A literature review on how smart grid penetration and performance testing can benefit from SOTA cloud testing approaches

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 emphasizes scientific papers from 2018 - 2023 about penetration and performance testing of cloud-based 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 communities during the last years. Smart grids are electrical grids that replace or complement manual by automated, i.e. digital / software-based monitoring, controlling and steering mechanisms of electrical flaws and electricity consumption mainly for optimization purposes. 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. Successful cyber attacks or misbehavior due to badly performing systems can cause huge damage to institutions and humans that depend on this infrastructure.

Appropriate security and protection mechanisms and well designed software and hardware are inevitable to mitigate these risks. Such systems require a high amount of thorough testing, especially with high focus to their vulnerabilities. Penetration and performance testing can be key to addressing the two main weaknesses of smart grids and cloud testing can make extended testing feasible by providing highly scalable test environments and resources.

This present review study emphasizes scientific papers containing research about penetration and performance testing of IoT devices - especially software for smart meters -, communication networks and data management systems, in the cloud.

II. Related Work

So far no literature review covering cloud testing techniques for IoT devices in smart grid industry have been found. However research has been done on the topic itself. Research about how to test IoT devices generally with regard to cyber security and performance aspects has been done, as well as proposals on how such tests could be executed on the cloud. Furthermore there is a bunch of literature about how software components of smart grids can be tested and which frameworks and tools are available. Finally there are also some papers, investigating how cloud-based testing might help improving smart grids' resistance to the mentioned risks / vulnerabilities. From all these papers the content that refers to smart grids testing in the cloud has been extracted and will be presented in this work.

Test reference: [1]

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 vulnerarbilities of smart grids and in general about risks in IoT development was examined. Furthermore it was examined if and how cloud testing and cloud testbeds come into play to address these aspects. Not all of this literature was also considered for the actual review.

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 [[penetration / performance / -] testing / co-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 some aspects were for general IoT software testing in literature but might suit well for smart grid devices, even if this was not explicitely mentioned / intended? by the authors.

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, 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. 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

B. 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

C. 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...
Testreference: [3]

References

[1] 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.

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

[3] 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, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/9/1043