U.S. DEPARTMENT OF ENERGY

PNNL-21724

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry

BA Akyol

September 2012

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry

BA Akyol

September 2012

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Acronyms and Abbreviations

AMI	advanced metering infrastructure
IP	internet protocol
IPSEC	internet protocol security
JSON	JavaScript Object Notation
NIST	National Institute of Standards & Technology
PII	personally identifiable information
PKI	public key infrastructure
PMU	phasor measurement unit
SaaS	software as a service
SCADA	supervisory control and data acquisition
VPN	virtual private network

Contents

Tables

1.0 Introduction and Document Scope

This document presents a summary of cyber security challenges associated with utilization of cloud computing in the electric utility industry. The reader is assumed to have familiarity with both the operational processes of the utility industry and cloud computing, including public (e.g., Amazon EC2, Microsoft Azure) or private clouds. We also assume that the reader is familiar with basic networking and web infrastructure constructs. Further, we recommend that the reader reviews the information presented in (Birman 2011; NIST 2012).

2.0 Cloud Computing Roadmap for the Electric Utility Industry

The most significant challenge in utilizing cloud computing in the electric utility industry is the uncertainty associated with relinquishing "control" from a utility-owned infrastructure to an infrastructure that exists outside the physical and electronic security perimeter of the utility. It is this challenge that will dictate the roadmap that the utilities will use to transition from their existing practices to a computing paradigm that includes cloud computing. The transition will likely follow these steps:

- **Now to 5 years in the future:** In this timeline, especially with the advances made in smart metering and dynamic demand-response, utilities will transition their back-office and billing systems including their customer portals to software-as-a-service (SaaS) providers. While some larger utilities serving millions of customers may afford to provide these services in-house, small to medium utilities including rural co-ops and municipals will be the ones that will embrace and lead this transition to the cloud due to lack of resources and expertise. Note that in some cases, this transition has already happened as part of the 2009 American Recovery and Reinvestment Act funded Smart Grid Investment Grant program, where all participants in this program were *required* to file and implement a cyber security plan. We also note here that there are utilities using outsourced equipment and network and cyber security monitoring services that exist outside their electronic security perimeters.

- **5 to 10 years in the future:** During this timeline, we expect non-real-time processes in utilities to take advantage of cloud computing. The processes that will migrate to cloud computing platforms will include short- and long-term planning, wide-area information sharing, energy market operations, and asset monitoring for maintenance. The capabilities provided by SaaS providers for planning and forecasting will level the playing field between large and small utilities. In order to perform effectively, the data that will be exported to the cloud will include power and communication system topology; operational data including supervisory control and data acquisition (SCADA) and phasor measurement unit (PMU) outputs; and bulk and distributed generation information. Note that most of this information for the bulk power system is considered "Critical Infrastructure Information" and must be protected at least at the Official Use Only level. The forecasting and planning functions that are now associated with a balancing authority may also be performed in a cloud computing facility. For monitoring of equipment for maintenance reasons, performance parameters such as gas and humidity in transformer oil, top and bottom oil temperature, and cooler efficiency are collected and analyzed in the cloud.

- **5 to 25 years in the future:** The last utility function that may be transferred (and it is questionable whether this will actually happen) is real-time control and status monitoring. Although some utilities are experimenting with management of demand-response in the cloud today, we believe that there are many challenges that need to be addressed before real-time control functions will be performed by resources provided by cloud computing facilities as we will discuss in Section 3. Status monitoring such as transformer, breaker, and relay monitoring may evolve such that the devices being monitored communicate with a cloud and the operators at the utility monitor the equipment via the cloud.

The following table presents a non-exhaustive list of information used for performing each of the utility functions described above[1]:

Table 2-1. Information Used for Each Utility Function

	Back-office, billing, and customer interface	Planning, Forecasting, Market Participation	Utility Operations Real time	Utility Operations Non-real time
Customer Information Including Metering	Contains personally identifiable information, but no system control information	Included in the historical load data	Included in the real-time load data	N/A
Power System Topology	N/A	Yes	Included in the real-time topology	Included as part of asset monitoring
Communication System Topology	N/A	Yes	Included in the real-time topology	Included as part of cyber/IT monitoring
Historical Operational Power System Data (SCADA, PMU etc.)	N/A	Yes	Not directly used	Included as part of past asset monitoring
Historical Bulk Generation Data	N/A	Yes	Not directly used	N/A
Historical Distributed Generation Data	N/A	Yes	Not directly used	N/A
Historical Power Export/Import Transactions	N/A	Yes	Not directly used	N/A
Real-time Topology	N/A	N/A	Yes	N/A
Real-time power system state data	N/A	Limited	Yes	N/A
Real-time control data	N/A	N/A	Yes	N/A
Asset performance data (e.g., transformer oil temp.)			N/A	Yes for all monitored assets
Waveform Data (Comtrade, others)	N/A	N/A	Currently not used but useful in the future	Yes

[1] Note that all of the information listed in this table is sensitive either due to PII or critical infrastructure information (CII) concerns.

