EPRI | ELECTRIC POWER RESEARCH INSTITUTE

TECHNOLOGY INNOVATION PROGRAM: SECURE CLOUD REFERENCE ARCHITECTURE FOR REAL-TIME UTILITY-BASED APPLICATIONS

December 2019

Introduction

Supervisory Control and Data Acquisition systems (SCADA) and microprocessor-based devices are used to manage time-sensitive applications and logic functions used to maintain reliability on the transmission and distribution grid. These real-time utility applications are the cornerstone systems of the technologies that operate the grid. The use of systems, networks and energy management applications have always been considered technologies that would remain under the tight control and management of the electric power organization.

However, this traditional belief is starting to change, in a recent testimony with the Federal Energy Regulatory Commission (FERC)[1], industry experts acknowledged the need for utilizing cloud service providers to manage grid data and to manage command and control functions. While many utilities may not have an urgent need to place real-time systems in the cloud today, there are expectations this capability should exist soon.

Therefore, this research focuses on expanding this concept and addressing the following questions:

- Which real-time grid applications and scenarios make sense to be used in the cloud?
- How regulatory compliance to the NERC CIP standards can be maintained while cloud services are being used for real-time grid applications
- What security tools and approaches are available to mitigate cloud-borne risks?

This report introduces cloud concepts and security approaches that are unique to off-premise cloud implementation and provides foundational considerations for reference architectures to manage cloud service provider deployments for grid-edge applications, low-impact BES Cyber Systems located in the cloud and managed security services for low impact BES Cyber Systems.

Key Scenarios Explained

While critical grid applications in the high and medium impact BES Cyber Systems [1] are not the focal point for this white paper, the approach is to field the issues at lower risk and impact levels to understand and identify the path forward to consider cloud service capabilities for higher impact levels in EPRI's 2020 Research.

Table of Contents

[1] *FERC Testimony, #pg no 152- https://www.ferc.gov/CalendarFiles/20190809142302-Transcript%20-%20062719ReliabilityTechnicalConference.pdf.*

For low impact BES Cyber Systems owners, the NERC CIP standards are of paramount concern when network and application architecture are designed to support them. Often, utilities will attempt to minimize any unnecessary compliance exposure by avoiding routable protocols and networks. While doing so, many solutions, especially those offered by cloud and managed security service providers have gone unapplied which could improve security and reliability if implemented correctly. The following lists examples of unapplied research:

- End-point protection validation
- Efficient Log monitoring, management and incident reporting
- Access point/firewall management
- Automated Threat Management and Threat Hunting
- Identify and access authentication

While many utilities are effective at these core security functions, it is important to understand which capabilities can be augmented by a third-party especially given that these solutions directly correlate to what is required by CIP-003-7 [2] for hundreds of substations and generation facilities.

The other key scenario explored in this paper is to identify how low impact BES Cyber Systems in Control Centers can be managed in the cloud. Two considerations will be explored here. The first is using SCADA-as-a-Service for low impact BES Cyber Systems for Distribution Substations. The second is utilizing cloud SCADAaaS model for emergency backup control center functions in the case wither primary or backup Control Center control systems functions have been compromised. In this case, EPRI research in Cloud for Data Storage [3] will be referenced.

Finally, this paper will address the security considerations for cloud service providers hosting grid-edge applications. EPRI has produced numerous papers on Distributed Energy Resources and Security which can be reference here below:

- EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-Based Approach for Network Design [4]
- Managing Integrated Distributed Energy Resources Programs: Communications, Cyber Security, and Architecture [5]
- Cyber Security Implications for an Integrated Grid [6]
- Prior to addressing the aforementioned scenarios, the first sections of the white paper will provide an overview of the key terms, technologies and security tools used in cloud deployments in order to illustrate how the utility, real-time applications could be applied to the cloud architectures.

Core Security Controls for Cloud Environments

Virtual Machines and Containers

In order to design and apply effective security architectures for grid related applications, this section describes the foundational terms and concepts that are core to cloud computing. Once the foundations have been described, this report in later sections will apply these concepts to utility-based applications use case. This section addresses the following core concepts:

- Virtualization
- Containers
- Virtual Private Cloud (VPC)
- Cloud Access Security Broker (CASB)
- Security recommendation for the above technologies, and SaaS, PaaS, IaaS service models.

Virtualization platforms are widely used within cloud environments to simplify operational processes which are otherwise resource exhaustive. Implementation of virtualization technology adds additional layers to the stack – software, hardware, storage, and services. While most virtualization platforms have reasonable security controls in place, others may not. Since most of the CSPs are using extensive virtualization technologies to enhance operational capabilities and also because utilities do not have control over or access to any hypervisor layers in the cloud, it is important to pay attention to this.

Containers are similar to VMs (see Figure.1) but have more relaxed isolation properties to share the host operating systems among the applications. They are considered lightweight as they have separate filesystem, CPU, memory, process space, and more. As they are decoupled from the underlying infrastructure, they are portable across clouds and OS distributions.

The utilization of hypervisors and containers varies across different cloud environments. For example, SaaS applications may be running on containers or other isolated resources whereas, IaaS and PaaS environments may have virtualization technology embedded.

