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
Email: {simmhan, kumbhare, baohuaca, prasanna}@usc.edu

***Abstract*—Power utilities globally are increasingly upgrading to Smart Grids that use bi-directional communication with the consumer to enable an information-driven approach to distributed energy management. Clouds offer features well suited for Smart Grid software platforms and applications, such as elastic resources and shared services. However, the security and privacy concerns inherent in an information-rich Smart Grid environment are further exacerbated by their deployment on Clouds. Here, we present an analysis of security and privacy issues in a Smart Grids software architecture operating on different Cloud environments, in the form of a taxonomy. We use the Los Angeles Smart Grid Project that is underway in the largest U.S. municipal utility to drive this analysis that will benefit both Cloud practitioners targeting Smart Grid applications, and Cloud researchers investigating security and privacy.**

I. Introduction

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 co-generation 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 realtime 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 PowerMeter[1] and Microsoft Hohm[2], 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.

[1] www.google.com/powermeter
[2] www.microsoft-hohm.com/

978-0-7695-4460-1/11 $26.00 © 2011 IEEE
DOI 10.1109/CLOUD.2011.107

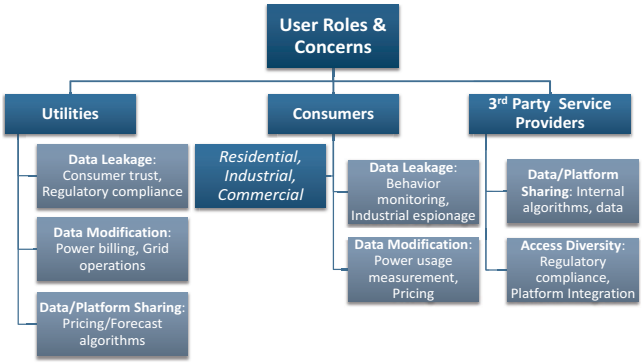

Figure 1. User roles and their security/privacy concerns in a Smart Grid ecosystem.

Data security and privacy remain top concerns for 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.

In this article, we use our experience gained in designing a Cloud-based software architecture for the Department of Energy sponsored Los Angeles Smart Grid Demonstration Project to identify and analyze security and privacy concerns for Smart Grids on Clouds. The project itself is discussed in detail elsewhere [3]. We present several perspectives on security and privacy – from the user, data, application and platform – that contribute to a **taxonomy of issues** that arise. While our primary focus is on the software architecture for the utility hosted on Clouds, we recognize that edge devices like Smart meters and third party applications operating on behalf of the utility or consumers play an equally important role in data collection, analysis and dissemination. Hence, we investigate a broader ecosystem of Smart Grid applications.

This analysis is intended to benefit and inform two audiences: (1) *Smart Grid developers* on Clouds, to help them better understand the security and privacy issues to be cognizant of, and (2) *Cloud researchers*, to identify novel research challenges posited by the Smart Grid domain that they can tackle.

In the following sections, we present our analysis of user (Section II), data (Section III), application (Section IV) and platform (Section V) characteristics that impact security and privacy of Smart Grid applications on Clouds. We discuss related work in Section VI and present our conclusions in Section VII.

II. Analysis of User Characteristics

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. These are summarized in Figure 1.

A. 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.

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. These networks have software logic that can optimize power usage based on user preferences and demand response signals received from the utility. However these networks may be vulnerable to attacks due to misconfiguration by the consumer. 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. Smart meters also communicate this information with the utilities and third party providers over the Internet, and attacks can target this transmission as well.

Consumers may share additional information with the utility which can be integrated with the usage data for generating better forecast models [3]. For residential customers, information about the installed smart appliances and plug-in electric vehicles (PEVs), room/home temperature and thermostat data, social network activity, and so on could be shared. However disclosure of such information to attackers can potentially reveal personally identifiable information about the consumers and can even be used to predict *personal behavior* [10]. For industrial and commercial consumers additional data points include information about the machinery used, manufacturing schedule, "sale" events, PEV fleet operations, and occupancy sensors. However, this information is highly sensitive and raises the prospects of

industrial espionage where competitors can gain access to this information, for example, to predict manufacturing output by integrating the fine grained power usage data with schedule information and data from people sensors.

