ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

An Analysis of Smart Grid Software Architectures on Clouds Environment

Utkarsh Gore, Prof. Shikha Pachouly

Dept. of Computer Engineering, AISSMS College of Engineering, Pune, India

ABSTRACT: Smart grids are modernized electricity grids with information technology support. Smart Grids are the most promising development in the energy and utilities market. Smart grids are being installed in many countries and it is expected to have multi-fold benefits in efficient energy management. The Smart Grids receive real time meter data with high velocity and volume. In such scenario, near real time efficient analytics of streaming smart meter data and quick decision making is significant. Cloud computing is the latest distributed computing paradigm and it offers tremendous opportunities to solve large-scale scientific problems. However, it presents various challenges that need to be addressed in order to be efficiently utilized for workflow applications. Although the workflow scheduling problem has been widely studied, there are very few initiatives tailored for cloud environments. Furthermore, the existing works fail to either meet the user's quality of service (QoS) requirements or to incorporate some basic principles of cloud computing such as the elasticity and heterogeneity of the computing resources. This paper proposes a resource provisioning and scheduling strategy for scientific workflows on Infrastructure as a Service (IaaS) clouds. Cloud computing makes your small business dependent on the reliability of your Internet connection. When it's offline, you're offline. How safe is your data? Cloud computing means Internet computing. So you should not be using cloud computing applications that involve using or storing data that you are not comfortable having on the Internet. Established cloud computing vendors have gone to great lengths to promote the idea that they have the latest, most sophisticated data security systems possible as they want your business and realize that data security is a big concern. In this paper, we survey the existing methodologies and means for real time energy data management in smart grids.

I.INTRODUCTION

There are three major participants in the Smart Grid ecosystem: consumers, utilities and third party service providers, each with a different perspective on privacy and security requirements. Here, we discuss how these stakeholders interact with the Smart Grid software architecture deployed on Clouds, and identify security and privacy concerns arising from those interactions.

Consumers

Electricity users include residential, commercial and industrial consumers. Residential consumers, such as single or multi-dwelling residential units, may provide limited access to utilities to directly control their appliances, and voluntarily curtail their power usage when notified of realtime pricing or other incentives by the utility. Industrial Consumers include large scale manufacturing units which usually have significant power requirements and are willing to pay more than the residential consumers for power quality guarantees.

Commercial consumers

encompass businesses, shopping malls, university campuses, restaurants, retailers and so on. Industrial and commercial consumers are typically more willing than residential consumers to participate in demand optimization through direct control, given appropriate pricing incentives.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Smart Grid Utility

Utilities are central to the Smart Grid ecosystem and have several responsibilities such as stable grid operations including generation, transmission and distribution of power, maintaining customer satisfaction, and complying with various regulatory norms. Moving from the traditional electric grid to a Smart Grid raises several concerns for the utility providers, particularly in a Cloud environment.

Third Party Service Providers

We envision a Smart Grid ecosystem where, in addition to the primary application of optimized demand response, various other applications will be developed and deployed by third party providers offering a range of value added services to the consumers. However, 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. For example, it can potentially expose various proprietary algorithms as well as intellectual property including data from private sources used by the third party to provide different services to the consumer.

II.LITERATURE SURVEY

Electric utilities are increasingly transitioning to Smart Power Grids that use large scale smart meter deployments at power consumers for bi-directional realtime communication using Internet protocols [1], [2]. This enables utilities to monitor electricity usage as it occurs and provide signals to consumers to reduce their usage if the load on the utility nears its available capacity. Smart Grids are expected to let utilities optimally manage the electric power capacity and load within their service area, leading to more sustainable energy use in the long term. One outcome of Smart Grids is the advent of an information-driven approach to energy management by the utility [3]. Such an informatics approach is essential as utilities undergo other transformational changes that impact their operations, such as the growing popularity of electrical vehicles that draw more power from the grid, and cogeneration by their customers who use solar panels and wind turbines to generate and feed back power to the utility intermittently. Such dynamism in power consumption and production affects traditional electricity forecast and planning models. New models for demand forecasting use direct and indirect information from diverse sources along with data mining and machine learning techniques for more accurate, adaptive and real time predictions. Many of these Smart Grid applications are compute and data intensive, requiring the use of scalable platforms to deploy and operate in a reliable manner. For example, the Los Angeles Smart Grid demonstration project will eventually support over 1.4 million electrical customers in the largest municipal utility in the United States [4], with data on the order of terabytes potentially processed daily. The resource needs for the utility also varies over the time of the day, with peak operation occurring during the day and information processing needs slowing down at night. In addition, the growth of third party Smart Grid applications for consumers, such as Google PowerMeter1 and Microsoft Hohm2, means that utilities need to share electricity usage and operational information it aggregates with external services. These requirements of scalable, elastic, reliable and sharable resources for deploying and running a Smart Grid utility's software architecture strongly fits the capabilities provided by Cloud platforms [5]. Indeed, some data warehouse vendors are already considering Cloud deployments for Smart utilities [6]. Smart Grids are cyber-physical systems that blur the line between physical electricity infrastructure and cyber infrastructure, with the Internet providing the backbone for utilities to assimilate content, control operations and even communicate with consumer appliances [7]. As a result of their online presence, Smart Grids have a greater exposure to cyber-attacks that can potentially disrupt power supply in a city [8]. A more mundane scenario is power theft by consumers hacking a smart meter or its communication channel to change the reported electricity usage. In addition, utility and other third party software can access and integrate electricity usage data with other personal consumer information available through, say, social networks and electric vehicles for better demand forecast and load curtailment response. This means that ensuring privacy of personally identifiable data within the utility's information integration platform is of growing concern. While some privacy concerns arise due to lack of security, others are side effects of integrating disparate data sources that together may provide unprecedented insight into user activities. Data security and privacy remain top concerns for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