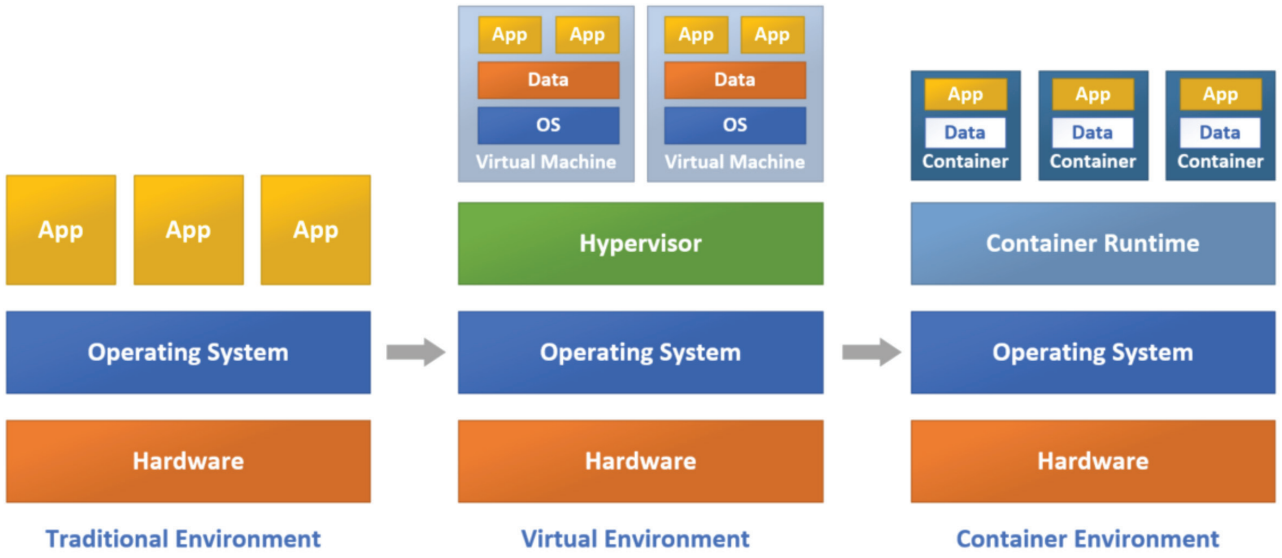

Figure 1: Traditional vs Virtual vs Container Environment

Multiple virtual machines with different host operating systems can run on a shared virtual hardware stack whereas multiple containers with different application can run on a shared operating system, hosted on a shared, virtual hardware stack.

Hardening VMs and Containers

VMs, Containers are often services offered by a CSP. In most cases, the CSP embeds security features within the components of a VM or a Container. These security features need to be validated against the security hardening guidelines provided either by the CSP or the Center for Internet Security (CIS)[2].

One of the security challenges related to virtual platforms is to identify the hypervisor platform provided by the CSP. With more information on the hypervisor. Utilities can better understand the threats and vulnerabilities associated with the platform. Utilities should also be able to evaluate CSP's process for mitigating threats if any occur.

Cloud Security Alliance (CSA)[3] Virtualization Security Recommendations

- Identifying virtualization platforms used at the CSP
- Virtualization-specific and internet security controls such as virtual firewalls, IDS
- Additional controls external to virtualization.
- Validation of VM images before using them.
- Handling patching of Hyper-V's and VM images.
- Ensure strong administrative control of VM environments in place.
- Inquire about segregation and separation of VM zones and types.
- Understand how multitenancy works and VM isolation is implemented. It is very critical to understand CSP's alerting procedures in case of any data breaches or zone breaches between isolated VM environments.

[2] *Center for Internet Security (CIS) is a non-profit entity that safeguard private and public organizations against cyber threats. The CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks.*

[3] *Cloud Security Alliance (CSA) harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products*

Container Security Best Practices

Containers are considered to be light weight and provide faster performance than VMs but, they're more vulnerable than VMs. Since they run on a shared OS, any vulnerabilities in the OS may result in compromise of all the containers running on it. Each container is a bundled application package which requires access to code repositories to install and configure software packages. If the repository or the software package installed contains malware, the container and its OS may be compromised. Here are a few best practices to secure containers:

- **Image Provenance** – A secure labeling system can be in place to identify the containers' source and origin.
- **Image Scanning** – A security gateway or a SeCaaS offering which includes HIDS/HIPS or anti-malware can be installed to automatically scan the OS images for vulnerabilities. Repositories should be taken from trusted sources and its contents need to be validated prior to installation on container. Container images should also be validated at various stages of the software development cycle including Continuous Integration/Continuous Deployment (CI/CD).
- **Auditing** – The environment hosting the containers should be regularly audited to ensure all containers are based on up-to-date images and both hosts, and containers are locked down to meet organizational standards.
- **Isolation and least privilege** – Containers run with the minimum resources/privileges needed within the runtime environment. By default, the resources are open to all so, it is critical to follow the least privilege rule and explicitly isolate the container resources from one another and also the underlying OS.
- **Runtime Threat Detection and Response** – Enable capabilities that detect active threats against containerized applications in runtime and automatically respond.
- **Immutability** – If an existing container requires a change or an update, the best practice is to destroy the existing version and create a new version to make changes. This approach will reduce vulnerabilities, malware injections resulting from updating applications or application packages in the container.

Virtual Private Cloud (VPC)

A Virtual Private Cloud (VPC) is a more isolated environment that leverages hypervisor controls to keep a utility's data and operations separate from each other. This virtual segmented model allows CSP's more flexibility to easily segregate Utilities' assets and deployments.

The isolation between a VPC belonging to a utility and other VPC's belonging to a different utility is achieved through virtual network segmentation such as Virtual Local Area Network (VLAN) or a set of encrypted communication channels, accompanied with VPN allocated per VPC user. It is mostly used in IaaS environments, with public cloud infrastructure.

Every VPC's resources are isolated from other VPCs but provisioned and connected globally. To separate resources based on regions within a VPC, subnets can be created for each zone.

Cloud Access Security Broker (CASB)

As discussed in the earlier sections, all the cloud service models are based on the shared responsibility model. In case of SaaS, even though CSPs own the underlying hardware and software infrastructure, which utilities cannot access, utilities would still need to meet security and compliance requirements. To overcome these challenges, a Cloud Access Security Broker (CASB) can be implemented, which acts as a middleman (see Figure 2.) between the CSP and the utility to meet security, compliance requirements.

CASB can be an in-house gateway device or a cloud-based security service such as Security as a Service (SecaaS). SecaaS is a cloud-based model to outsource complex security functions to a Managed Security Service Providers (MSSP). SecaaS solutions provide the capabilities of in-house security team, within the cloud environments. A few examples of such offering are data protection, identity and access management, logging, HIDS/HIPS, firewalls, Business Continuity and Disaster Recovery (BC/DR or BCDR).

Depending on the security requirements for a cloud-based application, Utilities' can define security policies and controls to ensure the security of their cloud applications and data transmitted to the cloud. CASBs can help monitor cloud applications and data using a combination of URL inspection, traffic and protocol analysis (similar to in-house proxy), and data loss prevention (DLP) pattern matching.

