A secure cloud migration, monitoring and analytics framework for Industrial Internet of Things

A Secure Cloud Migration, Monitoring and Analytics Framework for Industrial Internet of Things

Rafiullah Khan, Kieran McLaughlin, BooJoong Kang, David Laverty and Sakir Sezer
Queen's University Belfast, Belfast, United Kingdom
Email: {rafiullah.khan, kieran.mclaughlin, b.kang, david.laverty, s.sezer}@qub.ac.uk

***Abstract*—The fourth industrial revolution combines cutting-edge technologies such as Industrial Internet of Things (IIoT) and cloud computing. However, this inevitable revolution faces challenges due to the presence of legacy equipment in industrial systems. Legacy equipment hinders the adoption of emerging cloud technologies due to data privacy, security and interoperability issues. This paper proposes a secure cloud migration approach for industrial systems and investigates whether it can meet real-time control system requirements without compromising system safety and security. The proposed approach is generic enough to be applied for different industrial sectors with minimal interruption to operations during the cloud migration process. Due to the large number of IIoT devices, manual system monitoring to pin-point issues is a tedious and time-consuming task. This paper also proposes an automated monitoring and management framework for large complex IIoT network that tracks and reports issues using different forms of notifications. Experimental validation on a real microgrid testbed facility concluded that the proposed approach is promising for time-critical industrial systems.**

I. Introduction

Industry 4.0 promises increased efficiency, quality, higher productivity and countless value creation opportunities. Due to the critical nature of industrial operations, such a paradigm shift in technology is hindered due to security and data privacy challenges. Industrial devices typically have a lifespan of several decades and rarely receive security patches or updates, often to avoid breaking critical operations. Legacy devices are critical industrial assets and are cost-prohibitive to replace. Specifically, power systems have deployed a large quantity of phasor devices (i.e., Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs)) since the 1980s. Most phasor devices are based on the IEEE C37.118 standard that lack even basic security features [1]. Due to outdated and insecure protocols used by legacy equipment, a low-cost cloud migration approach needs to be investigated while ensuring system safety and security.

Due to the size and complexity of an Industrial Internet of Things (IIoT) network, it is a tedious and time-consuming task to manually monitor the state of devices and availability of services. A device or service may crash, overload or become unavailable due to cyber attack or misconfiguration. Thus, an automated and scalable network monitoring and management solution needs to be investigated for tracking, troubleshooting and pin-pointing issues in the IIoT.

A. Related Work

Security and data privacy are the major challenges in industry modernization [2]. Several cyber-security incidents have been reported in the last few years on critical national infrastructures such as the Ukraine blackout and Stuxnet [3], [4]. The root cause for most cyber-security incidents is the presence of legacy equipment with weak security [1], [5], [6].

Recent cyber-attacks on Industrial Control Systems (ICS) have exposed critical vulnerabilities highlighting that current security solutions and network architectures are insufficient to protect industry 4.0 [7]. Thus, new techniques need to be investigated to overcome vulnerabilities particularly those emerging from the presence of legacy devices and technologies. To bridge the technological gap between legacy and state-of-the-art equipment, authors in [8] proposed a low-cost gateway with protocols translation feature. Authors in [9] proposed a middleware that runs on the legacy device as well as the control application to ensure mutual authentication, encryption and communication integrity. However, presented works [8], [9] do not address cloud migration of legacy ICS equipment.

Challenges in migrating ICS equipment to the cloud have been identified by several researchers [10], [11]. Authors in [12] used a local PC with Windows OS in the middle between the Programmable Logic Controller (PLC) device and the cloud. The proposed work uses Windows Communication Foundation (WCF) and Azure IoT Hub to control ICS operations from the cloud. The presented work raises scalability concerns by attaching a Windows PC next to each ICS device. Authors in [13] proposed access control models for the cloud platform. It allows the latest devices to securely communicate directly with the cloud but does not address legacy devices. Authors in [14] proposed a cloud-based framework for connecting different industrial manufacturing sites. Each site has a local server that receives commands from the cloud when a customer places an order online. However, the presented work does not migrate control of each ICS device to the cloud.

