Testbed-Driven Assessment: Experimental Validation of System Security and Reliability

Daniel Chen, Cuong Pham, Zbigniew Kalbarczyk, and Ravishankar Iyer

GOALS

- Overall Goal: Develop tools and methods that can experimentally evaluate the reliability and security of cloud infrastructure and cloud-based smart grid applications on an ongoing basis.
- Stage 1: Design and build a distributed fault injection framework to support creation of realistic failures in a distributed cloud environment.
- Stage 2: Develop procedures to systematically explore failure scenarios in a cloud system.
- Stage 3: Integrate the fault injection framework and evaluation procedure into a cloud-based fault injection service for ongoing reliability and security evaluation and benchmarking of cloud-based smart grid solutions.

FUNDAMENTAL QUESTIONS/CHALLENGES

- How to ensure the reliability and security of cloud-based smart grid solutions on an ongoing basis.
- The fundamental questions and challenges of each stage of the project include:
- Stage 1: Building a fault injection framework.
  - What fault injection capabilities are needed to create realistic and representative cloud failures?
  - How should we design a fault injection framework that is distributed, scalable, and minimally intrusive to the system?
  - What capability is needed to create planned failures while maintaining control over the system (e.g., when injecting network failures)?
- Stage 2: Systematic exploration of failure scenarios.
  - How should we systematically explore the failure scenarios of a cloud computing platform?
  - How should we address the problem of exponential explosion of failure scenarios to achieve high evaluation coverage within reasonable time and cost?
- Stage 3: Create a failure injection service.
  - How do we ensure the safety of the live system when running a failure drill?
  - How do we properly specify each failure drill scenario and track its progress?
  - What is the performance impact and monetary cost for conducting a failure drill, and how often should it be conducted?
  - What safety mechanism is needed if planned failures are not handled as expected?

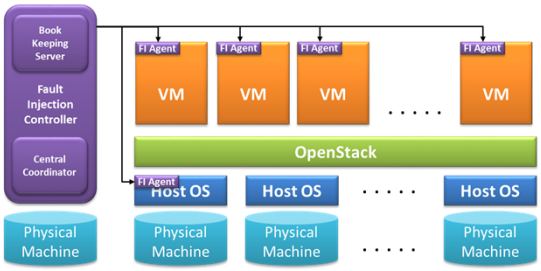
RESEARCH PLAN

- Stage 1:
  - Set up a cloud testbed for experimental evaluation of cloud-based smart grid solutions.
  - Design and implement a scalable and distributed fault injection framework.
  - Study past cloud failures to understand the common failure modes and what fault injection capabilities are needed to create realistic cloud failures.
- Stage 2:
  - Develop a systematic approach to explore failure scenarios in a cloud system and methods to reduce the fault space to a reasonable size.
  - Integrate the cloud testbed with the TCIPG testbed to simulate a realistic power system operating environment.
  - Set up real smart grid applications on the cloud testbed to evaluate our proposed fault injection approach.
- Stage 3:
  - Study how cyber asset failures might affect a physical power grid.
  - Demonstrate the feasibility of failure as a service on the testbed.
  - Set up a failure knowledge base to collect failure data for future failure analysis.

RESEARCH RESULTS

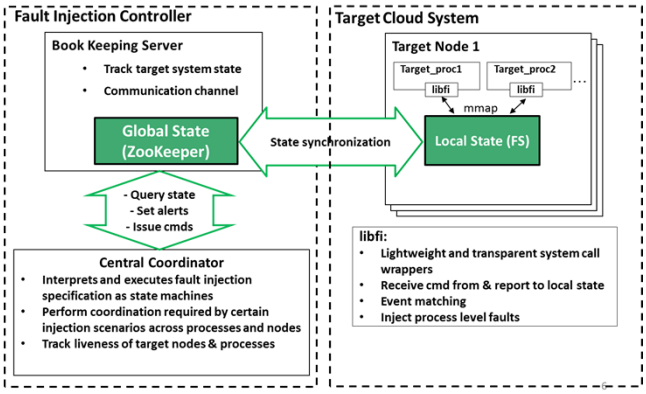
- An eight-machine cloud testbed has been set up to support experimental evaluation of smart grid applications in a cloud environment.
- OpenStack is being used as the scalable cloud management software that manages the provisioning of image, storage, and computation resources.
- NFTAPE, our previously developed fault injection framework for single hosts, has been re-implemented to support fault injection experiments in distributed and virtualized cloud environments.

Cloud Testbed with Distributed Fault Injection Framework



- The fault injection framework provides a powerful and flexible specification language to express how to track the cloud operating state in order to trigger and inject faults based on the state of the cloud (e.g., when a certain percentage of the resource is used).
- The fault injection framework architecture ensures minimum intrusiveness with efficient mechanisms to collect local state of each target node to form the global state of the cloud environment.

Fault Injection Framework Architecture



BROADER IMPACT

- In industry, most failure evaluation is done in scaled-down testbeds; not many production cloud systems do live failure drills to test and verify fault tolerance capabilities. We hope that through this research we can demonstrate the feasibility of failure as a service and start addressing the issues that prevent broad adoption of this approach.

INTERACTION WITH OTHER PROJECTS

- Potential collaboration with Cornell University to explore the possibility of using GridCloud as the example cloud-based high-assurance power grid middleware when evaluating our failure injection framework.

FUTURE EFFORTS

We are close to finishing Stage 1 of the project. The immediate next steps are:

- Finish implementing the fault injection framework for automated failure creation in cloud infrastructure.
- Find a suitable cloud-based smart grid application as an example workload for evaluation.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T