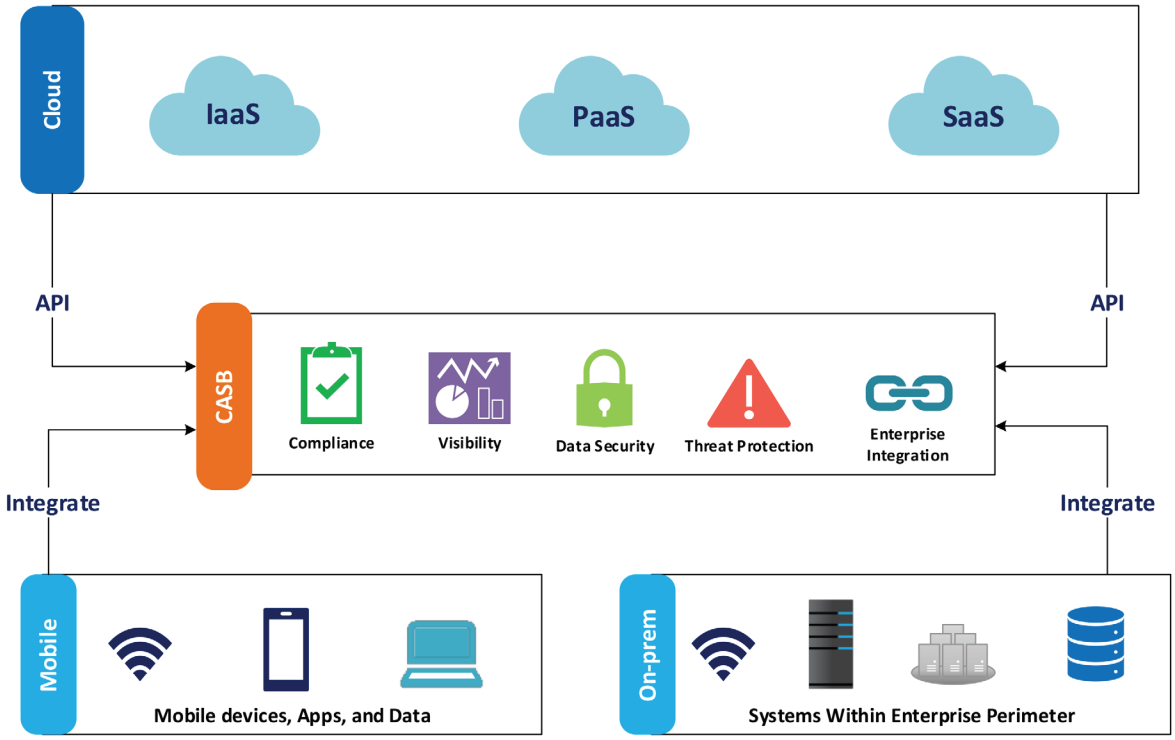

Figure 2: Cloud Access Security Broker (CASB) Architecture Model

Data Protection

CASBs may offer data protection controls such as encryption, tokenization, substitution. Utilities should carefully evaluate key management capabilities and practices with any CASB where they intend to implement encryption and decryption of data. It is important to note that Utilities need to minimize access to keys and scrutinize CASBs to ensure that they are not a man-in-the-middle.

Threat Protection

CASBs have the ability to monitor network traffic for indicators of malware and compromise by looking for behavior patterns.

Access Controls

Few of the CSPs may offer integration with on-prem user directories such as Active Directory, for identity and access management. In such cases, a CASB may help Utilities extend their existing security controls for on-prem identity and access management such as role-based access management, multi-factor authentication and audit log trails of user access, to the cloud-based services. *CASBs may be integrated with other cloud services, features, so utilities should carefully evaluate their partnerships when considering these services.*

SaaS Security Recommendations

- **Visibility** – Gain visibility into user activity, devices connected, and data being sent to the cloud.
- **Data Protection** – Protect data when stored, processed, and transported in the cloud.
- **Access Control** – Limiting access from unmanaged devices, preventing illicit access, locking down admin access for cloud deployments.
- **Compliance** – Regulatory mandates for IP, PII, PCI, PHI, CIP standards, and legal eDiscovery requests.
- **Detection and Response** – Detecting compromised accounts/systems and identifying anomalous behaviors in the cloud.

Application Security Best Practices

Security of all SaaS applications is entirely managed by the CSP. It is recommended to investigate the type of security functions built into the applications by the CSP. The best practice would be to follow the recommendation provided by the Cloud Security Alliance (CSA), listed in the next section.

Cloud Security Alliance (CSA) Recommendations for Application Security

1. Threat modeling components should be inherent in the Software Development Life Cycle (SDLC).
2. Application assessment tools like application scanners, static/dynamic code analysis should be integrated with development environments.
3. Any changes in the application architecture should be reflected in the SDLC as well.
4. Strong trust boundaries should be in place at the CSP, including the standard separation between development, staging, and production areas. Utilities' platform and hosting areas should be treated with care and isolated from internal development.
5. Use trusted VMs and harden them as discussed in the previous section.
6. Secure interhost communications with encryption or IPSec tunnels.
7. Manage and protect application credentials and keys. This includes usernames, passwords, encryption keys, and any other means used to authenticate systems and application components.
8. Application logs and debugging information may contain sensitive information so, they should be treated as sensitive information and be protected using cryptography, DLP tools, etc.
9. CSPs should support web application tools used for applications hosted on their platforms.
10. Get permission for vulnerability scans but ensure to put a strict process in place so that other application hosted on the same platform are not impacted by the scans.

PaaS Security Recommendations

The underlying infrastructure in a PaaS environment such as hardware, networking, virtual machine, operating system is owned and operated by the CSP. Utilities can host their applications and store application related data on this platform. The foremost salient aspect of protecting any PaaS offering is to secure the application components and the underlying OS. Utilities' level of control on OS depends on the PaaS environment setup. In case of limited control of OS, it is very critical to focus on application-level security.

Most of the PaaS providers may not support built-in network access controls like firewalls so, organization defined access controls would play a major role. A few best practices for access control in PaaS environments would include strong authentication, role-based access control and following least-privilege access rule even for admin users. The CSA recommendations for application security would apply to PaaS applications as well. All application components such as libraries, packages in use by performing scans and penetration tests. The underlying operating systems should be regularly patched and secured.

In addition to the organization-defined access controls, it is important to evaluate the access controls offered by the CSP to ensure that they align with the controls employed. PaaS environments may also involve container technology, which may add more security concerns, discussed in the further sections.

The utility would be responsible for any vulnerabilities existing in the application packages. To ensure the confidentiality and integrity of the code being deployed, Utilities may leverage security, service management APIs or additional security controls such as application monitoring, application firewalling offered by the CSP.

IaaS Security Recommendations

IaaS technology stack (see Figure 3.) is an interoperable group of individual components and layers that hook together in much more in-depth ways, and most of it is software-defined and virtualized. Every component in this technology stack can be isolated and controlled separately, and so can their security. At the same time, APIs and tools used for infrastructure integration may introduce some security concerns. Utilities may have the ability to control anything above the OS layer in the stack but not the hypervisor or its underlying components.