B. 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.

The utilities use the Cloud infrastructure to store and process large quantities of data collected from Smart meters and appliances as well as sensors deployed across the Smart Grid. This raises *regulatory compliance* issues since the data will potentially be stored and processed in a distributed manner across geographical boundaries. It also increases the exposed attack surface that can affect *grid operations*. It increases concerns over data leakage during data movement and sharing that can compromise *consumer trust*. It also exposes various forecast and *pricing algorithms* used by the utility to the Cloud provider. The 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. This further adds to the security and privacy concerns such as *unauthorized access* to the Cloud resources.

C. 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. Section IV provides examples of such applications. 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.

Another major challenge is the integration of the utility Cloud infrastructure with internal infrastructure including legacy security and privacy software. This makes it difficult to prove *regulatory compliance* since the required features will be distributed across private and utility's public infrastructure.

III. Analysis of Data Characteristics

A. Diversity of Data Sources

The Smart Grid's intelligence and adaptiveness depends on the ability to acquire and integrate diverse information that help perform accurate load forecasting and curtailment by utilities and provide rich services to customers. A Smart Grid utility uses both direct power systems information and information that indirectly helps forecast, correlate and control power usage. *Direct information sources* include consumer smart meters that transmit power usage and smart appliances data, sensors at transformers and distribution stations, and customer information systems used for billing. *Indirect sources* are historical, current and forecast weather from NOAA, social network and schedule information shared by consumers for load prediction, studying consumer behavior on the utility's website, and mobile applications that may send consumer location information and receive load curtailment response.

The conceptual diversity present in the Smart Grid system gives rise to a *wider range* of information from *multiple sources* that need to be secured and controlled according to policies defined by the data owners. These data sources include information that is both public and private, with *ownership* belonging to the different user roles introduced before. Increasing information flows raises the chance that personally identifiable information will be passed which, if not handled carefully, can lead to violation of an individual's privacy.

Cloud platforms need to support secure data acquisition from different information sources. While public Clouds are naturally suited for scaling out and processing millions of user requests, the diversity of information also requires *diverse storage services* that can enforce security and privacy policies. The policies themselves can be complex and varied, given the number of different information sources such as consumers, public agencies, online service providers and prior utility data.

B. Data Size and Temporal Granularities

Smart Grid utilities need to handle data at *extreme scales of data size*. At one end, HAN systems can report fine-grained usage of smart appliances, on the order of bytes/kilobytes to the utility through the smart meter. At the other end, this data accumulated from millions of consumers over years can grow to petabytes (PB) in size, and form a data mining corpus to detect load patterns and test response scenarios. The size of data collected may vary continuously as adaptive demand-response algorithms control smart meter data collection rates, and add or drop information sources [11]. Privacy policies and security infrastructure has to efficiently and effectively support such diverse information sizes.

The *frequency* of data generation and its *timeliness* of use in Smart Grids also differs from traditional power grids.

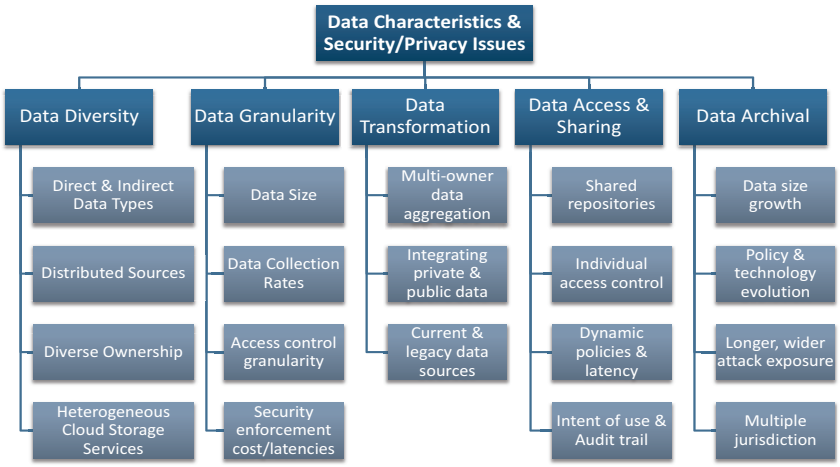

Figure 2. Characteristics of data and their security/privacy challenges in a Smart Grid ecosystem.