B. Paper Motivation and Contributions

The current research trend primarily focuses on developing new ICS devices specifically for the cloud [13], [14]. However, legacy devices are critical assets of industry and are cost-prohibitive to replace. Thus, the underpinning motivation of this paper is to develop a cloud migration framework that

can also apply to legacy devices with obsolete communication protocols. The proposed cloud migration approach is designed to be scalable with following key features: (i) the architecture is inherently secure, (ii) supports legacy devices with reduced risk to system security, (iii) operates plug & play with no or minimal interruption to ICS operations during cloud migration, (iv) improves infrastructure-wide system visibility, and (v) provides automated monitoring of system infrastructure with enhanced issues tracking and management.

This paper proposes an architectural design for securely migrating ICS to the cloud. It investigates necessary features for key architectural components to ensure the secure integration of legacy equipment. The proposed approach is implemented and validated for synchrophasor technology in the smart grid, considering distributed generation as a use case scenario. Synchrophasor technology uses phasor devices (PMUs, PDCs) for real-time control and monitoring in the smart grid. Due to the potentially large number of phasor devices deployed in power systems, manually monitoring, troubleshooting or pin-pointing system issues is a challenging task. Thus, this paper also proposes an automated and scalable network monitoring and management system which periodically scans the entire system for any failing component, device or service. As IIoT infrastructure is normally geographically distributed, the proposed monitoring system is integrated with an open-source web-based Request Tracker (RT) framework. It has user accounts for operators in different regions, each with defined rights and responsibilities. An operator can work on the assigned tasks, resolve issues within the set deadlines and update status globally on the RT ticketing platform.

This paper provides a walk-through demonstrating the cloud migration, system monitoring and data analytics for a real microgrid testbed facility. Synchrophasor technology in distributed generation has lower latency and higher data rate requirements than many industrial applications. The aim is to demonstrate cloud migration for real-time synchrophasor's control and thus validate the suitability of the proposed framework for time-critical industrial applications.

II. Proposed Cloud Migration Approach

Many industrial systems are geographically distributed (e.g., power systems, water and waste management, oil and gas, etc) with HMI located locally, or accessed via a remote system. They consist of heterogeneous devices including legacy systems with weak or no security. Thus, a cyber intruder can launch an attack on industrial operations if any internal network device is compromised by a malware. The proposed cloud migration approach is designed to operate in a 'plug & play' manner, adopting an architecture that is inherently secure, to mitigate the security vulnerabilities of legacy devices. It consists of two key components: (i) Cloud Connectivity Kit (CCK), and (ii) cloud platform.

A. Cloud Connectivity Kit (CCK)

The CCK or cloud enabler is a low-cost device attached next to the ICS device (PLC, RTU, actuator, sensor, etc) as shown in Fig. 1. It has two Ethernet ports (i.e., to connect one ICS device). It provides localized security to the ICS device and also migrates it to the cloud using an encrypted end-to-end VPN tunnel. The CCK ensures that all network traffic from the ICS device is securely routed via a VPN tunnel to the cloud. This approach is particularly useful to secure ICS devices which use weak legacy communication protocols.

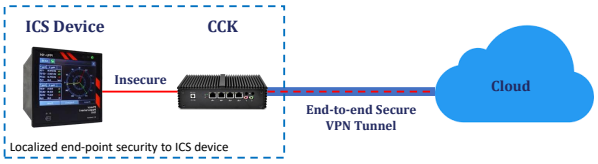


Figure 1. CCK provides localized security to the ICS device.

The CCK is also equipped with a firewall that blocks access to the ICS device from the local network after successful cloud migration. It ensures that the ICS device is accessible and controllable only from the cloud. Thus, the firewall protects the ICS device from malicious scanning and cyber-attacks if any local network device is compromised.

B. Cloud Platform

The cloud platform provides APIs for integration of industrial control operations or applications. The basic architectural components of the cloud platform for power system scenario are depicted in Fig. 2. The cloud performs data acquisition/-analytics, system monitoring, orchestration and control of ICS devices through CCKs. Each CCK has a unique identity and is remotely configurable from the cloud.

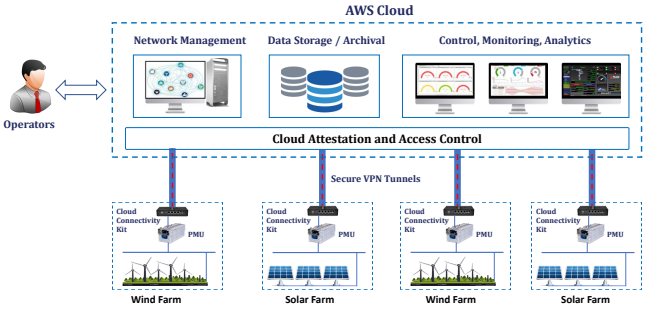


Figure 2. Proposed cloud migration approach for a typical industrial system.