In IaaS, Utilities can only define logical security controls as they can only access the virtual environment.

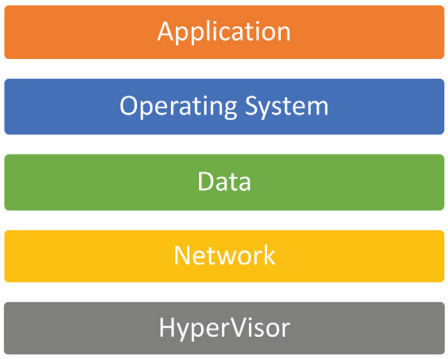

Figure 3: IaaS technology stack

Hypervisor Security

The security recommendations for hypervisor have been discussed in the earlier section**.** Public cloud models are based on multi-tenant architecture, which restricts utilities from having the ability to control the hypervisors. For a private, hybrid cloud models, utilities may have the ability to manage hypervisor security by performing activities such as patching, configuration management, and access management.

Network Security

Utilities may use logic network controls for all network layer (OSI layers 2-7) by placing firewalls, VLANs, routers with Routers with Access Control Lists (ACLs) to protect the resources in the technology stack (see Figure 3.). Backup and redundancy techniques offered by the CSP can be used to ensure network availability at all times. By segregation of software defined networks into zones, placing services belonging to different environments in those zones, can help utilities keep certain types of infrastructure separated and limit communication between them.

Data Security

Ensuring confidentiality and integrity of data being transmitted in and out of utilities' premises, and data stored in the cloud remains a concern. This may require cryptography or other robust data protection techniques to be applied. For a utility it is important to classify the types of data that can leave their premises versus those that cannot. Prior to storing or transmitting data to the cloud, the best practice for a utility would be to design a data lifecycle for cloud, based on data classification. Managing data storage in the cloud has been discussed in one of our previous research results [3].

In addition to the data security strategy applied by the organizations, CSPs may offer some native data security tools for performing Data Loss Prevention (DLP), data retention, and disposal. A CASB can also be implemented for checking quality and integrity of data inbound and outbound of Utilities' premises.

Operating System Security

Hardening of host OS is very critical for both IaaS and PaaS models. The key difference is that in IaaS, utilities would have control of the operating system, giving them the ability to lock it down in case of a compromise. Even though the virtual machine images are provided by the CSP, utilities would be responsible for patching and configuration management on a regular basis.

Application Security

Given the level of exposure in the cloud, applications should be as secure and bulletproof as possible. The CSA's security recommendations for application security would apply to IaaS applications as well.

Logging

Utilities may need to constantly monitor all admin accesses and changes within the IaaS environments. If the logging capabilities provided by the CSPs are not adequate, it is always recommended to request for additional logging capabilities to extensively monitor all the resources within the environment.

Scenario 1: Low-Impact Network Security, Security Monitoring and Access Controls in the Cloud

As Utilities are evaluating the possibilities of cloud-based operations, one key area to begin their evaluations is for network access control and monitoring for low impact BES Cyber Systems. For this category of systems, the CIP Standards are less extensive and can allow a simpler path for 3rd party CSPs to provide offerings that would enable effective security features while complying with the CIP standards. This scenario is based on CIP-003-7 [2], Reference Model 3 – Centralized Network-based Inbound and Outbound Access Permissions. According to NERC's reference model, the device performing electronic access controls need not necessarily be located inside the asset containing the low-impact BES Cyber System. The key aspect of this scenario is to manage network access controls for inbound and outbound access permissions between the

asset containing low-impact BES Cyber System in a Control Center and the low-impact BES Cyber Systems in Substations. (CIP-003-7 Attachment A [2]). The following attributes will be considered:

- Sites that contain ow impact BES Cyber Systems
- Network connectivity to the low impact sites
- Network access control to the low impact sites
- Network access monitoring to low impact sites

As described in Figure.4, and system definitions, the systems performing the controls pertinent CIP-003-7 [2] are located within the CSP. Similar to how network carriers are used, in this case the CSP provider executing controls within the Cloud Environment. The individual substations or low impact sites are located and managed by utilities, but the network access control functions can be managed in the cloud. Detailed service level agreements would have to be written manage some of the procedural and administrative aspects of the standards applicable to low impact BES Cyber Systems.

Requirements for Cyber Security Plan(s) for Assets Containing Low Impact BES Cyber Systems [2]:

1. **Cyber Security Awareness** – Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
2. **Physical Security Controls** – Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to
   a. The asset or the locations of the low impact BES Cyber System within the asset, and
   b. The Cyber Asset, as specified by the Responsible Entity, that provide electronic access controls implemented between a low impact
3. **Electronic Access Controls**
4. **Cyber Security Incident Response**
5. **Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation**

