart grid* or *iot*, *cloud*, and *testing* or *simulation*. The results were restricted to the years of publication from 2018 to 2023. The terms *smart grid* and *IoT* were treated as synonymous correspondants during the search and selection procedure, because it turned out that many findings for general IoT testing apply for smart grid testing. Equally, *testing* and *simulation* were treated according to the principle of synonymy. In the electrical engineering domain the term *simulation* seems to be widespread and some papers use it more often than the term *testing*.

From all documents retrieved by the search, those that met suitability criteria for the topic were selected in top down manner. Suitability was assessed in a two-step approach. Documents were directly selected, if they addressed all of the three above mentioned topics (*smart grid* or *iot*, *cloud*, *testing* or *simulation*) in their title or abstract. If they covered at least two in title or abstract, they were pre-selected and then scanned for occurrences of the third missing keyword. For example the content of a document, with the title *Cloud-Fog-based approach for Smart Grid monitoring* was scanned, if it also covered the term *testing* or *simulation* in the text.

Finally, manual backward snowballing iterations have been done on research papers that cited other papers in relation to cloud testing solutions for smart grids or IoT with publication date from 2018 to 2023.

C. Terminology

Bertolino et al. conducted a *systematic review on cloud testing* and they distinguish the term *cloud testing* by two meanings: *testing of the cloud (ToC)*, which refers to testing systems running in a cloud and *testing in the cloud (TiC)* which refers to leveraging cloud technologies for testing. They find that the cloud *offers the possibility to develop and maintain costly test infrastructures and to leverage on-demand scalable resources for configuration (by using cloud virtualization) and performance (by means of cloud elasticity) testing.* This literature review did not have a specific focus on one of the definitions. Both shapes of cloud testing were considered, as well as their intersection, which is called *testing of the cloud in the cloud (ToiC)* by Bertolino et al..

IV. Review Results

A. Cloud IoT and testing

It was in 2019, when Bertolino et al. concluded in their *systematic review on cloud testing* that the IoT domain could certainly benefit from the cloud potential, but that it had not yet done so in large measure. They found that IoT was mentioned in many studies, but when it came to the status of IoT *testing* in the cloud, numbers fell apart - at least compared with web or mobile testing. Despite of available studies and cloud testing tools and services like to CTaaS, a cloud-based TaaS (Testing as a Service) environment for example, that supports SaaS performance and scalability testing, only few of their respondents having IoT cloud products maintained a mature IoT testing environment. Half of them did not have a testing environment at all at that point [12].

In the past four years there has been progress in research as well as in industries employing IoT in regard to cloud testing. First of all, more and more cloud infrastructure is provided for IoT. Cloud computing offers expanded performance and scalability resp. elasticity. IoT devices benefit of this extraordinary deal of capacity to share information (Laghari et al.). Moreover, costs for resource consumption arise by degree of usage. However, Laghari et al. emphasize downsides of cloud computing in terms of IoT. Especially the data ownership and communication latency represent challenges. The latter is where fog computing (also known as edge computing) comes into play. Fog IoT instead of recording, processing or analysing data centrally, namely in the cloud, reorganizes the IT structure by locating some capabilities at the edge of the network - somewhere ”in the middle” between the data gathering hardware and the cloud. The minimized physical distance has a positive impact on latency reduction and the resolvement of bandwidth issues [13]. At the same time, fog IoT can improve safety and compliance [3] - it can contribute to the adherence to regulatory requirements e.g. in terms of restrictions towards the location of data stores. Fog IoT does not replace cloud IoT, the two complement each other.