A VPN certificate is issued for each CCK that is used for authentication and authorization to access cloud resources. The cloud works as a trusted Certificate Authority (CA) and issues, renews, revokes or manages certificates for all CCKs. These digital certificates ensure the security of VPN tunnels and their validity is configurable in the cloud. The cloud can revoke a certificate if a CCK device is compromised. Once a certificate is revoked, the specific CCK can no longer access cloud resources. Different Virtual Machines (VMs) can be created in the cloud for hosting HMI and industrial control/monitoring applications. Most public (AWS, Azure) and private (Openstack) cloud platforms offer configurable

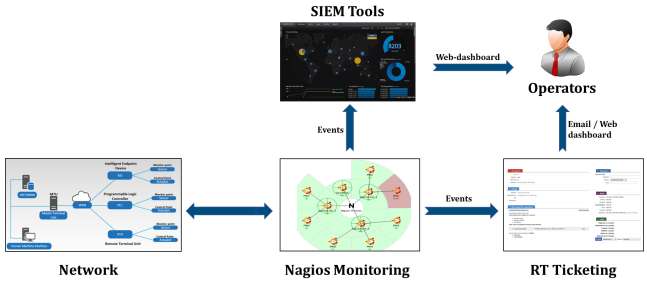


Figure 3. Proposed system monitoring framework.

security policies for each VM. These security policies control the cloud's external and inter-VM communication. Further, the cloud also provides VLAN technology for segregating resources.

III. System Monitoring and Alerting Framework

The IIoT system monitoring framework is responsible for ensuring that all devices and services are functioning properly. As soon as a device or service failure is detected in any part of the IIoT system, notifications are generated and sent to the relevant operator based on the fault location. The proposed system monitoring framework is designed with the following features: (i) it is continuous, automated and independent of manual human monitoring, (ii) it is versatile and scalable to dynamically add or remove an IIoT device, (iii) it supports different forms of notifications such as email, SMS or alerts to Security Information and Event Management (SIEM) tool, (iv) it can pin-point fault location in large and complex network, (v) it keeps track of changes in the system and stores statistics about devices and services, and (vi) it supports multiple operator accounts, each with different rights and allows secure remote authentication of users.

Fig. 3 depicts the proposed system monitoring framework. The monitoring task is performed by Nagios where the entire IIoT network topology is programmed using specific instructions. Nagios is an open-source solution that periodically probes devices and the services running on them. It provides information about fault location by using the parent-child relationship between devices. To avoid false positives (due to packet loss or glitch in the network), it can be programmed to perform checks a specified number of times before deciding about the status of a device or service. When a device or service fault is detected, notifications are sent to the SIEM tool and RT ticketing system.

A. Issue Management and Tracking

The RT ticketing system is responsible for managing events as tickets assigned to different operators or user accounts. The RT server is accessible via a web-based interface. It allows concurrent accessibility and control by multiple user accounts to work on the tickets/issues. At the backend, RT uses MySQL database to store events/notifications generated by Nagios.

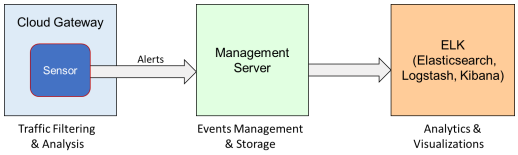


Figure 4. Network traffic analytics framework using ELK.

B. SIEM Analytics

As depicted in Fig. 3, events are also received by a SIEM tool. The SIEM tool can be programmed to generate visual analytics of events for improved IIoT infrastructure monitoring via a web interface. It captures and indexes events in real-time and allows users to search, monitor, analyze and visualize them in customized dashboards. The SIEM framework used in the proposed approach is Elasticsearch-Logstash-Kibana (ELK). ELK offers intuitive log search features and various visualization options on a highly customizable dashboard. The scalability and manageability make it a better choice for events monitoring and visualization in the proposed system.