3.0 Cloud Computing Cyber Security Challenges

The transition of functions used in power system utility operations to cloud computing will be gradual and will only occur if the cyber security challenges we describe in the following sections are addressed. To be able to describe these challenges appropriately, we first need to define what the traditional security triad of availability, integrity, and confidentiality means in the cloud computing context. From these definitions, we can start discussing cyber security challenges related to the handling of information input for processing; control and information outputs; shared tenancy; and finally, shared physical infrastructure.

3.1 Defining Availability, Integrity, and Confidentiality in the Cloud Computing Context

The implications of traditional cyber security concepts of availability, integrity, and confidentiality change in the context of cloud computing. For example, most public and private clouds automatically fail over to different locations in the event of equipment, power, or network outages. But what is the impact to availability when a utility based in Richland, WA uses a service based on Amazon EC2, and the Amazon EC2 starts sending utility applications to a data center in North Carolina instead of Seattle, WA, resulting in 70-80ms of increased latency? The applications are still "available," but the increased latency may hamper the functionality of a control application. The relocation of power system utility applications to the cloud also has a significant impact on the integrity and confidentiality requirements. For example, while it may be sufficient to leave data in the clear when they are on disk at the utility site, the shared tenancy of a service such as Amazon EC2 may require the use of an encrypted file system. Although most utilities may rely on physical security and private cable plants to assure the integrity of data communications for their environment, when data are being transported to the cloud, cryptographic means to assure integrity may be required. In summary, all three factors of availability, integrity, and confidentiality need to be carefully evaluated as applications and functionality are moved to the cloud. IT and cyber security professionals often replicate designs that they have used in the past. When cloud computing is being utilized, a complete cyber security requirements analysis and design using the methodology described in (NIST 2010; NIST 2011) must be performed.

In the following sections, we discuss specific cyber security challenges related to information inputs, control outputs, shared tenancy, and physical infrastructure.

3.2 Cyber Security Challenges Related to Information Input

A power system application hosted in the cloud requires information to produce results regardless of its purpose. A customer information portal that displays energy usage on a 15-minute basis requires metering information. A dynamic demand response application requires both metering (load) and power availability (generation) information to accomplish its mission. A planning application hosted in the cloud requires: detailed power system topology, historical and current power flow, and generation information among others. The cyber security challenges related to information input to applications running in the cloud are categorized into three areas:

1. *Deciding on methods for information collection and egress from utility electronic security perimeter*: In order to send information to applications running in the cloud, the utility needs to identify all pertinent sources of information and assign a sensitivity level to the information. The information will need to be collected from multiple sources and systems. The utility must then decide how this information will be delivered to the application in the cloud. The utility should ask and answer questions such as:

    - Does each system deliver the information separately through the utility electronic security perimeter?

    - Is the information collected on a messaging bus such as ActiveMQ and then delivered through the messaging bus or use a non-standardized mechanism?

    - How is the access to information at the cloud controlled?

    - Does the utility open holes through its electronic security perimeter for information egress or does it implement a VPN solution?

    - What type of auditing and logging is performed on the information being sent to the applications in the cloud?

    - How often is the information collected? How often is it sent? Specifically, how will information from legacy equipment using older protocols be collected, in a time-aligned fashion to be delivered to the cloud?

2. *Deciding on information transport from utility to cloud computing facility*: The utility will recognize all information types to be sent to the applications running in the cloud and will assign a sensitivity designation. After this step, the utility must decide on what mechanisms are used to transport the data by asking questions such as:

    - What are the integrity and confidentiality requirements for the information being sent to the cloud?

    - Is a private (utility-owned) communications network used to transport the information?

    - Does an internet protocol security virtual private network (IPSEC VPN) meet confidentiality and integrity requirements? What types of cryptographic mechanisms need to be used?

    - How are the communicating parties identified and authenticated?