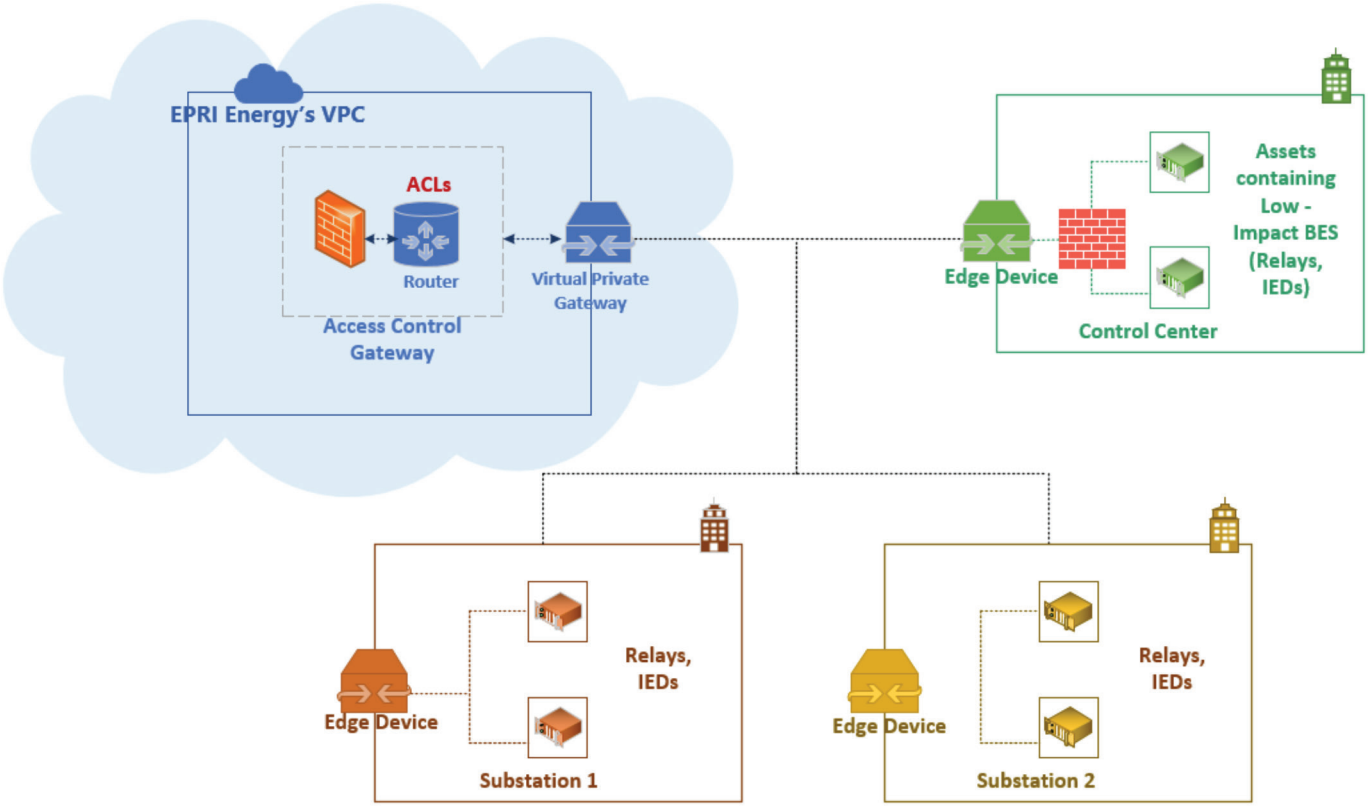

Figure 4: Cloud-based architecture for low-impact network security, security monitoring and access controls

Architecture Design

The architecture in figure describes a scenario where EPRI Energy uses a Cloud Service Provider's (CSP) Platform-as-a-Service (PaaS) model to remotely host the services. The shared responsibilities between the utility and the CSP for managing VPC, VPG, Edge Device remain the same as described earlier.

EPRI Energy Defined Platform in the Cloud:

- **Access Control Gateway** – Router with ACLs, firewall to remotely control inbound and outbound network access between assets containing low-impact assets in a Control Center and the low-impact assets in a substation.

Functional Requirements

The informed cloud-based architecture allows utilities to place this security device in the cloud, which controls inbound and outbound access permissions between the asset containing low-impact BES Cyber System in a Control Center and the low-impact BES Cyber Systems in Substations.

Functions Managed in the Cloud

Centralized network management through gateways, firewalls, and Access Control Lists (ACLs). CSP's Virtual Private Gateway can be connected to utility's in-house VPN concentrator to gain greater visibility and control over users accessing remote sites via the access control gateway.

Operational Benefits

It provides the ability to manage access to remote sites through a centralized location.

Scenario 2: Cloud-Based Data Concentrator/ Substation Gateway

Substation data concentrators or gateways can perform centralized access control, password management, and content management (relay settings and firmware management). They are typically located at substations. The goal of this scenario is to provide a mechanism for utilities to centralize the access and management of substation devices and relays through a centralized system or application. This section describes the cloud-based architecture to support this function.

Given that Bulk Electric System substation have specific NERC CIP Regulatory considerations, it is important to note that this scenario is only applicable to low impact, where the regulatory requirements for the CIP standards are more manageable for the CSP to achieve in coordination with the Registered Entities. This solution is not recommended for medium impact or CIP-014 substations. For low impact scenarios, the fictitious EPRI Energy VPC described in the diagram below would be considered a low impact BES Cyber System. All regulatory requirements applicable to low impact BCS would be applicable and compliance would be shared responsibility between the Registered Entity and the Cloud Service Provider.

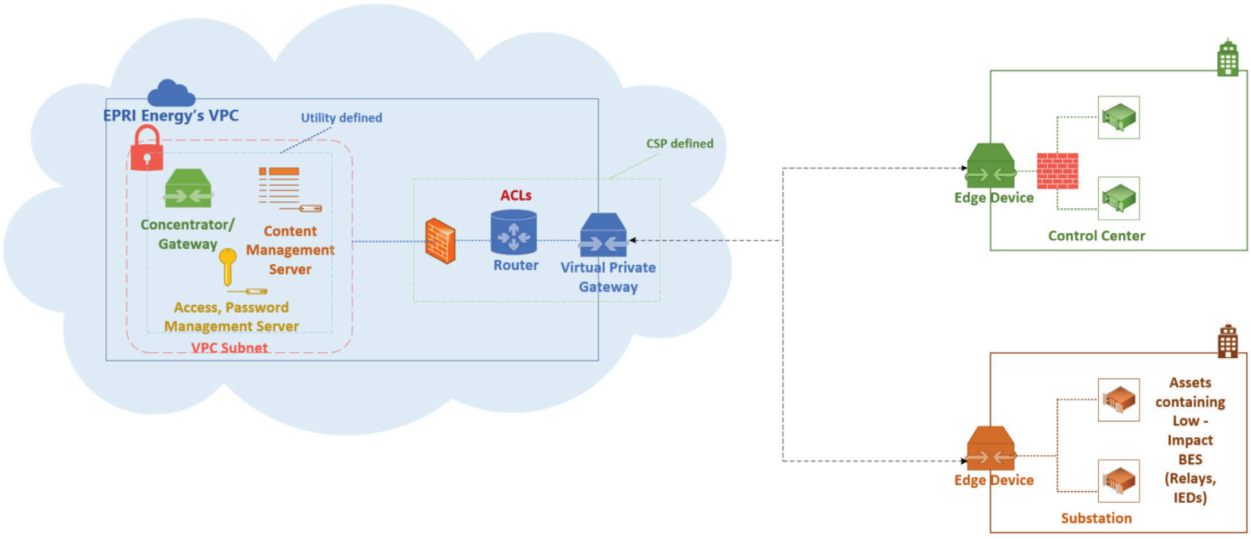

Figure 5: Architecture for cloud-based data concentrator/substation gateway.