The ELK in the proposed system is also used for monitoring network traffic from phasor devices for malicious behavior and network-based attacks detection. The basic setup in the cloud platform is shown in Fig. 4. For traffic filtering and analysis, a sensor is deployed on the cloud gateway. Features and capabilities of the sensor are beyond the scope of this paper and published in [15]. The sensor is developed using PCAP libraries and continuously monitors network traffic. It sends alerts to the management server which is responsible for event correlation and storage. The management server also forwards processed events to the ELK framework. The ELK's data collection engine 'Logstash' is programmed to receive events over a UDP socket and parse them using a defined format. The events are restructured in schema-free JSON format and provided to Kibana for visual analytics.

IV. Experimental Validation

This section performs functional and experimental validation of the proposed system for a real microgrid testbed facility in the laboratory. The concept of a microgrid is explained in Fig. 5 which contains generators and consumers over a certain geographical area. A microgrid may operate independently (i.e., disconnected/islanded) fulfilling its own local demand or be connected to the main grid to contribute power. The transitional state (known as synchronous islanding) when a microgrid is going to connect or disconnect from the main grid is most critical. If connecting, the microgrid should be synchronized (same voltage magnitude, phase angle and frequency) with the main grid to avoid physical equipment damage in either part of the grid. If disconnecting, the microgrid should be capable to meet its local electricity demand to avoid a blackout.

A. Testbed

The distributed generation testbed used for experiments is shown in Fig. 6(a). It consists of a microgrid, main grid

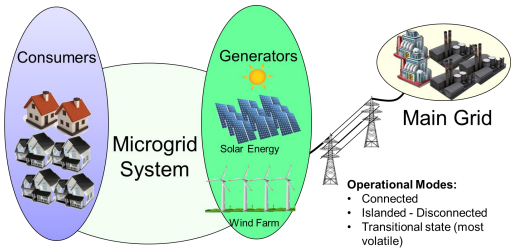
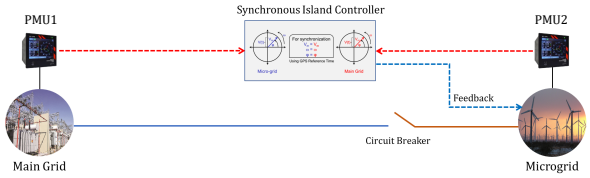
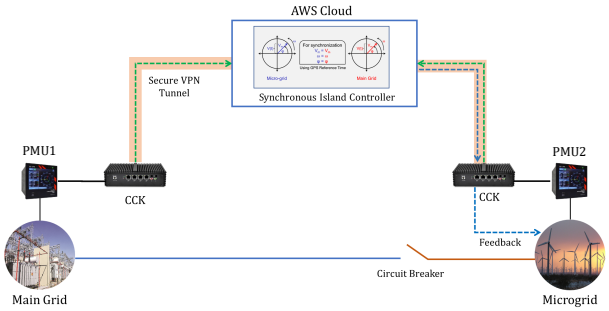


Figure 5. The microgrid concept.

(i.e., utility supply), two PMU devices, controller and circuit breaker. The microgrid is comprised of a DC machine coupled to the drive shaft of an alternator and 3 phase transmission load. The DC machine receives real-time feedback from the synchronous island controller based on which it increases/decreases torque on the drive shaft of the alternator to control electrical power output. The PMU devices measure electrical properties in real-time and send them to the controller. Controller processes received data, which includes GPS timestamps, to analyze if the microgrid is synchronized with the main grid. If not synchronized, the controller sends feedback to the microgrid to adjust its electrical power output. Once synchronization is achieved, the circuit breaker can be closed and the microgrid can be safely connected to the main grid.



(a) Local testbed



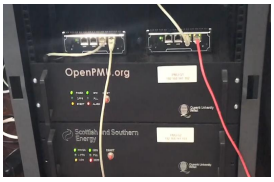
(b) Cloud migrated testbed

Figure 6. Synchronous islanding testbed.

