FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 32, N^{o} 3, September 2019, pp. 345-358
https://doi.org/10.2298/FUEE1903345S

SCADA SYSTEMS IN THE CLOUD AND FOG ENVIRONMENTS: MIGRATION SCENARIOS AND SECURITY ISSUES *

Mirjana D. Stojanović[1], Slavica V. Boštjančič Rakas[2], Jasna D. Marković-Petrović[3]

[1]University of Belgrade, Faculty of Transport and Traffic Engineering, Belgrade, Serbia
[2]University of Belgrade, Mihailo Pupin Institute, Belgrade, Serbia
[3]CE Djerdap Hydroelectric Power Plants Ltd., HPP Djerdap 2, Negotin, Serbia

Abstract. *This paper addresses scenarios and security issues when migrating SCADA systems to cloud and fog environments. Migration strategies to the cloud refer to different cloud infrastructures (public, private or hybrid) as well as selection of cloud service. Benefits of cloud-based SCADA systems mainly refer to improving economic efficiency. We further address migration risks, with regards to quality of service and cyber security. Challenges in security provisioning encompass security solutions, risk management and test environment. Finally, we address emerging evolution of SCADA toward fog computing, including the three-tier system's architecture and security issues.*

Key words: *Cloud computing, cyber security, fog computing, quality of service, SCADA*

1. INTRODUCTION

With respect to the earlier version [1], presented at the 4th Virtual International Conference on Science, Technology and Management in Energy – eNergetics 2018, this paper is extended with more thorough considerations related to cyber security when migrating Supervisory Control And Data Acquisition (SCADA) systems into cloud computing environment, and discussion on the evolution toward fog computing system architecture.

In the past few years, the focus of cloud computing has progressively shifted from consumer applications toward corporate control systems. The migration of applications, such as SCADA, into the cloud environment is interesting for business users due to potential reduction of costs, scalability, efficient system configuration and maintenance. Access and lease of resources are on-demand, with costs that are much lower than buying,

Received February 12, 2019; received in revised form April 18, 2019
Corresponding author: Mirjana D. Stojanović
University of Belgrade, Faculty of Transport and Traffic Engineering, Vojvode Stepe 305, 11000 Belgrade, Serbia
(E-mail: m.stojanovic@sf.bg.ac.rs)
* An earlier version of this paper was presented at the 4th Virtual International Conference on Science, Technology and Management in Energy, eNergetics 2018, October 25-26, Niš, Serbia [1]

installing and maintaining the hardware and software, and with decreasing the number of technical staff.

The industrial sector is experiencing substantial benefits from using the Industrial Internet of Things (IIoT) to automate systems, deploy different types of sensors, improve efficiency, and increase revenue opportunities. The amount of data from such industrial systems can be measured in the millions of gigabytes. Traditional information technology (IT) cannot fulfill requirements regarding data analysis, delay, mobility, reliability, security, privacy, and network bandwidth. Fog computing seems to be a promising solution to resolve such problems. Particularly, fog computing outperforms cloud computing for delay-sensitive applications with stringent security requirements.

Apart from industry efforts [2–5], only a few academic research papers systematically explored SCADA systems using cloud and/or fog environments, and particularly the related security issues.

Our primary motivation for this work was to provide an in-depth insight into migration of advanced SCADA systems to both cloud and fog environments, with focus to security as a crucial risk factor in the context of critical infrastructure. The main objectives of this review paper are: (1) to discuss security issues of cloud-based SCADA systems, regarding different migration strategies and types of cloud services; (2) to consider SCADA security solutions and challenges in security provisioning in the cloud environment and (3) to explore SCADA evolution toward fog computing system architecture, with special concern to security. Finally, we identify gaps in current research and propose relevant research priorities for future work in the area.

The rest of the paper is organized as follows. Section 2 provides a brief theoretical background, regarding operation principles of SCADA systems, as well as basic concepts of cloud and fog computing. In Section 3, we first explain migration strategies of SCADA systems to the cloud, with respect to different cloud infrastructures and selection of cloud service. Further, benefits and risks of cloud-based SCADA systems are explained, as well as challenges in cloud security provisioning in terms of security solutions, risk management and test environments. Section 4 considers evolution toward fog computing system architecture, including migration of SCADA systems to fog, and security issues. Section 5 concludes the paper.

2. THEORETICAL BACKGROUND

2.1. SCADA System: Architecture, Configuration and Protocols

SCADA systems are a class of industrial control systems that control and monitor geographically dispersed process equipment in a centralized manner. They are widely used in the industrial sectors like electric power systems, oil refineries and natural gas distribution, water and wastewater treatment, and transportation systems.