Consumer power usage data can be collected on the order of minutes from smart meters, as opposed to the typical, once a month of aggregated usage reported earlier. Phasor measurements from transformers measure power quality several times per minute. Traffic patterns and social media feeds also change at short time durations. Such fine resolution data is useful for low latency detection of a peak load event on the power grid. Enforcing security and privacy policies should not introduce unacceptable *latencies* that make the information stale.

The varying granularities of data sizes and their time sensitiveness poses a challenge in enforcing security and privacy policies in a Cloud. Cloud storage services will need to efficiently control access to small and large data sizes. The *access control granularity* for current file and table storage services in public Clouds are on the order of Files/BLOBs and Tables [12], [13]. These may be insufficient for, say, users to define (and utilities to implement) access policies at the level of individual appliances (KBs) that may be rows in a file or tuples in a table. Encryption is often used to secure data in untrusted storage environments. Utilities that need to secure PBs of annual meter data may find encrypting and decrypting using Cloud storage services *time and cost consuming* in the absence of native support for securing data or hardware accelerated cryptographic algorithms. Such digital signatures may also bloat the data size, causing additional storage and bandwidth usage.

C. Data Aggregation and Transformation

Information collected by the utilities from different sources needs to be processed and *aggregated* to provide various services to the consumer, and to provide infrastructural support to third party service providers. For example, utilities may integrate and analyze live power usage data from smart meters with historical usage data as well as current and forecasted weather data to provide demand-response services to the consumers in a format suitable for consumption. Utilities may run data mining workflows over data and return results used for operations and potentially shared with consumers and third parties, who may in turn integrate them with data they control to provide additional services.

Aggregating data from *multiple owners* gives rise to a range privacy concerns that is different from data authorized by a single source. For example, combining anonymized data from an individual with public datasets can potentially reveal information about the individuals unintentionally. These concerns are heightened while integrating Smart Grid data collected at the present with legacy data stores that were sourced for other purposes that did not foresee privacy considerations arising out of data integration. Integrating such *legacy data* with Smart Grid data hosted on Clouds poses challenges both in terms of conversion to appropriate data format and enforcing access control mechanism to ensure privacy.

D. Data Access and Dissemination

The sensitive nature of data generated in the Smart Grid behooves strict enforcement of policies for distributed data access and dissemination. Access control policies should support granular access at levels ranging from individual raw streams to large historical data archives, in a scalable manner. It is necessary to support mechanisms to allow consumers to specify and update access policies on *data they own* and provide to the utility, which may be hosted in a *shared repository* that is accessible both to the utility and third party providers.

Access policies may depend on *dynamically* changing external information. For example, users may specify an access policy for their energy usage data that is based on the friends that they have on their Facebook network. Any changes to their friends list should be dynamically propagated to the access control system. However the distributed nature of Clouds introduces an inherent latency in

information propagation and can lead to inconsistent policy enforcement. There is a trade-off between maintaining consistent access policies for each consumer, and the resource costs for updating the access control list frequently. The scalable resources available on Clouds, while alleviating some security issues such as parallel data en/decryption on multiple VMs also poses challenges to enforcing access policies on distributed resources consistently. There are open research issues on secure storage services that can scalably support such requirements out of the box.

Data collected for one purpose may be used by a number of future and *unintended applications*. For example, GPS data from an individual's PEV can used to predict its charging schedule and hence can be used for load forecasting. However, the same information can also be used to mine user's travel pattern which can be integrated with information about other social activities and hence monitor a user's actions. This leads to a question of the intention for which data is shared by their owners, and the need for the access control system to ensure that utilities and service providers restrict data usage only for agreed purposes, for example, by allowing access only to certain data APIs. It should also be possible to *audit* and ascertain liability for misuse of the data

E. Data Archival and Regulatory Compliance

Information acquired and integrated by the power utility needs to be preserved over long time periods. This data is necessary both for the utility operations, as well as for complying with regulations and legal requirements.