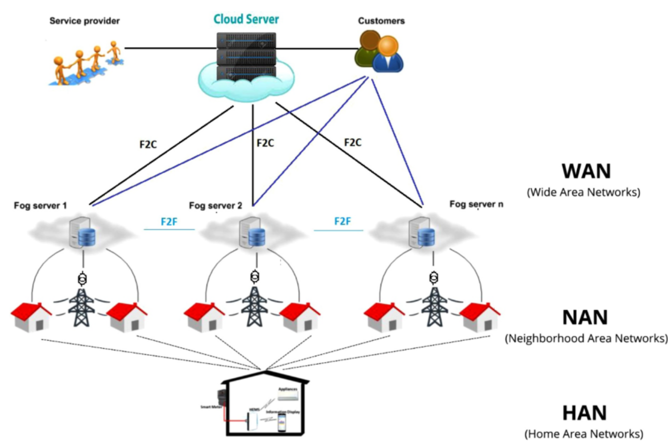

Fig. 2. Cloud-fog-based smart grid architecture by Forcan and Maksimović

IoT testing poses new challenges. Kim et al. sum up aptly: *”The amount of IoT devices and their collaborative behavior causes new challenges to the scalability of traditional software testing, and the heterogenity of IoT devices increases costs and the complexity of coordination of testing due to the number of variables.”* They introduce how IoT Testing as a Service (IoT TaaS) *”aims to resolve constraints regarding coordination, costs, and scalability issues of traditional software testing in the context of standards-based development of IoT devices”*. They design how a prospective IoT testing framework supports new requirements of IoT testing, like automatic test operation, flexible protocols, reduced costs, and better scalability and they present related work and research on various IoT test systems. Basically, they propose to rethink traditional interoperability and conformance testing approaches and semantic validation in IoT by putting the core testing logic into a so-called IoT-TaaS cloud.

B. Smart grid testing

The introduction of communication into a power grid exposes the system to various types of attacks [2] and multiplies its complexity. Due to the high criticality of smart grids, it is crucial to test robustness, safety and reliability of smart grid components upfront their integration into the real power grid. Happenings such as the cyber attack on the US power grid in 2009 or the attack on Ukraine's power grid in December 2015, resulting in large-scale blackouts [15], raised the awareness of the community towards the vulnerability of smart grid systems and the necessity of verifying the systems compliance towards these non-functional requirements in a systematic and thorough manner. However, mainly due to the complexity of smart grids, this is a very challenging and expensive task.

According to El Mrabet et al., security requirements of a smart grid encompass far more than only the resistance against "classical" cyber attacks, like eavesdropping, interception and tampering, or denial of service attacks, listed by Xue et al.. It is basically about any threat of confidentiality, availability, integrity - requirements defined by the US National Institute of Standards and Technology (NIST) - and about accountability [16] throughout the entire system. The successful adherence to these four key requirements is not only threatened by intended malicious attacks, but also by the heterogeneous nature of a smart grid itself. The communication between devices requires aggregation of data and translation between protocols which can enable accidental breaches and vulnerabilities, simply because a feature in one protocol could not be translated properly into another [16] for example.

Smart grids testing faces mostly the same difficulties like in general does IoT testing. Smart grids represent highly heterogenous soft- and hardware landscapes. Testing is either time-consuming and expensive or lacks reality. Smadi et al. mention that the complex nature of a smart grid structure requires the implementation of testbeds which include different capabilities for extensive experimental verifications and that so far most testbeds do not provide complete hardware and software platforms to test tightly coupled smart grids sufficiently. They suggest the usage of testbeds simulating power grids, where control, operation, and security algorithms can be explored, developed, evaluated, and validated. Instead of performing tests directly on the real physical system, the actual grid should be replicated e.g. with testbeds that allow to perform tests in an isolated environment. Smadi et al. differentiate between simulation- and physical-based testbeds. The first type is known to be economical because physical devices are simulated with software. The physical-based are more realistic thanks to the employment of real devices, but their extensive setup is far more costly.

C. Cloud test environment for smart grids

Cloud technologies are a substantial part in the rise of smart grids. IoT devices, like smart meters, compose a sensor network to collect physical world data, which is uploaded into commercial clouds, that provide flexible computational resources as utilities to build up the cloud based application systems [17]. According to Li et al., cloud computing helps

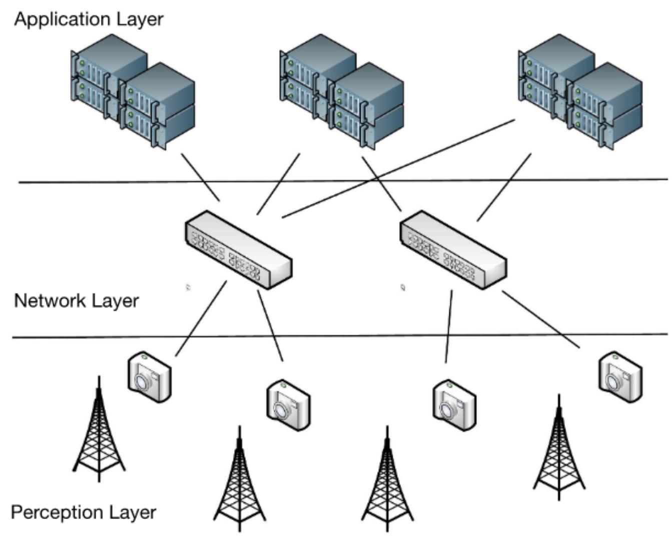

Fig. 3. Example of IoT-Cloud architecture by Li et al.. The application layer tends to be cloud-based.