Fig. 1 presents layered architecture of a SCADA system, with common components and configuration. Hierarchy of SCADA system is defined according to interconnection of its components and their connectivity with external networks [6–8]. The lowest layer 0 represents physical devices that are in direct interaction with industrial hardware, interconnected via fieldbus.

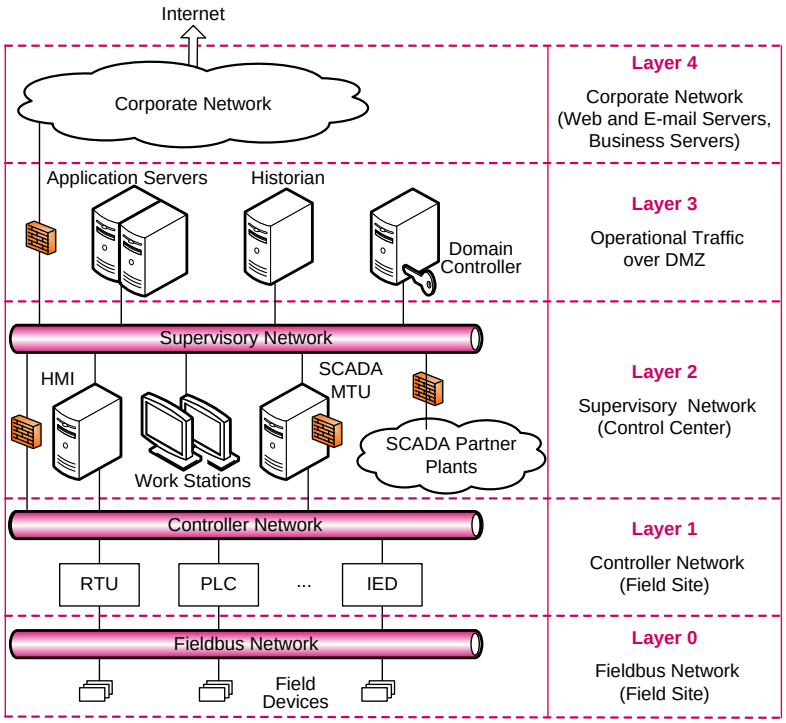

Fig. 1 The layered architecture of a SCADA system

Controllers at layer 1 process signals from field devices and generate appropriate commands for these devices. They encompass remote terminal units (RTUs), programmable logic controllers (PLCs) and intelligent electronic devices (IEDs) that perform local control of actuators and sensor monitoring.

Processing results are forwarded to control center at layer 2 for further analysis and response control. Supervisory network connects SCADA server (Master Terminal Unit, MTU), historian server, engineering work stations, human machine interface (HMI) server and consoles, as well as communication devices, such as routers, switches or modems. Control center collects and analyzes information obtained from field sites, presents them on the HMI consoles, and generates actions based on detected events. Control center is also responsible for general alarms, analysis of trends and generating the reports. Communication subsystem connects control center with field sites and allows operators remote access to field sites for diagnostic and failures repairing purposes. It also connects control center with SCADA partner plants.

Layer 3 typically represents demilitarized zone (DMZ), where application servers, historian server and domain controller are located. Layer 4 corresponds to the corporate IT network, which is connected to the Internet.

Modern SCADA systems are based on open communication standards, such as Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP) suite and a variety of wireless standards. A set of standard or proprietary protocols are used for communications, over point-to-point links or a broadband IP-based wide area network (WAN). There are several standard

and vendor-specific SCADA communication protocols, and the most widespread are Modbus, Distributed Network Protocol (DNP3), IEC 60870-5 series and IEC 61850 series used for electrical substation automation systems. Most of these protocols are designed or extended to operate over TCP/IP networks. Besides, most of the existing fieldbus protocols are based on Ethernet technology. A comprehensive review of SCADA protocols can be found in [9] and [10].

2.2. Cloud Computing: Basics and Security Issues

According to [11], cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Public cloud infrastructure is owned by a provider and sold as a service to business and residential users. Private cloud refers to an infrastructure that is owned or leased by a business user (single organization). Hybrid cloud infrastructure is a combination of private and public cloud infrastructures, which remain mutually independent and connected by standard or proprietary technology that enables portability of data and applications.

Service architecture of a cloud computing system is hierarchically structured [12]:

- The lowest, hardware layer at the data center actually consists of the physical hardware devices including the processor, memory, storage and bandwidth.
- The infrastructure layer assumes the virtualization to provide the **Infrastructure as a Service (IaaS)**, which usually consists of a pool of virtual machines (VMs) that can be provisioned on demand to the IT consumers.
- The platform layer enables creation and development of software, which can be later delivered over the Web. Hence, this layer provides the **Platform as a Service (PaaS)** by utilizing the components and services of the infrastructure layer.
- The highest, software layer provides the ready-to-use software and applications for the business needs of the cloud service customers. Hence, this layer facilitates and provides the **Software as a Service (SaaS)** by utilizing the components and services of the platform layer.