Models for forecasting energy usage use historical electricity consumption data [14], [15]. Typically, availability of a longer time period of historical power usage data leads to *better forecast models*. The information used by next generation load forecast models in Smart Grids will use diverse information sources introduced before. The dynamic nature of the Smart Grids due to smart appliances, intelligent HANs/BANs and cogeneration of power by consumers also means that unique events occur often, and there is less opportunity for information compression through aggregation before storing them, causing *data bloat*.

Utilities in the United States are regulated by federal and state energy regulatory commissions. Different regulations are applicable to corporate and municipal utilities [16] to monitor competition, power supply and, more recently, data security and privacy in Smart Grids [17]. Regulations may require the utility to not just protect consumer and private data, but also be *transparent* about energy pricing by, for e.g., disclosing information used for setting the power price. This requires utilities to maintain the information they use for their operations over long terms.

The longer duration of data preservation means some of the security codes and privacy policies will have to *evolve over time* as user's perception of privacy changes and the computational ability to break cryptographic algorithms increases. Also, it *prolongs the exposure* to security attacks.

Long term data preservation on Cloud platforms also need to address *data migration* between Cloud vendors in case the original vendor is unable to continue providing the service. Such large scale data migration also needs to migrate security and privacy policies and their enforcement mechanisms. The migration process itself has to be secured.

Cloud service providers distribute datacenters globally to ensure reliability, provide locality of services, and leverage incentives provided by local governments and power suppliers. This can potentially raise multiple *jurisdiction issues* with regard to data protection requirements and enforcement mechanisms. The life sciences domain has already encountered such issues with the HIPAA regulation[3]. Offering datacenter-specific access policies, or placing data at datacenters that meet the required user policy will be useful. In addition, there should be the ability to prove that such policies were enforced through audit trails for data access, and logging of policy violations through *provenance tracking* to assist with dispute resolution [18].

IV. Analysis of Application Characteristics

A. Application Services

A number of applications within the Smart Grid use the integrated information that is available. These information processing, analysis and power control services may be provided by the utilities and third party vendors for use by consumers, utilities and other third parties. These applications include demand forecast services for utilities, consumer usage analysis sites and mobile apps, home and building power management software, and information aggregation and sharing services. These applications may themselves be deployed across *Cloud and non-Cloud platforms*, employing their proprietary protocols. This makes it difficult to deploy a *common security architecture* across the Smart Grid ecosystem.

Data shared between these applications need to be secured and their privacy preserved. Smart Grid applications will have to be designed with security and privacy in mind. Data leakage becomes harder to contain once it leaves the confines of the utility's software and Cloud environment. Utilities may provide services and application platforms on public and private Cloud platforms that offer a *secure sandbox* within which third party applications can access restricted information from the utility and provide services to consumers.

B. Application Access

Smart Grid applications can be designed to be accessed as local executables, mobile applications and online websites and Web services. In addition, applications may also

[3]http://www.hipaa.org/

be shared as a virtual machine (VM) image that can be instantiated for a Cloud IaaS. These approaches provide different mechanisms for securely accessing the applications and ensuring data privacy.

Specifically, extensive work on Web services for eCommerce has led to standards such as WS-Policy[4], WS-Agreement[5], WS-Security, WS-XACML[6] and SAML[7] that can be used to negotiate service level agreements and monitor their enforcement. Some research on defining and executing service contracts has been done [19]. These can form part of a solution to protect information by the utilities.

Such Web services can be hosted on Cloud infrastructure or platform. In addition, application executables or websites may also be hosted in the Cloud. Cloud providers currently let applications, whether services or executables, define their own access mechanisms to these by external clients. 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.