to manage devices, that are widely spread among large space, more efficiently. Various sources indicate the great potential of cloud computing with regard to the feasibility of large-scale systems with variable resource needs. Rapid elasticity, ubiquitous network access, and highly-reliable services are some of the desirable features of cloud computing that are attractive for building cloud-assisted data-intensive smart grid applications [18].

Cloud testing in IoT as well as in smart grids usually refers to the intersection of ToC and TiC categories, i.e. *testing of the cloud in the cloud (ToiC)* [12].

Barbierato et al. have developed a framework that addresses some challenges of smart grid testing. Basically they present a *distributed framework for real-time management and co-simulation of demand response (DR) in smart grids*. It is meant to address especially the lack of reality, accuracy, efficiency and configurability in previous approaches and to improve the evaluation of interoperability of DR algorithms with multiple smart grid control and management strategies. DR is the automatical balancing of power supply and demand in smart grids and seeks to influence consumers e.g. by financial incentives, in order to distribute power consumption evenly through time i.e. to diminish consumptions peaks. While traditional power grids adjust the power supply depending on the demand, DR aims for adjusting the demand for power. Barbierato et al.'s simulation framework is equipped with some novelties, like a very realistic testbed, which allows to easily assess DR algorithms in a plug-and-play fashion, evaluation of interoperability of DR algorithms with other smart grid control and management strategies, very accurate and efficient simulation of the smart grid, or configurability of involved components.

Barbierato et al. highlight the importance of simulating power systems in order to assess DR service feasiblity in terms of network communication, data management, and the resulting smart grid behavior. They claim that none of the existing simulation frameworks is capable to perform simulation of DR policies, while integrating also real-time simulation.

The distributed simulation framework, that they propose, consists of a cloud-based advanced multimetering infrastructure (AMI), the energy aggregation platform (EAP) and the real-time simulator (RTS). The EAP leverages upon the AMI, called FLEXMETER, with one or more digital RTS [19]. FLEXMETER is an open source framework for measuring the change in energy consumption, driven by the EU Horizon 2020 Inititative. It provides EAP with necessary information to perform DR services. The FLEXMETER's technology integration layer, is made up of different technology integration adapters (TIA), that can deal with real or virtual IoT devices likewise. Like this, an easy switch from simulation environment to a real-world smart grid and vice-versa as well as bidirectional data exchange between real-world devices and RTS [19] are possible.

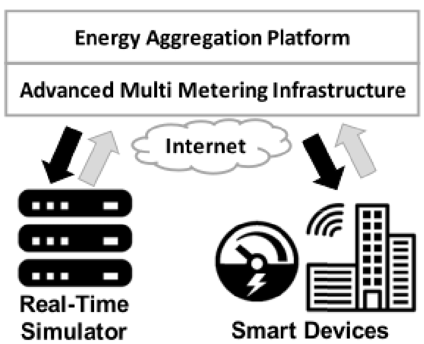

Fig. 4. Scheme of the proposed framework by Barbierato et al.

The authors stress that the entire framework for DR follows the modern software design patterns, to build distributed architecture that can be deployed on cloud systems. The FLEXMETER infrastructure is offered to stakeholders as platform as a service and the EAP as software as a service.