Besides security threats that are present in the existing computing platforms and networks, cloud computing faces a number of additional vulnerabilities [13]. They include: (1) attacks by other customers; (2) shared technology issues; (3) failures in provider or customer security systems; (4) flawed integration of provider and customer security systems; (5) insecure application programming interfaces; (6) data loss or leakage and (7) account or service hijacking.

In particular, susceptibilities depend on the type of cloud service. In general, IaaS is susceptible to all of the threats that are well known from the traditional information and communication environment [14]. All of the client applications running on the virtual machines are like "black boxes" for the provider. In other words, the customer is responsible for securing these applications. PaaS is particularly susceptible to shared technology issues, because security settings may differ for various kinds of resources. Another problem caused by shared resources refers to data leakage. Finally, protection of user objects is one of the most serious issues of PaaS [15]. Since SaaS requires only a Web browser and the internet connection, its security aspects are similar to the Web service [16]. SaaS is susceptible to data security, and particularly to their confidentiality.

The other common problems with data security include data backup, data access, storage locations, availability, authentication, etc.

Table 1 summarizes the attacks types and their impacts, regarding layered cloud service architecture and emphasizes responsibilities of cloud service provider (CSP).

Table 1 Types of attacks on the cloud and their impacts (adapted from [16])

Security issues	Attack types	Impacts	CSP responsibility		
			SaaS	PaaS	IaaS
Software layer	SQL injection attacks, cross site scripting	Modification of data, confidentiality, session hijacking	✓		
Platform layer	Domain Name System attacks, sniffing, reuse of IP address	Traffic flow analysis, exposure in network security	✓	✓	
Infrastructure layer	DoS and DDoS, VM escape, hypervisor rootkit	Software interruption and modification, programming flaws	✓	✓	✓
Hardware layer	Phishing attacks, malware injection attack	Limited access to data centers, hardware modification and theft	✓	✓	✓

2.3. Fog Computing: Basics and Security Issues

Fog computing is a decentralized network architecture in which data storage, processing and applications are distributed in the most efficient way between the data source and the cloud. Fog computing and cloud computing show similar characteristics in terms of computation, storage and networking technologies. However, the most important difference of fog computing is its close distance to end users. This property is essential to support delay-sensitive applications and services. Another difference refers to support of big data by means of edge analytics and stream mining. Finally, location-awareness property enables mobility support. Comprehensive surveys on fog computing, including applications in the electric power industry, can be found in [17] and [18].

Another benefit of fog computing is its high security because data is processed by a large number of nodes in a distributed system. However, including the virtualization just like cloud, fog environment can still be affected by the similar threats. As opposed to cloud computing, standard security certifications and measures still do not exist for the fog computing. Stojmenovic and Wen first explored security and privacy issues in the fog computing environment [19]. A more detailed review of fog security solutions can be found in [20].

3. Cloud-Based SCADA Systems: Migration, Benefits and Risks

3.1. Migration of SCADA Systems to Cloud

Cloud computing provides support for SCADA applications in two ways [3]:

1. SCADA application is executed on premises (company, organization, etc.). It is directly connected with control center and transfers data to the cloud where they can be stored and distributed.
2. SCADA application is completely executed in the cloud, and is remotely connected to the control center.

The first method, presented in Fig. 2, is more widely used. Control functions of SCADA application are isolated in the controller network, while SCADA application is connected to cloud services that allow visualization of processes, reports and remote access. Such applications are usually implemented on a public cloud infrastructure.

Implementation illustrated in Fig. 3 is suitable for distributed SCADA applications. Controllers are connected via WAN links to SCADA application that is executed in the cloud. Such applications are usually implemented on private and hybrid cloud infrastructures.

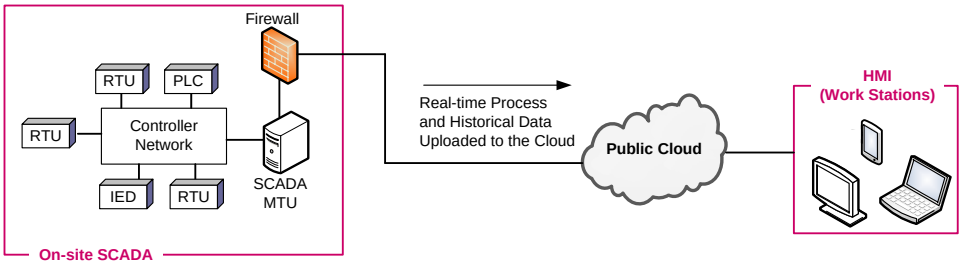

Fig. 2 Public cloud infrastructure, with SCADA system operating on-premises and sending data through cloud