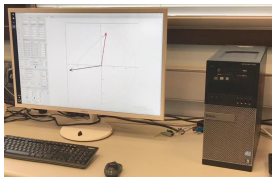
B. Cloud Migration

For migrating the synchronous islanding control system to the cloud, a CCK is connected to each PMU device as shown in Fig. 6(b). In the experiments, Amazon AWS cloud is used for hosting the synchronous island controller, VPN server, system monitoring, analytics and archival applications. Each application is hosted on a different VM with appropriate security policies to allow or block access to specified protocols

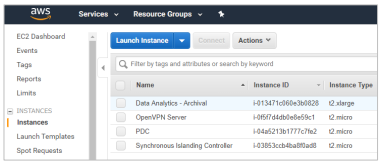
(a) Microgrid and 3-Phase Transmission Load



(b) PMUs connected to CCK



(c) Local Controller



(d) AWS Cloud VMs

(e) Cloud Controller

Figure 7. Pictorial view of synchronous islanding testbed components.

and port numbers. A private network is created for inter-VM communication. External access to the cloud is allowed only through the cloud gateway after successful authentication with the VPN server. A sensor is also configured on the cloud gateway for network traffic analysis, logging activities and generating alerts to the system monitoring framework. The pictorial view of connected testbed components is shown in Fig. 7.

To access cloud-based services, a web application is developed as shown in Fig. 9. It is integrated at the backend with the monitoring system, SIEM analytics, VPN server, etc. Through the web interface, the user can also orchestrate or configure ICS devices such as PLCs and PMUs. For the VPN setup, a scalable open-source solution is used i.e., OpenVPN. Through the OpenVPN server, a certificate can be issued for each CCK. These digital certificates are used for CCK's security credentials and identity verification at the cloud. Only a CCK with a valid certificate can authenticate at the cloud.

C. Evaluation of System Monitoring Framework

Nagios is configured to probe devices and services at an interval of 10 seconds. A device is announced in 'soft error state' if unreachable in the first attempt. After 10 failed attempts, the device is put into 'hard error state' and notification is generated. Increasing the number of attempts can reduce false positives due to packet loss or glitch in the network at the cost of increased network overhead. However, the overhead is small due to the very small size of probe packets. For functional verification, PMU2 is made unreachable by disconnected the network cable. The cloud-based monitoring

system automatically detected the down status of PMU2 and sent out alerts as shown in Fig. 8.

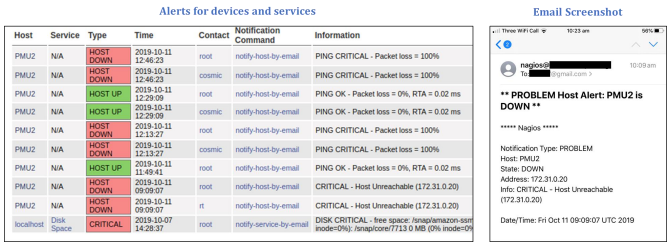


Figure 8. Alerts generation for a network issue.

Nagios alert also generated a ticket in RT and indexed it in the 'Power System Monitoring' queue as shown in Fig. 9. The ticket can be assigned to a specific operator based on their skills, capabilities and type of issue/event. The ticket can be delegated to a different operator if necessary and deadlines or reminders can be created to resolve the issue on time. Ticket status can be updated once the issue is resolved. The monitoring system will also send a notification to the responsible person when the issue is resolved. It also stores statistics about the status of each device and service.

D. SIEM Analytics and Latencies Analysis

For log and network traffic analytics, ELK is programmed on a cloud VM to receive events over a UDP socket. The events are processed by Logstash and provided to Kibana for indexing in the database. They are analyzed by the powerful elastic-search engine and displayed in a customized dashboard using different visualizations for meaningful analysis. Visual analytics can improve problem diagnosis, analyzing patterns and identifying security threats. SIEM analytics are based on the IEEE C37.118 protocol in current implementations and different severity levels are assigned for events based on system knowledge. For testing purpose, synchrophasor events were generated and visualized as shown in Fig. 10.

Communication latency is a critical performance factor for real-time industrial control operations. Like many industrial systems, power systems also have strict latency requirements for synchrophasor-based distributed generation systems. According to IEC 61850-90-5, communication latency for synchrophasor technology has a 100 ms limit for correct functioning. It is obvious that communication latencies will increase in the cloud migrated system. The main objective is to analyze whether latencies are still within a safe limit for

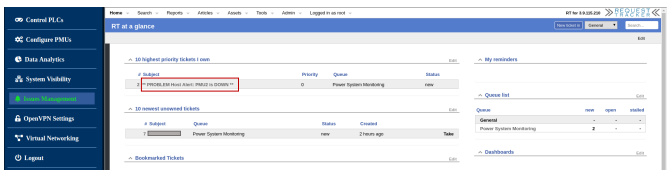


Figure 9. Ticketing system for issues management.