In view of the *ever large cyber attack surface caused by the exponential growth of the IoT*, Atalay and Angin recommend a more integral approach to perform smart grid security testing. Instead of only simulating parts of a system for testing purposes, they suggest the employment of a digital twin for continuous and comprehensive penetration testing. A digital twin is the virtual construction of a (physical) object or a system and can include multiple simulations, algorithms, and services. Once a digital twin is set up with real-world data, it can be used for execution of experiments, tests, or simulations. Atalay and Angin argue that digital twins offer the opportunity, firstly, to model cyber physical objects, whose behavior may not be captured with a purely simulation-based approach accurately and secondly, to run realistic attacks outside the real infrastructure. Running attacks on the actual grid itself, could cause major service disruptions or infrastructure damage [20]. The digital twins concept separates the system into three layers: The physical tier consists of mainly hardware or hardware-near components like storage, terminal, perception and networking resources. The virtual tier composes of libraries for models, environment states, and optimization parameters. Finally the decision-making tier with of algorithms mapping the physical tiers to the virtual tiers, optimizing monitored data, and raising alarms in case of anomalies. Atalay and Angin propose to employ a private cloud architecture for smart grids due to its strengths in terms of high availability, scalability and flexibility. For the edge-computing systems, they recommend the usage of *cloudlets* which represent small-scale wireless sensor networks. The main advantage of using *cloudlets* is the decentralized device management and that the data can be analysed in a manageable number of devices' own microecosystem.

Besides the big advantages of smart grids integrating the cloud, Demir et al. highlight the security risks smart grids are exposed to, due to the cloud's usage of the public network and shared resources. They propose a *hybrid hierarchical cloud-extension concept (HHCEC)*, with a 3-layer cloud-assisted architecture, that takes smart grid security requirements into account, with the implementation of *hybrid and geographically dispersed structure and a specialized broker-based publish-subscribe communication system*, a *strong proactive DDoS attack defence mechanism*, and a token-based authentication mechanism. For testing their prototype, they used (amongst other) *Amazon Elastic Compute Cloud (EC2)*. EC2, as part of Amazon.com's cloud-computing platform, rent virtual computers to users, so that they can run their own applications on them. Demir et al. used two EC2 micro instances, one that represents a broker server (first layer of HHCEC), and the second for running the smart grid application (third layer of HHCEC). They assessed the effectiveness of HHCEC in a large network by emulating the proof-of-concept in EC2. HHCEC and the way it was evaluated represent a good example of *Testing of the cloud in the cloud (ToiC)*.

V. Conclusion

Testing smart grids, and IoT in general, in the cloud is popular and the two things are tightly interconnected. Smart grid systems' complexity and heterogenity demand for services where traditional technologies reach their limits but the advantages of cloud technologies, like elasticity, costs per usage, efficiency, flexibility, or reduced maintenance effort arise. Cloud computing models, like *platform as a service* and *software as a service* facilitate the life of engineers or researchers by providing complete development and deployment platforms resp. by taking responsibility on a software's entire lifecycle.

In general there is consensus that smart grid testing is crucial in view of the criticality and vulnerability of electricity supply systems, but also that testing smart grids, especially from an end-to-end perspective is still a big challenge. Three concrete examples of how systems or system components can

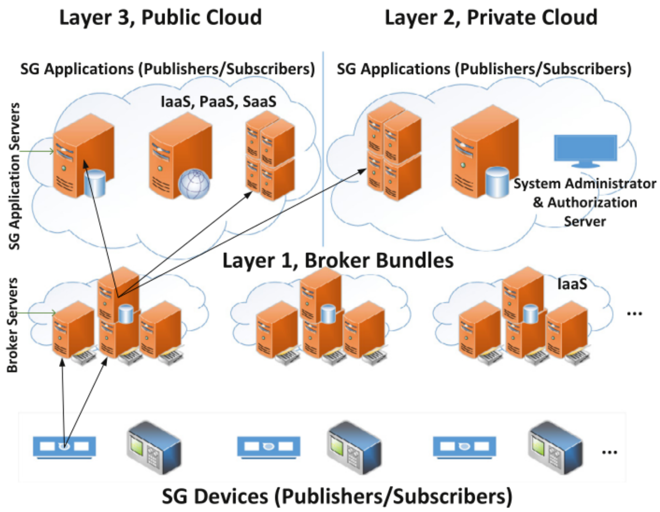

Fig. 5. Hybrid hierarchical cloud concept (HHCEC) by Demir et al.

be replicated for testing purposes have be presented. They build up on (co-)simulations, testbeds, or a digital twin. At the core, all of them head towards the same goal and face similar obstacles. They attempt to provide an as holistic and flexible test environment as possible by keeping computational and economical costs and maintenance effort within an acceptable limit.