Architecture Design

The architecture in figure describes a scenario where EPRI Energy uses a Cloud Service Provider's (CSP) Infrastructure-as-a-Service (IaaS) [3] model to remotely hosts the services. Since a utility does not own or operate the underlying infrastructure for an IaaS model, it is important to understand the coordination of security and compliance responsibilities between the utility and the CSP.

- EPRI Energy has defined a VPC within a CSP's cloud region to have isolated resources.
- Within the defined VPC, resources can be held in different subnets to keep the resources in one subnet isolated from the other.
- EPRI Energy can route and control access to/from this VPC by using a Virtual Private Gateway (VPG). The traffic coming in through the VPG is further filtered using router containing custom Access Control Lists (ACLs) and firewall.
- Any communication between the VPC subnets is controlled by the router based on the ACLs defined by EPRI Energy.
- Edge devices at the utility premises, such as individual substations and control centers, secure communication between them and the cloud.

EPRI Energy Defined Infrastructure in the Cloud:

1. **Concentrator/Gateway** – A virtual machine that gathers alarm data, device settings and activity logs from different devices of a substation.
2. **Content Management Server** – A virtual machine that performs configuration management for multiple devices of a substation.
3. **Access/Password Management** – A virtual machine that manages passwords and controls access to multiple devices of a substation.
4. **VPG offered by CSP** can be connected to an in-house VPN concentrator/edge device, physically located at substations, control centers to control remote access to the services in the VPC under dedicated subnets.

Functional Requirements

The informed cloud-based architecture allows utilities to perform these security functions from a centralized, remote infrastructure in the cloud. This allows utilities to gather alarm data, activity logs, perform centralized configuration and access management for assets containing low-impact BES Cyber System in a Control Center and the low-impact BES Cyber Systems in Substations.

Operational Benefits

These security functions can be performed in the cloud environment to gain visibility over low-impact sites, substation managed and operated within the utilities.

Scenario 3: Grid-Edge Applications in the Cloud (Non-CIP Applicable Assets)

In this architecture, the primary goal is to provide buffers to the utility environment by leveraging cloud architectures to improve the integrity and security of untrusted field assets that may support grid-edge applications like distributed generation services, electric vehicle charging infrastructure and energy storage. In each of these cases, given that thresholds of beneath that of what constitutes a BES Cyber Asset, a utility has a wide range of options to consider to security this environment. The section describes the foundational aspect of this category of systems used in a cloud environment.

Architecture Design:

The architecture in the figure describes a scenario where EPRI Energy hosts a Data Aggregator service and gird-edge applications in the cloud. This can be considered as a hybrid cloud-based architecture.

Components:

1. Grid-Edge devices such as Electric Vehicles (EV), Photovoltaics (PV), Smart Meters, Battery Storage
2. Third-party data aggregator: Few grid-edge devices may communicate with only a specific data aggregator provided either by a third-party or the device manufacturer.
3. CASB: Acts as a middle-man between the field devices, third-party aggregator and the utility.

EPRI Energy Defined Applications in the Cloud:

1. **Data Aggregator** – A real-time database that collects and caches data from different field devices.
2. **Grid-Edge applications for microgrid, EV, Distributed Energy Resources (DER), Battery storage, PV, Demand Response and Load Management** can be hosted as real-time containerized applications using the data gathered from the cloud-based data aggregator or a third-party data aggregator.

The architecture components are categorized into the trusted, semi-trusted and untrusted zones for traffic flows to identify the security controls needed for each zone. The utility premises are highly trusted zones as they have complete control over traffic flows in and out of their premises. The traffic flows through the cloud infrastructure and the third-party aggregator platform can be considered as semi-trusted since there exists a shared responsibility model between the service provider and the utility in both the cases. The field devices can be considered as untrusted as they are not secured.

Based on these trust zones, the recommended security functions to be performed by the CASB (see figure) in this scenario are:

- Perform data quality and integrity checking over any data inbound and outbound to the cloud.
- Authentication of field devices prior to establishing communication with them.
- Perform end-to-end encryption over any data that is exchanged.
- Monitor the cloud infrastructure through a secured interface.
- Gather device tamper notifications from the field devices and alert the cloud-based data aggregator, utilities.

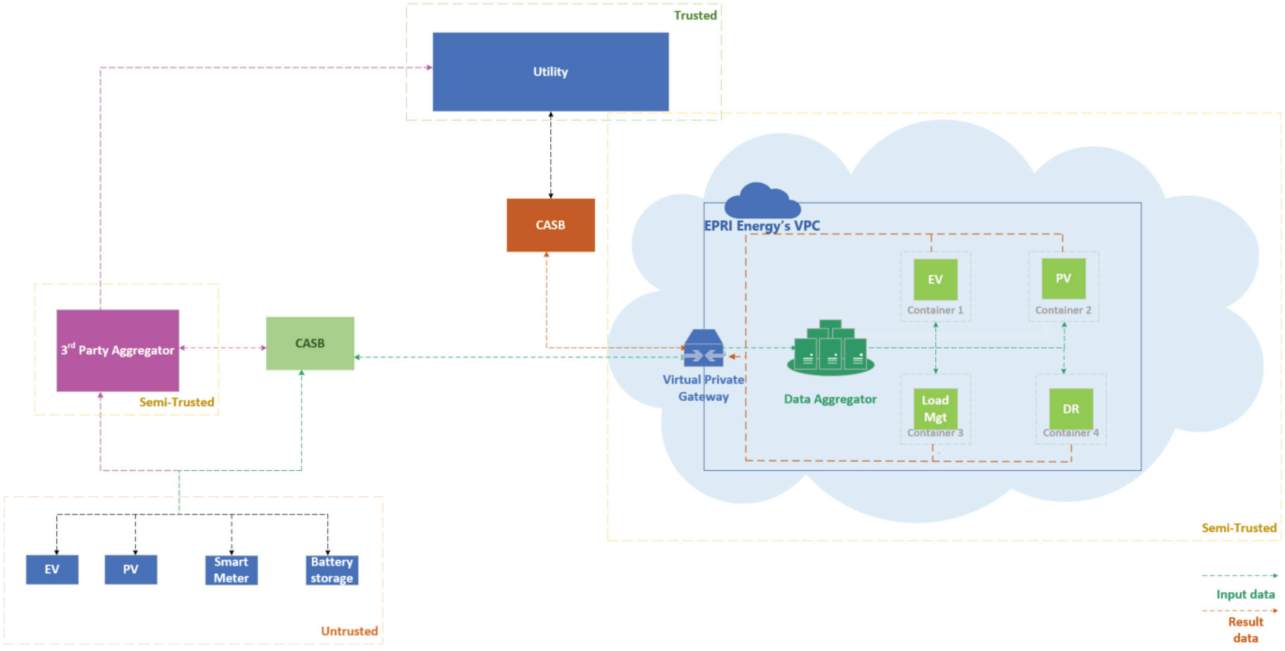

Figure 6: Architecture for Grid-Edge applications in the cloud (trust-zone model)