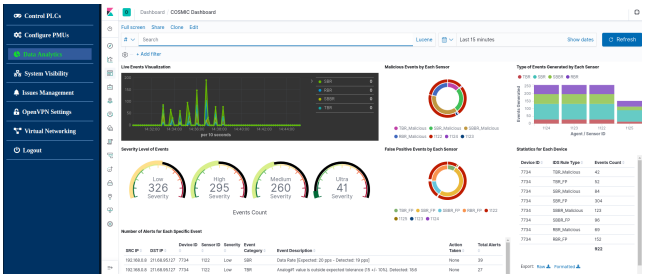


Figure 10. Visualization of synchrophasor traffic analytics.

Table I
COMMUNICATION LATENCIES AVERAGED OVER 24 HOURS (100 TRIALS EACH HOUR).

	Latency (ms)			
	Min	Avg	Max	Std. Dev.
Local system	0.25	0.44	1.42	0.082
Cloud (London)	7.58	8.08	10.61	0.172
Cloud (North Virginia)	45.34	46.61	49.28	0.494

system operation. In the cloud migrated system, communication latencies depend on the cloud location, ISP and access technology.

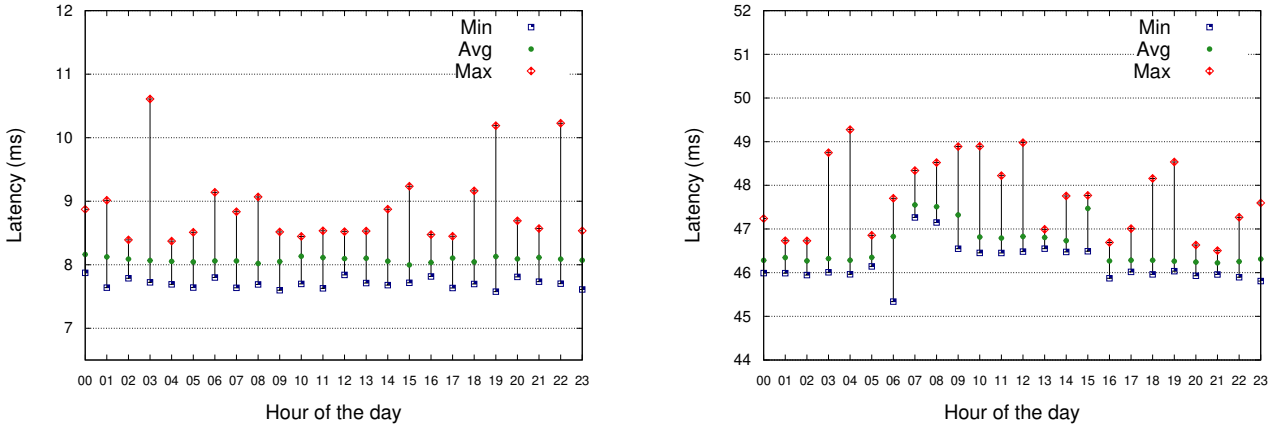
For experimentation, field devices (i.e., PMUs) were placed in Belfast (Northern Ireland) and AWS cloud VMs were deployed at two different locations: London (UK) and North Virginia (USA). Field devices have a much shorter distance to AWS London than AWS North Virginia. For both cloud locations, latencies were measured over a period of 24 hours and averaged over 100 trials during each hour. It can be observed in Fig. 11 that communication latencies significantly depend on the cloud location. Fig. 12 provides visual comparison of average latencies. It can be observed that communication latencies for AWS London are at-least 6 times lower than AWS North Virginia.

Table I shows latencies for local and cloud migrated synchronous islanding operations. It can be observed that incremental latencies are much lower than the 100 ms limit for synchrophasor technology at both cloud locations. This validates that the proposed cloud migration approach is suitable for time-critical microgrid control operations. Due to advancements in cloud and Internet access technologies, public cloud platforms are now feasible for many industrial systems.

V. CONCLUSIONS

Cloud migration is a challenging task for industrial systems due to the presence of legacy devices with weak or no security. They are cost-prohibitive to replace and emerging cloud technologies should adopt them. The current research trend primarily focuses on developing new ICS devices specifically for the cloud [13], [14] or use a cloud migration approach without addressing legacy adaptation [12].