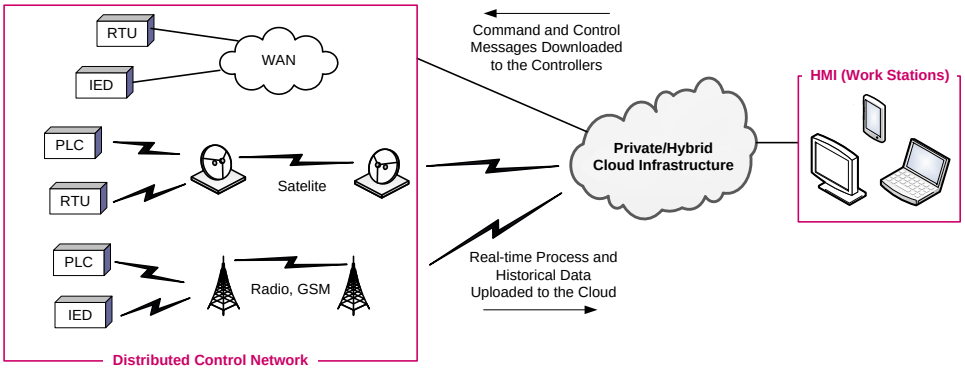

Fig. 3 Private or hybrid cloud infrastructure where controllers are connected via WAN links to SCADA application that is executed in the cloud

Regarding service selection, there are three possible migration scenarios of SCADA system to the cloud, namely the re-hosting, refactoring and revising [21].

The first scenario (re-hosting) is the fastest and the simplest, and represents installing the existing SCADA applications to cloud environment, based on IaaS. This is the first step of the gradual migration, that allows analysis and, if needed, extension of the applications, through several iterations.

The second and the third scenarios assume re-engineering to better benefit from the features of cloud computing, primarily in terms of scalability and reliability. This can be a simple modification of particular features (refactoring). An example is implementation of resource control capabilities that allows adding additional resources when the application

is intensively used and releasing resources when they are not needed. Larger modifications at the application core are also possible (revising). An example is the use of PaaS database for modification of application in such a way that multi-tenancy SaaS offering is possible. The increase of the number of SaaS offers requires the replacement of the existing SCADA applications with cloud-based SaaS solutions.

3.2. Benefits and Risks

There are several advantages of cloud computing that motivate users to migrate to cloud-based SCADA system.

With public cloud, access and lease of resources are on-demand, at a much lower price than purchasing, installing and maintaining company's own software and hardware. Consequently, the number of technical staff, needed for IT resource maintaining, decreases. According to [3], cloud-based SCADA solution can reduce end-user costs up to 90% over a traditional SCADA system.

Scalability is enhanced, since there is no need for purchasing and installing server farm, databases, Web servers, when more resources are needed. Users can easily purchase additional resources on a virtual cloud server, with no need of installing and maintaining the additional hardware [3].

Information located on a cloud server can be accessed from anywhere; hence, the collaboration on projects is more efficient due to easier access to information.

Upgrade of existing and implementation of new applications is simplified through re-hosting, refactoring and revising [21].

With private cloud, efficient resource usage, reduced energy consumption and efficient maintenance enable faster upgrade, business continuity, rapid deployment of new services and overall cost reduction [22].

Despite the aforementioned benefits, there are two serious risk factors for cloud-based SCADA systems, quality of service (QoS) and cyber security, which will be considered in the following subsections.

3.2.1. QoS Requirements

QoS refers to system's performance, as well as reliability and availability. Most of the industrial applications pose stringent performance requirements regarding delay, packet loss and bandwidth. The most stringent requirements for delay are in the fieldbus and controller networks. Response times are in the range of 250 microseconds to 1 millisecond, while for less demanding processes they are in the range of 1 to 10 milliseconds [9]. Upper layers have progressively less stringent delays, typically up to 1 second. Industrial applications also assume highly reliable network infrastructure with service availability higher than 99.98% [23].

The use of public cloud services increases the risk that these requirements will not be met, because the user cannot control the network performance. Increased and unpredictable delay is challenging, since it can block the real-time SCADA operation.