References

[1] M. Talaat, A. S. Alsayyari, A. Alblawi, and A. Hatata, "Hybrid-cloud-based data processing for power system monitoring in smart grids," *Sustainable Cities and Society*, vol. 55, p. 102049, 2020.

[2] A. A. Smadi, B. T. Ajao, B. K. Johnson, H. Lei, Y. Chakhchoukh, and Q. Abu Al-Haija, "A comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges," *Electronics*, vol. 10, no. 9, p. 1043, 2021.

[3] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, "A review and state of art of internet of things (IoT)," *Archives of Computational Methods in Engineering*, pp. 1–19, 2021.

[4] N. Almolhis, A. M. Alashjaee, S. Duraibi, F. Alqahtani, and A. N. Moussa, "The security issues in IoT-cloud: a review," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE, 2020, pp. 191–196.

[5] S. Zahoor, S. Javaid, N. Javaid, M. Ashraf, F. Ishmanov, and M. K. Afzal, "Cloud–fog–based smart grid model for efficient resource management," *Sustainability*, vol. 10, no. 6, p. 2079, 2018.

[6] S. Zahoor, N. Javaid, A. Khan, B. Ruqia, F. J. Muhammad, and M. Zahid, "A cloud-fog-based smart grid model for efficient resource utilization," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 1154–1160.

[7] S. Nastic, G. Copil, H.-L. Truong, and S. Dustdar, "Governing elastic iot cloud systems under uncertainty," in *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, 2015, pp. 131–138.

[8] N. Bornhöft, L. Hilty, and S. Rasathurai, "Simulation der Smart Grid Integration eines modernen Bürogebäudes am Beispiel von IBM-Schweiz," in *IT-gestütztes Ressourcen- und Energiemanagement: Konferenzband zu den 5. BUIS-Tagen*. Springer, 2013, pp. 59–68.

[9] L. Baumgartner, T. Feizi, D. Mountouri, C. Köhler, and M. von Euw, "Monitoring concept suitable for utilising flexibilities in the low-voltage distribution grid: Learning from implementation in Greencity Zurich," in *CIRED 2020 Berlin Workshop (CIRED 2020)*, vol. 2020. IET, 2020, pp. 521–524.

[10] M. H. Cintuglu and O. A. Mohammed, "Cloud communication for remote access smart grid testbeds," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[11] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele University*, vol. 33, no. 2004, pp. 1–26, 2004.

[12] A. Bertolino, G. D. Angelis, M. Gallego, B. García, F. Gortázar, F. Lonetti, and E. Marchetti, "A systematic review on cloud testing," *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, pp. 1–42, 2019.

[13] M. Forcan and M. Maksimović, "Cloud-fog-based approach for smart grid monitoring," *Simulation Modelling Practice and Theory*, vol. 101, p. 101988, 2020.

[14] H. Kim, A. Ahmad, J. Hwang, H. Baqa, F. Le Gall, M. A. R. Ortega, and J. Song, "IoT-TaaS: Towards a prospective IoT testing framework," *IEEE Access*, vol. 6, pp. 15 480–15 493, 2018.

[15] Y. Xue, J. Wang, Y. Ding, and H. Zhang, "Research on security testing and simulation platform of smart grid substation system," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2019, pp. 510–515.

[16] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[17] W. Li, K. Liao, Q. He, and Y. Xia, "Performance-aware cost-effective resource provisioning for future grid IoT-cloud system," *Journal of Energy Engineering*, vol. 145, no. 5, p. 04019016, 2019.

[18] K. Demir, H. Ismail, T. Vateva-Gurova, and N. Suri, "Securing the cloud-assisted smart grid," *International Journal of Critical Infrastructure Protection*, vol. 23, pp. 100–111, 2018.

[19] L. Barbierato, A. Estebsari, E. Pons, M. Pau, F. Salassa,

M. Ghirardi, and E. Patti, “A distributed iot infrastructure to test and deploy real-time demand response in smart grids,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 1136–1146, 2019.

[20] M. Atalay and P. Angin, “A digital twins approach to smart grid security testing and standardization,” in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*. IEEE, 2020, pp. 435–440.

[21] I. Behnke, L. Thamsen, and O. Kao, “Héctor: A framework for testing iot applications across heterogeneous edge and cloud testbeds,” in *Proceedings of the 12th IEEE/ACM international conference on utility and cloud computing companion*, 2019, pp. 15–20.