    - If public key infrastructure (PKI) is used for authentication, what are the trust roots for the PKI?

    - If multiple applications are ingesting the information provided by the utility, how is the information distributed once it gets to the cloud?

- What are the availability requirements for the information being transported?
- Are the applications sensitive to latency and jitter? What is the maximum latency that can be tolerated?
- Can any of the information be delivered by physical means such as CD-ROM via carrier?
- How is the cloud computing facility protected against denial of service attacks?

3. *Deciding on information storage at the cloud computing facility*: Once the information is sent to the cloud, the utility needs to be concerned about how that information is being stored and, if applicable, archived. The cyber security challenges related to information storage highly depend on whether the utility is using an infrastructure-as-a-service or a software-as-a-service application. The utility needs to answer questions such as:

    - What is the storage infrastructure provided and used by the cloud application? Is it shared?
    - Are all types of information stored in the cloud encrypted?
    - Where is the geographic location of the storage system (as it could be different from the geographic location of the application being hosted)?
    - What types of backup strategies protect the information being stored in the cloud?
    - What is the geographic location of the backup systems? If tape archives are being used, what is the geographic location of the tape archives?

3.3 Cyber Security Challenges Related to Information and Command Output

There are classes of power system utility applications that interface with systems and operators back at the utility. Other classes of applications may interface with utility customers via the public Internet, typically using a web browser or mobile application. In this section, we will specifically discuss challenges related to the former classes of applications excluding cloud applications that directly interact with the customer. Cyber security challenges related to output of information and commands from cloud applications can be examined in three areas:

1. *Choosing a data transport from cloud computing facility to the utility*: The utility must identify and assign sensitivity to all information and commands being sent by the cloud applications. Similar to the questions we stated in the previous section, the utility must then ask (and answer) questions such as:

    - What are the integrity and confidentiality requirements for the information being sent from the cloud?
    - Is a private (utility-owned) communications network used to transport the information?

- Does an IPSEC VPN meet confidentiality and integrity requirements? What types of cryptographic mechanisms need to be used?

- How are the communicating parties identified and authenticated?

- If PKI is used for authentication, what are the trust roots for the PKI?

- Are the systems using the information being sent by the cloud application sensitive to latency and jitter? What is the maximum latency that can be tolerated?

- What are the availability requirements for the information being transported?

- Can any of the information be delivered by physical means such as CD-ROM via carrier?

2. *Configuring data ingress through the utility electronic security perimeter(s)*: Many utilities in the electric power system architect their communication networks following guidelines established by (NIST 2010; NIST 2011). Multiple levels of firewalls and other network isolation mechanisms are typically used to implement defense-in-depth strategies. The utility must then decide how the information and control commands coming from the cloud applications must be transported to the appropriate systems. The utility must answer questions such as:

   - What systems interact with the cloud applications?

   - What types of communication mechanisms are being used?

   - Is it possible to place intermediary servers in the utility demilitarized zone to receive the information and commands being sent by the cloud applications?

   - What types of communication pathways and firewall holes need to be opened to distribute the information coming from the cloud? For example, if a dynamic demand-response mechanism is being implemented and the commands need to be sent through the advanced metering infrastructure (AMI) network, a communication pathway must be present that allows the cloud application to communicate through the AMI system.

   - What type of intrusion detection and prevention system must be used to reduce the risk of unauthorized parties exploiting the established communication pathways?

   - Is it possible to lock the communicating cloud applications with a set of IP addresses? (Note that this may have adverse consequences when geographic distribution is used.)

3. *Performing information and command validation*: The cyber security challenges in this area are related to validation of content irrespective of the transport layer security. The power system utility receiving information and commands from cloud applications must not rely on the transport layer to provide all integrity and confidentiality services. Aligned with the defense-in-depth strategy, each information and command type must have integrity and

potentially confidentiality protections in accordance with its sensitivity type. The utility must answer questions such as:

- What type of cryptographic keys and credentials must be used to provide integrity services to content? For example, does each application possess its own credentials or are the credentials shared?

- What is the workflow to handle commands being issued by the cloud applications? Do they need to be validated by an operator before being sent to equipment in the field?

- If multiple pieces of information are contained in an XML, JavaScript Object Notation (JSON), or binary packed message, does each piece of information need to be validated individually or is the entire message validated?

- How are the information and commands sent by cloud applications captured for audit and accounting purposes?