Church et al. presented a case study on migration of a SCADA system to the IaaS cloud [21]. They analyzed several open source SCADA applications and applied re-hosting approach to migrate SCADA application to a real academic network. Performance evaluation has shown that delay introduced by the cloud-based SCADA system was not a limiting factor. Measured response times were in the range from several hundreds of milliseconds to one

second. However, problems emerged with polling protocols (e.g., Modbus TCP), which are based on individual polls of remote stations. Applying event-driven communication protocols seems to be more efficient solution, because of reducing both delay and amount of data sent across a network. If such a solution is not possible and polling protocols have to be applied, field devices should be spread across several remote servers.

Before migration of a SCADA system to the public cloud, the following questions should be answered [2, 3]:

- What are the consequences of variable QoS on the industrial process controlled by a particular SCADA system?
- What is the impact of increased delay and delay variation on SCADA system?
- What is the upper bound for delay in each system's part? For example, increased delay is not critical at the upper layers, which perform monitoring and reporting.

The problems of availability and reliability exist in every system in the public cloud. The servers are placed in unknown locations that users cannot access. The data of SCADA systems encompass results of the industrial process control in real time; therefore, the loss of functionality, even for a few seconds, can cause serious consequences to the industrial process.

The situation is different with private cloud infrastructure. Chen et al. conducted a study on private cloud-based electric power SCADA system [22]. Their experimental results indicated technical feasibility of the professional private cloud solution; such a system meets the actual need of power grid operations, and some QoS parameters such as network load rate are even better than those of the traditional IT architecture.

3.2.2. Security Issues

The security issue of the hard real-time system requires overall analysis and holistic understanding of network protection, management theory and physical systems. This problem is getting even more complex in the case of migration to the cloud.

Cyber attacks on SCADA systems can be categorized into: hardware attacks, software attacks and communication stack attacks [24]. SCADA control center performs its actions based on the data received from RTUs. Attacks that jeopardize process control focus on modifying control data or blocking the data transfer. Primary threats to SCADA systems are command/response injection, various forms of denial of service (DoS) attacks, including distributed DoS (DDoS), and man-in-the-middle (MITM) attack [25, 26].

Cloud-based SCADA systems suffer from the same cyber security risks (indicated in Section 2.2) as the other systems integrated into cloud [27]. Still, there are a number of threats in the public cloud environment that might make SCADA systems more vulnerable.

First, cloud-based SCADA systems are more exposed to cyber threats such as command/response injection, DoS/DDoS attacks, and MITM attack. This comes as a consequence of sharing an infrastructure with unknown outside parties [3].

Second, network connections between SCADA systems and the cloud potentially increase the risk of jeopardizing the whole industrial control systems by outside attackers [27, 28].

Third, some of SCADA-specific application layer protocols lack protection [4, 27]. For instance, the most widespread SCADA protocols, Modbus and DNP3, do not support authentication and encryption.

Finally, the use of commercial off-the-shelf solutions (instead of proprietary ones) potentially increases the cyber security risk [27].

3.3. Security Solutions

According to [28], security solutions concerning public cloud infrastructure should address the challenges related to:

- Information input;
- Information and command output;
- Shared storage and computational resources and
- Shared physical infrastructure.

Regarding information input/output, it is essentially important not to expose the critical, control infrastructure to the Internet. For that reason, when using public cloud infrastructure, push technology should be utilized to move data to the cloud rather than pull technology. Thus, there are no open network ports on the control infrastructure, while SCADA applications remain isolated in the controller network.

Concerning shared storage and computational resources, SCADA utility interacting with a CSP should be aware how the computational resources are managed for different applications running in the cloud, including guarantees for resource allocation and network access, service levels, fault-tolerance strategy, etc.

Finally, security of shared physical infrastructure refers to secure cloud infrastructure locations, communication links connecting the cloud infrastructure to the rest of the communications infrastructure, ability to inspect and audit the locations from which SCADA application will be served, etc.

Consequently, when selecting the CSP and assessing maturity of the offered cloud service, the following criteria should be taken into account [4]:

- Ensuring secure user access.
- Mutual isolation of information originating from different applications.
- Determining the level of users control regarding changes of the CSP infrastructure.
- Data encryption.
- Automated distribution of software patches.
- Provisioning scheduled and unscheduled reports that satisfy business needs.
- Continuous monitoring, which includes assessment of security mechanisms efficiency in near real-time.
- Continuous analysis of events, incidents, suspicious activities and anomalies.
- Capabilities to create and analyze log files, to detect intrusions in real-time, to generate responses to detected attacks.
- Readiness to take immediate corrective actions of all vulnerabilities identified.
- Consistent and reliable customer service.

The most efficient way to protect SCADA system connected to the public cloud is to establish precise service level agreement (SLA) that fulfills the aforementioned criteria. Similar research, regarding enterprise resource planning, pointed out the importance of introducing SLAs in the context of using SaaS and open-source software [29].