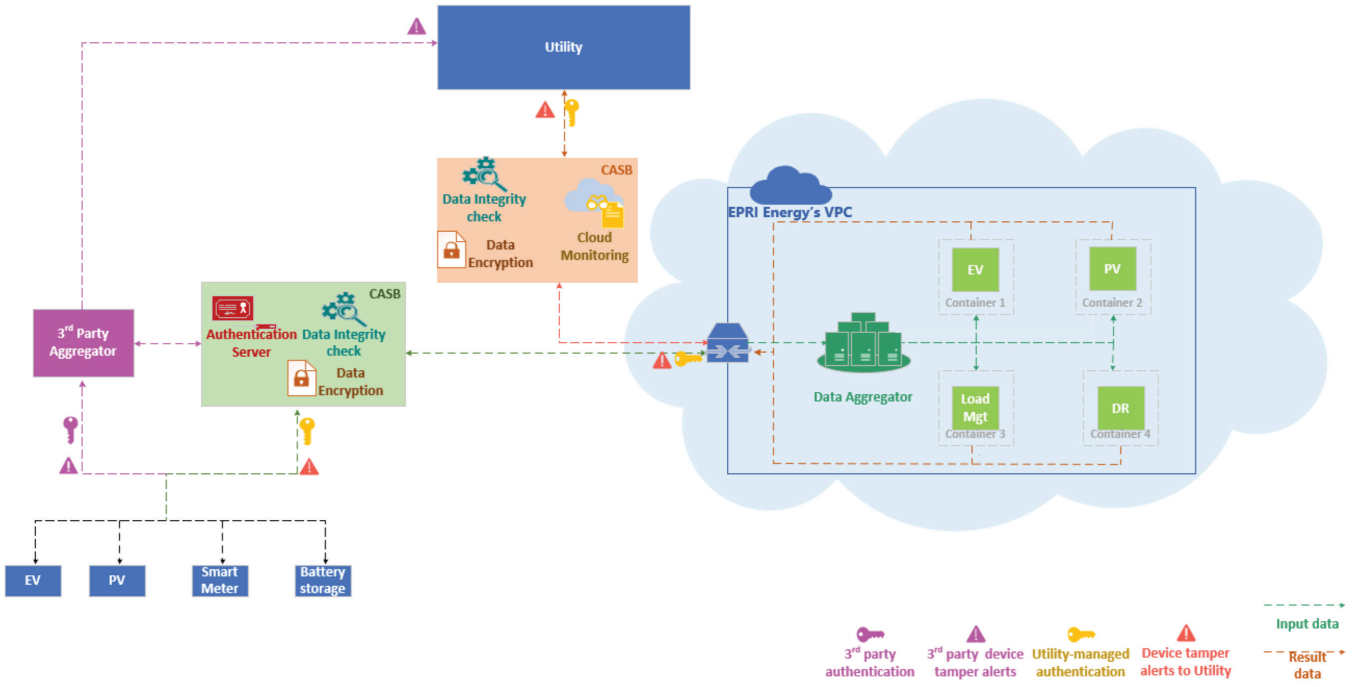

Figure 7: Secure architecture for Grid-Edge applications in the cloud.

Operational Benefits

The informed cloud-based data aggregator is an enhancement to the current data aggregator platforms as it allows to host the corresponding grid-edge applications on the same platform thereby reducing the need for a third-party aggregator. Delays and latencies in real-time data processing can be minimized by leveraging the advanced real-time database/cache technologies offered by the CSP. Each of these grid-edge applications can be hosted in a containerized environment which allows Utilities to run multiple applications within a container reducing memory, processing times.

Scenario 4: SCADA-as-a-Service for Low-Impact Systems (for Small to Medium Sized Utilities)

For this scenario, the CIP Standards would heavily impact the options for this environment. Given the regulatory impact, this report only addresses the scenario applicable to low impact BES Cyber Systems. EPRI is working on solutions for medium and high impact for 2020. This scenario would be most applicable to utilities prioritizing cost improvements.

Architecture Design

The architecture in figure describes a scenario where EPRI Energy uses a Cloud Service Provider's (CSP) Platform-as-a-Service (PaaS) model to remotely host Distribution Management System (DMS) and Front-End Processor services. The shared responsibilities between the utility and the CSP for managing VPC, VPC Subnet, VPG, and Edge Device remain the same as described earlier.

EPRI Energy Defined Platform in the Cloud:

- **Front-End Processor** – A real-time database that collects data from remote distribution substation sites containing low-impact BES Cyber Systems and communicates with the DMS.
- **DMS** – A virtual machine that processes the data sent from front-end processor and provides remote access to Operator and Engineering Workstations in the Control Center.