C. Legacy and Emerging Applications

Utilities that are moving to Smart Grids often have legacy systems for meter data and customer information management in place. In addition, third party applications may be interacting with these existing applications. Moving to a Smart Grid software architecture will, in practice, necessitate co-existence of legacy and emerging applications since not all Smart Grid utilities can re-architect their entire system. Often, the existing systems run on mainframes or server farms.

In such cases, a security and privacy framework will have to be compatible with both new and existing applications. While the former will introduce new information, it will be integrated with existing information in the latter. Existing information policy enforcement, such as access control based on organizational hierarchy, will need to be migrated and operated across Cloud and non-Cloud platforms. This may be non-trivial, a number of security threats and vulnerabilities in the Smart Grid systems that arise from insecure legacy devices have been identified. This challenge can be mitigated by migrating legacy applications to VMs with identical configuration as the legacy system and running both the new and old software stack on Cloud infrastructure.

V. Analysis of Platform Characteristics

A. IaaS, PaaS, SaaS

Clouds are commonly categorized into Infrastructure, Platform and Software as a Service (IaaS, PaaS and SaaS), depending on what scalable abstraction and virtualization is provided: the compute and data resources, a development platform or working software applications respectively.

IaaS providers like Amazon[8] offer 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. Limited security and coarse grained access control is provided for IaaS storage and compute services. PaaS such as Microsoft Azure[9] provide access control and identity management like Active Directory as platform services in the Cloud. These controls can be applied to Cloud applications, Enterprise Service Bus, and storage services. Service providers are starting to host Smart Grid applications such as power usage monitoring for consumers (Google PowerMeter, Microsoft Hohm), and meter data management, demand response and outage detection for utilities (SilverSprings UtilityIQ [10]).

Migrating existing utility software and security policies into IaaS may be easier compared to the application rewrite that would be required for PaaS and SaaS. On the other hand, software vendors have started providing new software stacks customized for Smart Grid Utilities (Oracle Utilities [11], Microsoft SERA[12]), that have the potential to be hosted on Clouds. These may satisfy some of the regulatory requirements but sacrifice information integration from diverse sources. PaaS allow utilities to integrate their custom applications with platform access control and identity services, but may not provide the fine grained access control, audit tracing and regulatory compliance required by utilities. Most Cloud vendors only provide a best effort at security and privacy of data and compute services with limited legal liability for non-compliance [20].

B. Public, Private, Hybrid Clouds

Clouds can also be classified according to whether applications run on shared or exclusive Cloud infrastructure. Public Clouds provide multi-tenant services where more than one organization shares the same underlying hardware, with application and data separation enforced by the Cloud fabric. 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.

Public 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

[4]http://www.w3.org/Submission/WS-Policy/
[5]www.gridforum.org/documents/GFD.107.pdf
[6]http://xml.coverpages.org/Anderson-WS-XACMLv10.pdf
[7]http://saml.xml.org/

[8]http://aws.amazon.com
[9]http://www.microsoft.com/windowsazure
[10]http://www.silverspringnet.com/products/utilityiq_apps.html
[11]http://www.oracle.com/us/industries/utilities/
[12]http://www.microsoft.com/enterprise/industry/power-utilities/

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.

VI. Related Work

Security and privacy issues in Smart Grid have been discussed in the literature specially in the context of cyber physical systems. The differences between the traditional power grid and the Smart Grid has been studied to identify new vulnerabilities that arise [21], [22]. [23] categorizes attacks on Smart Grid into *network availability*, *data integrity*, and *information privacy*. [24], [25] provide a high level overview of security concerns in the Smart Grid and classifies concerns into three general categories, trust, communication and device security and issues due to complexity and scale at which Smart Grid will be deployed. Various literature identify and classify Smart Grid security and privacy concerns and their impact on deployment and general adoption [8], [17], [26]–[30]. They however do not delve into issues arising from an information-driven Smart Grid software architecture hosted on Clouds.

[29] implements Smart Grid security as a SaaS service, with all communication and data being passed through their access control and intrusion detection service. However, most of these identify and tackle specific aspects of security and privacy without taking a holistic approach. In particular, they focus on security but fail to sufficiently tackle the data privacy issues that stem from extensive information integration. Too, there has been limited discussion of issues specific to a broad deployments of Smart Grid Applications to Clouds.