SCADA protection is much simpler in private cloud, since security solutions are responsibility of the network owner. It is recommended to apply a strategy known as "defense-in-depth", i.e., a multilayer security architecture that minimizes the impact of a failure in any one layer mechanism [30]. This strategy assumes corresponding security policies, employing DMZ network architecture to prevent direct traffic between the corporate and SCADA networks, as well as security mechanisms such as smart access control, firewalls, intrusion detection and prevention systems, antivirus software, deploying security patches on a regular basis, etc.

In hybrid cloud, using secured virtual private network (VPN) connection to the control infrastructure is strongly recommended [28].

3.4. Risk Management

Security risk management is a cyclic process that encompasses several phases: risk analysis through identification of vulnerabilities and threats, risk assessment, making decisions on acceptable risk level, selection and implementation of measures to mitigate the risk.

Risk assessment is the most important phase in the risk management process, but also most susceptible to errors. According to [30], risk assessment is "the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact".

Different qualitative and quantitative approaches, methods and tools for risk assessment in industrial control environment can be found in the literature. Two comprehensive reviews of risk assessment methods for SCADA systems have been published only recently [31, 32]. However, none of the reviewed methods considers cloud-based SCADA. Hence, significant research efforts are needed to address this important issue, because risk management takes the outputs of the risk assessment process to consider the options for risk mitigation and finding the trade-offs among overall costs, benefits, and risks of SCADA migration to the cloud.

3.5. Test Environments

Due to need to support the operational continuity, it is often unfeasible to perform security experiments on a real SCADA system. Hence, proper test environments should be developed, consisting of testbeds, datasets and simulated attacks. While test environments for SCADA in traditional IP-based networks have gained certain level of maturity, research work is still needed regarding cloud-based SCADA systems.

SCADA security testbed can be implemented as: (1) a single software simulation package; (2) laboratory testbed, which may have several interacting simulations and (3) emulation or implementation-based, which uses emulator or real hardware [8]. In the context of cloud-based SCADA, probably the most valuable option will be laboratory testbeds that allow other researchers to repeat the experiments and validate their own upgraded solutions. Such testbeds should be built on the top of some of the general-purpose cloud simulators, which interact with domain specific models or real world field devices. Some examples of such simulators are CloudSim, GreenCloud, CloudAnalyst, iCanCloud and EMUSIM [33].

Due to confidentiality of real SCADA network data, researchers often use synthetic datasets or datasets obtained from SCADA testbeds. This is a general problem in verifying security solutions for SCADA systems. Besides synthetic datasets, there is a strong need to use datasets from real SCADA networks or to reuse publicly available ones.

Finally, proper attack models and scenarios, in which the attackers try to exploit vulnerabilities in cloud-based SCADA systems, should be developed. Building accurate and plausible threat models is a prerequisite to design secure architecture concepts. This is generally an open issue in SCADA security, while in the context of cloud-based SCADA, it has been explicitly recognized for the first time very recently [34].

4. Evolution toward Fog Computing System Architecture

4.1. Migration of SCADA Systems to Fog

Fog computing essentially extends cloud computing and services to the edge of network. Consequently, end users, fog and cloud together form three-tier system architecture. Considering migration of SCADA system, a possible architecture is proposed in Fig. 4 (based on [17]).

The end users stratum corresponds to end user devices, e.g., field devices, smart energy meters, line sensors, etc. It can also include IIoT devices.

The fog stratum encompasses one or more fog domains, managed by the same or different providers. Fog domain is constituted by the fog nodes, i.e., devices with computing, storage, and network connectivity. Examples of fog nodes are industrial controllers, switches, routers, embedded servers, etc. Fog nodes provide integration with cloud stratum, routing and switching, data storage and sharing, real-time analytics, outage management, controller functions (RTUs, PLCs, IEDs), wireless access, etc. The end users stratum and fog stratum are typically connected via wired or wireless local area networks (LANs).

The cloud stratum is responsible for functions such as high level storage, utility billing system, demand prediction, high level processing and historical data analysis. The fog stratum and cloud stratum communicate via WAN connections.

Table 2 is based on [5] and summarizes comparison of fog computing and cloud computing environments in the context of SCADA system requirements.

