An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds

Yogesh Simmhan∗‡, Alok Gautam Kumbhare∗†, Baohua Cao∗†, and Viktor Prasanna∗†‡

∗Center for Energy Informatics †Computer Science Department
‡Ming Hsieh Department of Electrical Engineering
University of Southern California, Los Angeles CA 90089

-Ritesh Reddy Kanuganti
Contents:

• Introduction
• Analysis of User Characteristics
• Analysis of Data Characteristics
• Analysis of Application Characteristics
• Analysis of Platform Characteristics
• Advantages, Limitations
• Related Work
• Conclusion
Introduction:

• Smart Grids let utilities optimally manage the electric power capacity and load within their service area, leading to more sustainable energy use in the long term.
• Smart Grids are cyber-physical systems that blur the line between physical electricity infrastructure and cyber infrastructure.
• Smart Grids have a greater exposure to cyber-attacks that can potentially disrupt power supply in a city.
• Data security and privacy remain top concerns for utilities and consumers that is affecting Smart Grid adoption.
Usage of LA Smart Grid Demonstration Project

• To identify and analyze security and privacy concerns for Smart Grids on Clouds.
• Analysis is intended to benefit and inform two audiences
  ➢ *Smart Grid developers* on Clouds, to help them better understand the security and privacy issues to be cognizant of.
  ➢ *Cloud researchers*, to identify novel research challenges posited by the Smart Grid domain that they can tackle.
• **Utilities**: Utilities have several responsibilities such as stable grid operations including generation, transmission and distribution of power, maintaining customer satisfaction, and complying with various regulatory norms.

  Utilities may also provide an infrastructure for third party services to run their applications in the Cloud and access consumer and other data available in the Cloud.
Analysis of User Characteristics

• **Consumers**: Smart meters installed at the consumers’ end communicate with various smart appliances within the home and building area network (HAN and BAN) to gather power usage data as well as send control signals to these appliances and equipment within the facility.

  This can lead to *data leakage* and *data modification* attacks in which the hackers break into HANs and generate bogus usage data or control signals.

• **Third Part Service Providers**: Regulatory norms may restrict Smart Grid data to flow out of the utility infrastructure and hence require the third party providers to deploy their services within the sandboxed environment provided by the utility in the Cloud.

  This raises security and privacy concerns for the application providers.
Analysis of Data Characteristics

Data Characteristics & Security/Privacy Issues

- **Data Diversity**
  - Direct & Indirect Data Types
  - Distributed Sources
  - Diverse Ownership
  - Heterogeneous Cloud Storage Services

- **Data Granularity**
  - Data Size
  - Data Collection Rates
  - Access control granularity
  - Security enforcement cost/latencies

- **Data Transformation**
  - Multi-owner data aggregation
  - Integrating private & public data
  - Current & legacy data sources

- **Data Access & Sharing**
  - Shared repositories
  - Individual access control
  - Dynamic policies & latency
  - Intent of use & Audit trail

- **Data Archival**
  - Data size growth
  - Policy & technology evolution
  - Longer, wider attack exposure
  - Multiple jurisdiction
Analysis of Application Characteristics

• Application Services
  Data shared between these applications need to be secured and their privacy preserved.
  Data leakage becomes harder to contain once it leaves the confines of the utility’s software and Cloud environment.

• Application Access
  The utility may need to provide their own security and privacy framework to access their applications and potentially, external applications, they host on the Cloud.

• Legacy and Emerging Applications
  Security and privacy framework will have to be compatible with both new and existing applications.
Analysis of Platform Characteristics

• IaaS, PaaS, SaaS
  ✓ IaaS providers provide the flexibility to deploy and operate any software environment by the utility, and this extends to the convenience of deploying and managing any security and privacy framework required by the utility.
  ✓ PaaS provide access control and identity management like Active Directory as platform services in the Cloud.

• Public, Private, Hybrid Clouds
  ✓ Public Clouds provide multi-tenant services where more than one organization shares the same underlying hardware,
  ✓ Private Clouds use hardware exclusively for a single organization at a local site, with the Cloud fabric providing virtualization and storage services.
  ✓ Hybrid Clouds are composed of resources on both public Clouds and an organization’s private Cloud.
Related Work

- The differences between the traditional power grid and the Smart Grid have been studied to identify new vulnerabilities that arise. Categorizes attacks on Smart Grid into network availability, data integrity, and information privacy.
- Implements Smart Grid security as a SaaS service, with all communication and data being passed through their access control and intrusion detection service to identify and tackle specific aspects of security and privacy without taking a holistic approach.
- Research to identify threat vectors arising from using Cloud infrastructure, and privacy concerns have been studied separately.
Conclusion

• Classify various factors and user roles that contribute to Cloud security and privacy issues in an information-driven Smart Grid application domain that is of increasing importance.

• They organize known security concerns in Clouds from a Smart Grid application practitioners perspective, and identify several unique privacy and regulatory issues that pose a challenge for further research.

• Recognize issues that they need to address in our Cloud-based software architecture for the Los Angeles Smart Grid project,
References

• “FERC Assessment of Demand Response and Advanced Metering,” Staff Report, December 2008.
• Smart Grid Deployment Tracker 3Q10,” Pike Research, November 2010.
Thank you!