In contrast to previous works [12], [13], the proposed cloud migration approach is inherently secure to adopt legacy



(a) AWS London

(b) AWS North Virginia

Figure 11. Communication latencies at different AWS cloud locations. Results are averaged over 100 trials during each hour.

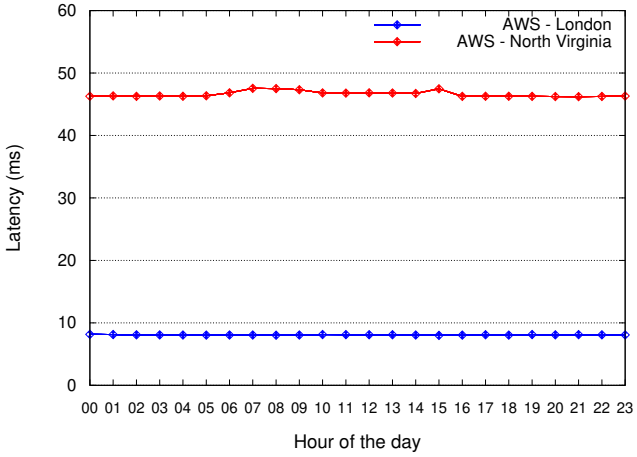


Figure 12. Average communication latencies at different cloud locations.

devices as well. The insecure communication of legacy equipment passes through an end-to-end encrypted VPN tunnel without risking system security. Moreover, the proposed approach operates as plug & play for smooth migration of industrial operations to the cloud.

For validation purposes, this paper presented implementation details for a distributed generation use-case in the smart grid. Cloud migration using secure VPN technology, automated system monitoring and SIEM analytics have been successfully demonstrated for a real microgrid testbed facility. The CCK software is lightweight and can be deployed on a low-cost hardware to significantly reduce cost in an industry modernization process. System monitoring is a tedious and time-consuming task for large and complex IIoT platforms with thousands of devices. The proposed system automates the monitoring process making issues identification, reporting and fixing process much faster than manual troubleshooting. It is dynamically scalable to meet IIoT requirements and ensures that devices/services are operational 24/7.

Experimental results proved that the incremental communication latencies due to cloud platform are small and do not impact real-time microgrid control operations. Successful demonstration for synchrophasor technology with strict low latency requirements confirms that the proposed approach is feasible for similar industrial systems.

REFERENCES

[1] R. Khan, K. McLaughlin, J. Hastings, D. Laverty, and S. Sezer, "Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid," in *Privacy, Security and Trust (PST)*, 2018.

[2] K. Maqbool, X. Wu, X. Xu, and W. Dou, "Big data challenges and opportunities in the hype of industry 4.0," in *IEEE ICC*, 2017.

[3] I. Stellios *et al.*, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys Tutorials*, 2018.

[4] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid," in *4th ICS-CSR*, August 2016.

[5] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in pmu-based power network and countermeasures," *IEEE Access*, 2018.

[6] R. Khan, K. McLaughlin, J. Hastings, D. Laverty, and S. Sezer, "Inter-technology bridging gateway: A low cost legacy adaptation approach to secure industrial systems," in *IEEE PES-GM*, 2018.

[7] J. E. Rubio, R. Roman, and J. Lopez, "Analysis of cybersecurity threats in industry 4.0: The case of intrusion detection," in *Critical Information Infrastructures Security*, 2018.

[8] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid," *IEEE Access*, 2017.

[9] T. A. Rizzetti *et al.*, "Cyber security and communications network on scada systems in the context of smart grids," in *UPEC*, 2015.

[10] H. P. Breivold, "Towards factories of the future: migration of industrial legacy automation systems in the cloud computing and internet-of-things context," *Enterprise Information Systems*, 2019.

[11] A. Ibrahim, M. Zubaida, and H. Yahaya, "Information security factors in the implementation of industrial control system into cloud environment," *Advanced Science Letters, Vol. 24, No. 7*, 2018.

[12] P. Papcun1 *et al.*, "Cloud based control of industrial cyber-physical systems," in *CIE48 Proceedings*, 2018.

[13] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," *Computer Networks*, vol. 134, 2018.

[14] X. Liu *et al.*, "Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed," *Manufacturing Systems*, 2017.

[15] R. Khan *et al.*, "Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid," in *IEEE PES-GM*, July 2017.