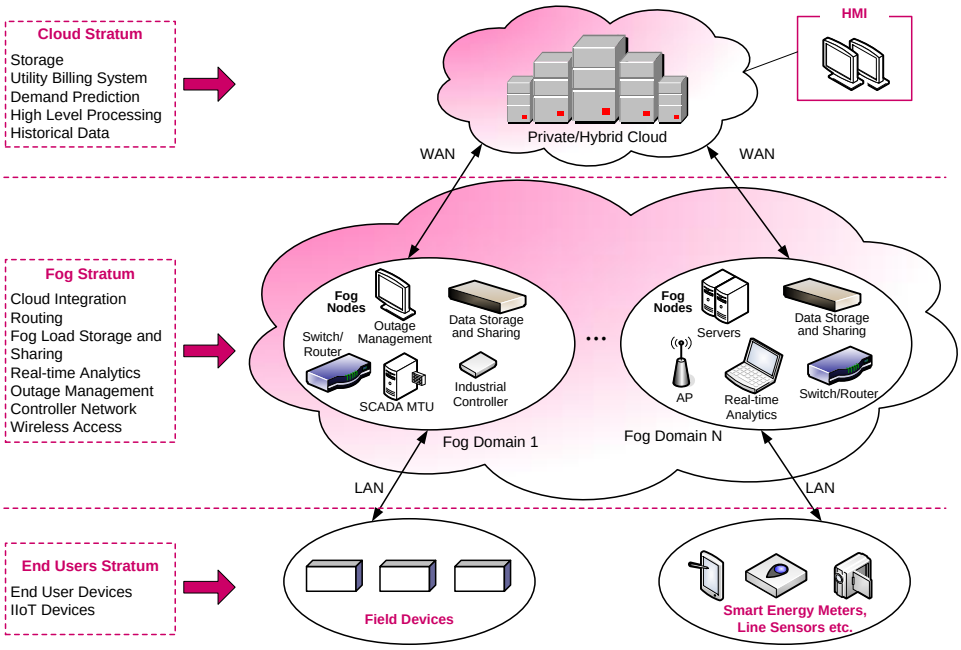

Fig. 4 Three-tier architecture of a fog-based SCADA system

Table 2 Fog computing vs. cloud computing in terms of SCADA requirements

Feature	Fog computing	Cloud computing
Architecture	Decentralized (distributed)	Centralized
Communication	Wired or wireless LAN	IP WAN
Number of server nodes	Large	Few
Real-time operation	Supported	Supported
Delay	Low	Relatively high
Bandwidth cost	Low	Relatively high
Security	High	Relatively high
Mobility and location awareness	Supported	Limited

4.2. Security Considerations

With fog computing, security does not function in the cloud, but locally, thus using the same corporate IT policy, controls, and procedures as in traditional SCADA system. Inherently, there is opportunity to increase cyber security as compared to the cloud environment. Most fog nodes include a hardware root of trust [35], which represents a basis for protection chain from the field devices, through the fog stratum up to the cloud stratum. Traffic is supervised from the cloud to the distributed fog network, which can use different anomaly-based techniques to detect malicious activities in the local context.

Security solutions for fog-based SCADA systems are generally similar to the ones applied for cloud-based SCADA. The emphasis is on the following techniques [20]:

- **Authentication.** All messages and entities must be authenticated, which is particularly important to prevent MITM attacks. Different techniques can be applied, including public cryptography coupled with decoy technology, biometric authentication, etc.
- **Access control.** All fog nodes should provide access control and ensure authorization, to protect operations such as reading or writing data, executing programs and controlling sensors/actuators.
- **Intrusion detection.** Intrusion detection techniques are generally deployed within cloud environment to identify possible incidents, e.g., different types of cyber attacks, and violation of network security policies or standard security practices. In fog computing, intrusion detection systems can be implemented both on the client side and the fog network side thus allowing double protection, from insider attacks and attacks originating from the cloud. If a threat is detected, fog nodes block malicious traffic and protect the critical SCADA network. Highly-sensitive data can be processed locally without leaving the field site.
- **Privacy.** Fog nodes are located close to, or at the field sites and collect more sensitive data compared to the cloud computing. For that reason, security techniques must ensure privacy for all field sites.

Similar to the cloud environment, challenges in security provisioning of fog-based SCADA systems include further development of fog-specific security solutions, risk assessment methods, as well as dedicated test environments.

5. CONCLUDING REMARKS

This paper provided a review of migration scenarios of SCADA systems toward cloud and fog environments with special attention to cyber security as a main operational risk factor, which requires additional research work and stipulates gradual migration. We have identified a progress in some areas, but also some open issues remain.

First, public and private cloud architectures can both be the right selection for SCADA, but one size does not fit all. A proper risk analysis should be conducted to make right choice, and there is a strong need to develop appropriate risk assessment methods for that purpose. Taking into account the assessed risk, the cost increase is justified to provide secure cloud services.

Second, proper testbeds should be developed to validate security solutions. They include laboratory testbeds, but also research efforts to develop sophisticated hardware/software emulation platforms that are able to interact with the network.