Cloud researchers themselves have analyzed security and privacy challenges posed by Clouds in detail [31], [32]. Research to identify threat vectors arising from using Cloud infrastructure [33], [34], and privacy concerns have been studied separately. Risks of multi-tenancy in public Clouds are exposed in [35]. Among solutions, [36] proposes a user centric approach for privacy management while [37] promotes awareness of security during the application design phase. [38] defines Privacy as a service (PaaS) framework for ensuring user privacy and legal compliance of user data in the Cloud environment. Much of these surveys look at security and privacy concerns at large in the Cloud, and to our knowledge, there is no substantial perspective on specific issues related to the emerging area of Smart Grids that introduces unique challenges due to the distributed nature of its applications, information diversity and data sizes. While overlapping with some of the earlier analyses, our contribution lies in highlighting aspects specific to Smart Grid applications and novel security/privacy problems posed by them for Clouds.

VII. 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.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000192. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

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.

[16] R. J. Michaels, *Concise Encyclopedia of Economics*. Liberty Fund, 2001, ch. Electric Utility Regulation.

[17] The Smart Grid Interoperability Panel Cyber Security Working Group, "Guidelines for smart grid cyber security, v1.0 (3 vols.)," National Institute of Standards and Technology (NIST), Tech. Rep. NISTIR-7628, 2010.

[18] Y. L. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," *SIGMOD Rec.*, vol. 34, pp. 31–36, September 2005.

[19] P. Groth, S. Miles, S. Modgil, N. Oren, M. Luck, and Y. Gil, "Determining the trustworthiness of new electronic contracts," in *International Workshop on Engineering Societies in the Agents World X*, 2009.

[20] T. Espiner, "Cloud providers shrug off liability for security," http://www.zdnet.co.uk/news/compliance/2010/02/12/cloud-providers-shrug-off-liability-for-security-40037148/, ZDNet UK.

[21] F. Boroomand, A. Fereidunian, M. Zamani, M. Amozegar, H. Jamalabadi, H. Nasrollahi, M. Moghimi, H. Lesani, and C. Lucas, "Cyber security for smart grid: A human-automation interaction framework," in *IEEE Innovative Smart Grid Technologies Conference Europe*, 2010, pp. 1 –6.

[22] S. Clements and H. Kirkham, "Cyber-security considerations for the smart grid," in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, pp. 1 –5.

[23] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Military Communications Conference (MILCOM)*, 2010.

[24] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, pp. 81–85, 2010.

[25] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security Privacy, IEEE*, vol. 7, no. 3, pp. 75 –77, 2009.

[26] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in *IEEE Power and Energy Society General Meeting*, 2008, pp. 1 –5.

[27] A. Metke and R. Ekl, "Smart grid security technology," in *Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1 –7.

[28] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57 –64, 2010.

[29] W. Yanliang, D. Song, L. Wei-Min, Z. Tao, and Y. Yong, "Research of electric power information security protection on cloud security," in *International Conference on Power System Technology*, 2010, pp. 1 –6.

[30] G. S. Michael Echols, "Cyber security is now considered to be a critical component of keeping the lights on," in *Transmission & Distribution World*, 2010.

[31] H. Takabi, J. Joshi, , and G. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy*, vol. Nov.-Dec, pp. 24–31, 2010.

[32] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *ACM workshop on Cloud computing security*, 2009.

[33] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing." IEEE Computer Society, 2009.

[34] A. A. Friedman and D. M. West, "Privacy and security in cloud computing," in *Issues in Technology Innovation*, 2010.

[35] T. Ristenpart, E. Tromer, H. Shacham, , and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *ACM Conference on Computer and Communications Security*, 2009.

[36] A. Cavoukian, "Privacy in the clouds," *Identity in the Information Society*, vol. 1, pp. 89–108, 2008.

[37] S. Pearson, "Taking account of privacy when designing cloud computing services," in *ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 44–52.

[38] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in *IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 2009.