3.4 Cyber Security Challenges Related to Shared Storage and Computational Resources

Most implementations of cloud services share computational resources, including storage, memory, processor, and network bandwidth across multiple applications and "tenants." The sharing of resources presents a unique challenge for power system applications running in the cloud. This challenge is especially true for any application that either needs to produce output or ingest input in real time. A utility interacting with a cloud service provider or a vendor must ask questions such as:

- How are the computational resources managed for different applications running in the cloud?

- Are there any guarantees for resource allocation and network access? If so, what types of service levels can be expected?

- What is the fault-tolerance strategy?

- What type of quality of service can we expect for our network traffic? What is the topology of the network infrastructure inside the cloud service provider?

- Are there enough resources to accommodate all tenants sharing the computational resources? Can a misbehaving tenant disrupt service for other tenants?

- How are the storage and memory resources isolated for each tenant isolated from each other?

- What are the communication mechanisms for multiple applications for the same utility hosted in the same cloud? Is it possible for another tenant to intercept these communications?

- If a SaaS application is being used, how are the data for multiple users of the same application isolated?

3.5 Cyber Security Challenges Related to Shared Physical Infrastructure

Of all the cyber security challenges associated with using cloud applications within a power system utility, the physical security is the most interesting. One of the main benefits of running applications in the cloud is the fault tolerance and resource scaling provided by the cloud infrastructure. An application can exist in multiple cloud infrastructure locations at the same time and transfer execution between these different locations without any noticeable impact to service. Unfortunately, this flexibility and seamless transition of processes from one location to another present a problem for utilities. Specifically, a utility using a cloud application must ask questions such as:

- Are there any cloud infrastructure locations in an undesired or unallowed jurisdiction?
- Do all cloud infrastructure locations providing an application meet the same cyber security standards? Are there any jurisdictional and legal differences between different locations?
- Can we inspect and audit the locations from which our application will be served?
- How are the communication links connecting the cloud infrastructure to the rest of the communications infrastructure secured?
- Are any of the locations serving our application located in an area with potential natural disasters (e.g., hurricanes, earthquakes, etc.)? If yes, how are these locations protected against natural disasters?
- What is the power and cooling reserve in case of an emergency?
- What types of physical security mechanisms are in place to prevent undesired access to physical computing infrastructure? Who has physical access to the physical computing infrastructure?
- How are the employees vetted? What are the types of background checks performed?

4.0 Future Research Directions and Conclusion

The transition of functions used in power system utility operations to cloud computing will be gradual and will only occur if the cyber security challenges are addressed. Cloud computing has already provided many financial and social benefits to billions of consumers and millions of commercial and government entities and has the potential to provide many benefits to the power system industry. Many utilities are already experimenting with the use of cloud applications for their billing, customer interface, and smart metering portals. We believe that further research in the following areas is warranted:

- *Concrete* cyber security guidelines and recommendations for utilities using cloud computing
- Cyber security and service-level monitoring techniques to detect problems that can occur with shared computational resources in the cloud
- Algorithms and tools to guarantee computational resources to applications with real-time requirements
- Metrics to measure and provide service guarantees in cloud environments
- Algorithms and tools that protect instruction and in-memory data streams to prevent snooping of sensitive data or tampering with sensitive computations
- Algorithms and tools to detect subversive routing of network traffic between the cloud infrastructure and the utility.
- Research into which applications can support failover and how
- Research into additional benefits of use of cloud computing such as: Merged power system view across multiple utilities and regions; high performance analytics performed in the cloud for power systems.

5.0 References

Birman KP, L. Ganesh , and R. van Renesse. 2011. "Running Smart Grid Control Software on Cloud Computing Architectures," Workshop on Computational Needs for the Next Generation Electric Grid, Cornell University, April 19-20, 2011, Ithaca, NY, USA.

NIST. 2010. Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." National Institute of Standards & Technology. Accessed September 7, 2012 at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

NIST. 2011. Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security." National Institute of Standards & Technology. Accessed September 7, 2012 at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

NIST. 2012. Special Publication 800-146, "Cloud Computing Synopsis and Recommendations." National Institute of Standards & Technology. Accessed September 7, 2012 at http://www.nist.gov/itl/cloud-052912.cfm.

U.S. Congress. 2009. American Recovery and Reinvestment Act. 111th Congress, 1st session, U.S. Government Printing Office, Washington, D.C.

Pacific Northwest
NATIONAL LABORATORY

U.S. DEPARTMENT OF
ENERGY

Proudly Operated by Battelle *Since 1965*

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)
www.pnl.gov