How smart grid testing can benefit from cloud testing - A literature review

Wildermuth Salome
Department of Informatics
University of Zurich
Zurich, Switzerland
salome.wildermuth@uzh.ch

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

***Abstract*—The present document contains a review on the topic of cloud testing approaches that have been applied in the domain of smart grid testing so far. Intelligent electrical supply systems are subject to an emerging field of research, especially the related risks of cyber security attacks and the challenge of processing high data volumes in real-time. The review encompasses scientific papers from 2018 - 2023 about cloud-based testing of IoT devices, like smart meters, and metering infrastructure, like communication networks or data management systems. (https://www.blackridgeresearch.com/blog/what-is-a-smart-grid-what-are-the-major-smart-grid-technologies))**

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 are electrical grids that complement traditional power grids with automated, i.e. digital / software-based monitoring, controlling and steering mechanisms of electrical flaws and electricity consumption. The performance and efficiency of the power grid are enhanced with the incorporation of communication networks, intelligent automation, advanced sensors, and information technologies (Smadi et al.). 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. 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, simulated cyber-attacks can damage a system considerably - another reason why the employment of testbeds that mimic productive environments is highly recommended.

This present review study encompasses scientific papers containing research about how safety, interoperability and efficiency of IoT devices - especially software for 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

So far no literature review covering cloud testing techniques in smart grid industry have been found. However research has been done on the topic itself. Quite extensive research about how to test IoT in general with regard to cyber security, performance and interoperability has been done, as well as proposals on how cloud computing could support the implementation of extensive test environments is available. There is also literature about challenges of testing smart grids and how they might be solved. The focus lies mainly on the verification of smart grids' cyber and physical security and the interoperatiblity of the systems components.

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* [2]. 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 support testing of software in smart grids in terms of the non-functional requirements of cyber security and performance. Firstly, to get a solid overview of the context, literature about vulnerabilities of smart grids and in general about new 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.

Furthermore it was examined if and how cloud testing, cloud testbeds or co-simulations come into play to address the challenges. Recurring statements, difficulties and solution proposals were collected from research papers and evaluated. The section IV provides an overview of findings and discusses the most relevant aspects.

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 the search term *[smart grid / IoT] cloud [[security / performance / -] testing / simulation]* and 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 aspects that apply for general IoT software testing in literature can be applied smart grids as well. The search terms *testing* and *simulation* applied according to the same principle. Especially in the electrical engineering domain the term *simulation* is widespread and some papers use it more often than the term *testing*.

From all documents retrieved by the search, XX were selected based on suitability criteria for the topic in top down manner. Suitability was assessed in a two-step approach. Documents were pre-selected, if they addressed at least two topics of the following: smart grid or IoT, testing, cloud computing. If they covered all of them, they were directly selected. All the pre-selected documents were 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 (software) testing somewehere. Finally, manual backward snowballing iterations have been done on the five most relevant papers, which added another XX papers to the existing review collection. The five most relevant papers were selected based on how extensively they discuss the topic of testing cloud solutions for smart grids.

IV. Review Results

A. IoT cloud testing

In 2019, 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.

In the past three 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. 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 IoT comes into play. Fog IoT instead of locating data recording, processing and storage in one place, namely in the cloud, reorganizes the IT structure by placing the capabilities of the cloud somewhere ”in the middle” between the data gathering hardware and the cloud. At the same time Fog IoT can also be used to ensure safety and compliance (Laghari et al.). Fog IoT does not replace cloud IoT, it is more of a complement, addressing the issues with efficiency loss and data ownership of cloud IoT.

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 heterogeneity 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.

(ev. Bild (vereinfacht) aus IoT-TaaS: Towards a Prospective IoT Testing Framework, S. 15490)

B. Testing of smart grids

Smart grids testing shares common challenges with general IoT testing. Smart grids are highly heterogenous soft- and hardware landscapes. Smadi et al. point out that the complex nature of smart grid structure requires the implementation of testbeds including different capabilities for extensive experimental verifications and that so far most testbeds do not provide complete hardware and software platforms to test for all research applications simultaneously. Furthermore they suggest the usage of testbeds simulating power grids where control, operation, and security algorithms can be explored, developed, evaluated, and validated. With testbeds, instead of working directly on the real physical system, a model of an actual power grid can be used. Especially cyber-attacks should not be done on live power systems due to their potential negative impact and in generalt because the deployment and usage of real system hardware and software for testing purposes is very expensive.

C. Cloud test environment simulation

It turns out that the robustness, safety and reliability of a smart grid should be tested upfront in various manners. There is the safety and performance requirement on one hand towards the software of a single device in the grid and on the other hand towards the interplay of many component - in the end the entire smart grid.

D. Google Scholar

Number of papers: 156 +
Selected papers:

- Cloud-Fog-based approach for Smart Grid monitoring
- A Digital Twins Approach to Smart Grid Security Testing and Standardization
- Internet of things and cloud computing-based energy management system for demand side management in smart grid
- A Resilient Architecture for the Smart Grid
- A Distributed IoT Infrastructure to Test and Deploy Real-Time Demand Response in Smart Grids
- Certificateless public key encryption with conjunctive keyword search and its application to cloud-based reliable smart grid system
- The Design of a Novel Smart Home Control System using Smart Grid Based on Edge and Cloud Computing
- Securing the cloud-assisted smart grid
- Smart Grid: a demanding use case for 5G technologies
- Cyber-security in smart grid: Survey and challenges
- Hybrid-cloud-based data processing for power system monitoring in smart grids
- Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies
- A Big Data platform for smart meter data analytics
- Hybrid-cloud-based data processing for power system monitoring in smart grids
- Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies

E. IEEE eXplore

Number of papers:
Selected papers:

- Research on Security Testing and Simulation Platform of Smart Grid Substation System
- Design and Implementation of Test System for Power 5G Communication Module Base on Cloud Computing Architecture
- Research on Security Testing and Simulation Platform of Smart Grid Substation System
- Analysis of Digital Utility Endpoints in Smart Grid using Modular Computing Platform
- Monitoring concept suitable for utilising flexibilities in the low-voltage distribution grid: Learning from implementation in Greencity Zurich
- Fog Computing for Smart Grid Systems in the 5G Environment: Challenges and Solutions
- Deployment and Performance Verification of 5G Smart Grid Based on LoRa
- Data storage in smart grid systems
- Smart Grid Co-Simulation Tools: Review and Cybersecurity Case Study
- Cloud communication for remote access smart grid testbeds (2016)

F. ACM Digital Library

Number of papers:
Selected papers:

- Hctor: A Framework for Testing IoT Applications Across Heterogeneous Edge and Cloud Testbeds (iot)
- Testing uncertainty of cyber-physical systems in IoT cloud infrastructures: combining model-driven engineering and elastic execution (iot)
- Modeling and Provisioning IoT Cloud Systems for Testing Uncertainties (iot)
- Test patterns for IoT (iot)
- On the simulation of smart grid environments (no cloud)
- Combining Simulation and Emulation Systems for Smart Grid Planning and Evaluation (no cloud)
- Resource Orchestration of Cloud-Edgebased Smart Grid Fault Detection

V. Conclusion

We conclude that blablabla...

References

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.