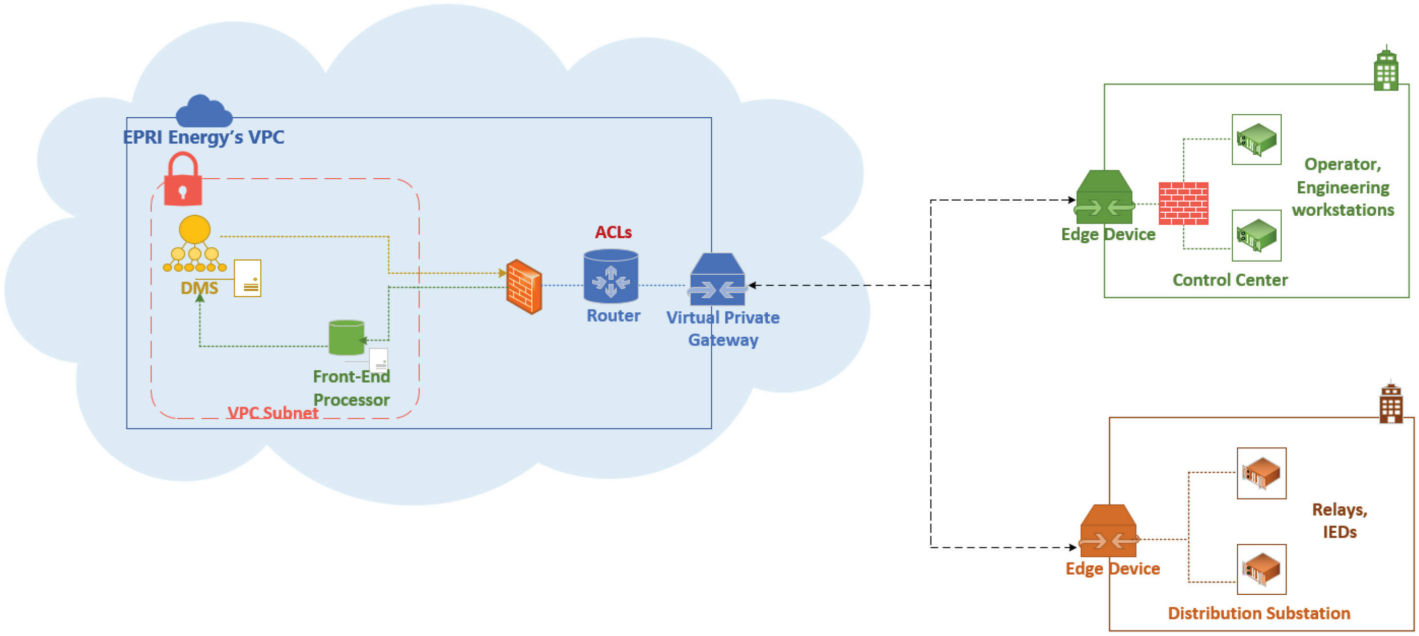

Figure 8: SCADA-as-a-Service for Low-Impact Systems

Functional Requirements

The informed architecture allows small to medium-sized utilities to authenticate Distribution Substation devices, allow users to access Operator and Engineering Workstation's DMS via the cloud-interface.

Functions Managed in the Cloud

A CSP's Virtual Private Gateway (VPG) can be connected to utility's in-house VPN concentrator to gain greater visibility and control over users accessing remote sites via the access control gateway. Network firewalls, Router containing ACLs can be used to secure inbound and outbound communication between VPC subnets. Perform end-to-end encryption for data in and out of the cloud.

Operational Benefits

It provides the ability to remotely authenticate distribution substation devices such as RTUs, PLCs, IEDs, Relays. It also allows users to remotely access the cloud applications (DMS, Front-End Processor) through the VPN connection established between the Edge Device and the VPG.

Key NERC CIP Considerations

1. Do not exceed low impact thresholds – once more than 1 asset is controls on the BES, the SCADA Control Center becomes at least a medium impact. Generally, this solution should only be used for sub-transmission and distribution SCADA at the low or no impact levels.
2. Ensure the cloud service provider can meet all of the controls and can provide evidence of compliance upon request
   a. *Cyber Security Awareness* – Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices).
   b. *Physical Security Controls* – Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to
      – The asset or the locations of the low impact BES Cyber System within the asset, and
      – The Cyber Asset, as specified by the Responsible Entity, that provide electronic access controls implemented between a low impact
   c. *Electronic Access Controls*

d. *Cyber Security Incident Response*

e. *Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation*

6. Label the cloud-based SCADA system as a low impact BES Cyber Asset and manage it consistent with the CIP standards for low impact BCS.
7. Manage and control access to the low impact, cloud-based SCADA system as if was housed locally. Engineering and operator workstation can reside either locally or remotely accessible to the hosted environment.

Conclusion

Each reference architecture and scenario addressed in this report represent key recommendations for implementing cloud computing securely for real-time grid applications. Three primary considerations should be addressed before designing the aforementioned solutions:

Understanding the Regulatory Compliance Impact

This report, while represents plausible reference architectures for consideration when implementing cloud computing for real-time grid applications, is not devoid of regulatory implications. In fact, most of the recommendations that address low impact environments, will require a thorough coordination with NERC and possibly the Federal Energy Regulatory Commission to validate proposed cloud-based designs and architectures. While this paper attempts to address concerns that tackle compliance challenges with the NERC CIP standards, the technical considerations included should provide industry a solid baseline to formulate more robust strategies to securely apply the benefits of cloud computing. This can be done through correspondence with Compliance & Enforcement Authorities or via the Implementation Guidance process[4] defined by NERC.

Cloud Providers are Inherently Different

While several of the main cloud service providers were open to sharing their ideas and concepts with us, none of the recommendation included in this report reflects a specific cloud service provider. The controls and environment depicted are derived from interviews, reference material and documentation associated with cloud vendors, but sanitized to ensure that EPRI was not endorsing any one solution. It is recommended that the systems and applications that a utility considers using within a cloud environment are discussed in detail with the CSP to ensure they can meet both technical and regulatory requirements.

Identifying the Applications to be Leveraged by Cloud Service Providers

Real-time applications are not all designed in the same manner within utility environments. Before contacting a cloud service provider, it will be important to understand the application, security and data needs of the enterprise's system in question. While some applications such as transmission planning software for meter data already resides in the cloud for several utilities, the applications described in this report are not fully embraced by the utility community to be managed in an off-premise approach. It will be essential that the system and data owners agree to the potential cost or operational benefits to be achieved before engaging a CSP. Once the cost and operational benefits are defined for the application, security and compliance considerations will need to be developed and clearly described. The security and compliance recommendations included in this report can be used as a guide to facilitate the discussion with CSPs and Compliance and Enforcement Authorities.

References

1. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf
2. https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-003-7&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls&jurisdiction=United%20States
3. https://www.epri.com/#/pages/product/000000003002015657/?lang=en-US
4. https://www.epri.com/#/pages/product/000000003002014321/?lang=en-US
5. https://www.epri.com/#/pages/product/000000003002016781/?lang=en-US
6. https://www.epri.com/#/pages/product/000000003002013699/?lang=en-US

[4] *NERC Implementation Guidance process- https://www.nerc.com/pa/comp/guidance/Pages/default.aspx*

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together . . . Shaping the Future of Electricity

.

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

Note

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

EPRI RESOURCES

Tobias Whitney, *Technical Executive*
650.855.7918, twhitney@epri.com

Alekhya Avadhanula, *Engineer - Cyber Security*
650.855.8552, aavadhanula@epri.com

Cyber Security

3002017577

December 2019

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com