utilities and consumers that is affecting Smart Grid adoption [9]. Consumers need to gain more confidence in sharing data to help engender a rich space of Smart Grid services that can improve the operational efficiency of the utility and allow customers better manage their energy usage. Cloud platforms heighten some of these concerns and are presented with unique challenges to address security and privacy issues for Smart Grid software deployment for utilities. These concerns need to be adequately addressed before the true potential of Clouds can be realized for Smart Grids.

III.ANALYSIS AND REVIEW

Public as well as private clouds provide a high degree of scale-out and geographically distributed datacenters for data replication and reliable access. This has the consequence of increasing the attack surface and the potential for data leakage. While the fabric that runs on Public and Private clouds may be identical, private clouds may provide stronger security by curtailing and monitoring physical access to their datacenter. In addition, the private datacenter may deploy additional firewall measures and virtual private networks to gain fine grained control and auditing of access to the Cloud resources. These may help meet regulatory requirements better than public clouds. Hybrid Clouds can get the benefits of both public and private Clouds by running essential services and applications on more secure private Clouds and offloading those with lesser guarantee needs to public Clouds that are easier to manage. This however, also brings issues of policy consistency across public and private Clouds into light.

IV.CONCLUSION

In this taxonomical analysis, we 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. We 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. Besides helping us recognize issues that we need to address in our Cloud-based software architecture for the Los Angeles Smart Grid project, we expect this article to guide both researchers and developers in building secure and privacy-reserving Smart Grid applications.

REFERENCES

[1] "FERC Assessment of Demand Response and Advanced Metering," Staff Report, December 2008.
[2] "Smart Grid Deployment Tracker 3Q10," Pike Research, November 2010.
[3] Y. Simmhan, S. Aman, B. Cao, M. Giakkoupis, A. Kumbhare, Q. Zhou, D. Paul, C. Fern, A. Sharma, and V. Prasanna, "An Informatics Approach to Demand Response Optimization in Smart Grids," Computer Science Department, University of Southern California, Tech. Rep., 2011.
[4] Electric Power Industry Overview 2007. [Online]. Available: http://www.eia.doe.gov/electricity/page/prim2/toc2.html
[5] Y. Simmhan, M. Giakkoupis, B. Cao, and V. K. Prasanna, "On Using Cloud Platforms in a Software Architecture for Smart Energy Grids," in IEEE International Conference on Cloud Computing (CloudCom), 2010.
[6] D. Harris. (2011, February) Teradata scores 100tb deal for smart grid data. [Online]. Available: http://gigaom.com/ cloud/teradata-scores-100tb-deal-for-smart-grid-data/
[7] J. Sztipanovits, J. A. Stankovic, and D. E. Corman, "Industry Academy Collaboration in Cyber Physical Systems (CPS) Research," CRA, Tech. Rep., 2009.
[8] M. T. BURR, "SMART-GRID SECURITY; Intelligent power grids present vexing cyber security problems," PUBLIC UTILITIES FORTNIGHTLY, p. 43, 2008.
[9] J. Polonetsky and C. Wolf, "How privacy (or lack of it) could sabotage the grid," Smart Grid News, 2009.
[10] E. L. Quinn, "Smart metering and privacy: Existing laws and competing policies," SSRN eLibrary, 2009.
[11] Y. Simmhan, B. Cao, M. Giakkoupis, and V. K. Prasanna, "Adaptive rate stream processing for smart grid applications on clouds," in ACM Workshop on Scientific Cloud Computing (ScienceCloud), 2011.
[12] B. Rimal, E. Choi, and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," in International Joint Conference on INC, IMS and IDC, 2009.
[13] A. Kumar. (2011, January) A review of windows azure security. [Online]. Available: http://www.brighthub.com/environment/green-computing/articles/104281.aspx
[14] E. A. Feinberg and D. Genethliou, Applied Mathematics for Restructured Electric Power Systems. Springer US, 2005, ch. Chapter 12: Load Forecasting, pp. 269–285.
[15] T. Zhang, W. Lin, Y. Wang, S. Deng, C. Shi, and L. Chen, "The design of information security protection framework to support smart grid," in Conference on Power System Technology, 2010, pp. 1 –5.