Finally, although evolution of SCADA toward fog computing environment is an emerging trend, which eliminates some of the problems inherent to the cloud, it is not risk-free by default. Besides an obvious need for security standards in the area, additional research work is needed to assess suitability of a complicated three-tier system for SCADA applications, regarding additional expenses and limited scalability.

Acknowledgement: *The paper is a part of the research funded by the Ministry of Education, Science and Technological Development of Serbia, within the projects TR 32025 and TR 36002*.

REFERENCES

[1] M. Stojanović, S. Boštjančič Rakas and J. Marković-Petrović, "Cloud-based SCADA Systems: Cyber Security Considerations and Future Challenges", In Proceedings of the 4th Virtual International Conference on Science, Technology and Management in Energy – eNergetics 2018. Niš, Serbia: Research and Development Center "ALFATEC", and Complex System Research Center, 2018, pp. 253–260.

[2] E. Nugent, "How Cloud and Fog Computing will Advance SCADA Systems", *Manufacturing Automation*, pp. 22–24, November/December 2017.

[3] L. Combs, "Cloud Computing for SCADA", InduSoft, 2011. http://www.indusoft.com/Documentation/White-Papers/ArtMID/1198/ArticleID/430/Cloud-Computing-for-SCADA (accessed February 05, 2019).

[4] P. D. Howard, "A Security Checklist for SCADA Systems in the Cloud", GCN, 2015. https://gcn.com/articles/2015/06/29/scada-cloud.aspx (accessed February 05, 2019).

[5] C. Byers, "Fog Computing for Industrial Automation", Control Eng., 2018. https://www.controleng.com/articles/fog-computing-for-industrial-automation/ (accessed February 05, 2019).

[6] I. Ahmed, S. Obermeier, M. Naedele and G. G. Richard III, "SCADA Systems: Challenges for Forensic Investigators", *Computer*, vol. 45, no. 12, pp. 44–51, December 2012.

[7] J. Marković-Petrović and M. Stojanović, "An Improved Risk Assessment Method for SCADA Information Security", *Elektron. Elektrotech*., vol. 20, no. 7, pp. 69–72, September 2014.

[8] S. Nazir, S. Patel and D. Patel, "Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques", *Comput. Secur.*, vol. 70, pp. 436–454, September 2017.

[9] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks", *IEEE Commun. Surv. Tut.*, vol. 15, no. 2, pp. 860–880, Second Quarter 2013.

[10] J. Gao, J. Liu, B. Rajan, R. Nori, et al., "SCADA Communication and Security Issues", *Secur. Commun. Netw*., vol. 7, no. 1, pp. 175–194, January 2014.

[11] P. Mell and T. Grance, *The NIST Definition of Cloud Computing*. NIST Special Publication 800-145, 2011.

[12] A. Bashar, "Modeling and Simulation Frameworks for Cloud Computing Environment: A Critical Evaluation", In Proceedings of the International Conference on Cloud Computing and Services Science – ICCCSS 2014. World Academy of Science, Engineering and Technology, 2014, pp. 1–6.
[13] B. Hari Krishna, S. Kiran, G. Murali and R. Pradeep Kumar Reddy, "Security Issues in Service Model of Cloud Computing Environment", *Procedia Comput. Sci.*, vol. 87, pp. 246–251, 2016.
[14] P. Chavan, P. Patil, G. Kulkarni, R. Sutar et al, "IaaS Cloud Security", In Proceedings of the 2013 International Conference on Machine Intelligence and Research Advancement. IEEE, 2013, pp. 549–553.
[15] M. T. Sandikkaya and A. E. Harmanci, "Security Problems of Platform-as-a-Service (PaaS) Clouds and Practical Solutions to the Problems", In Proceedings of the IEEE 31st Symposium on Reliable Distributed Systems. IEEE, 2012, pp. 463–468.
[16] S. Soufiane and B. Halima, "SaaS Cloud Security: Attacks and Proposed Solutions", *Trans. on Machine Learning and Artificial Intelligence*, vol. 5, no. 4, pp. 291–301, August 2017.
[17] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, et al, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges", *IEEE Commun. Surv. Tut.*, vol. 20, no. 1, pp. 416–464, First Quarter 2018.
[18] P. Hu, S. Dhelima, H. Ning and T. Qiu, "Survey on Fog Computing: Architecture, Key Technologies, Applications and Open Issues", *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, November 2017.
[19] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues", In Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. IEEE, 2014, pp. 1–8.
[20] S. Khan, S. Parkinson and Y. Qin, "Fog Computing Security: A Review of Current Applications and Security Solutions", *J. Cloud Comput.*, vol. 6, no. 10, pp. 1–22, August 2017.
[21] P. Church, H. Mueller, C. Ryan, S. V. Gogouvitis, et al., "Migration of a SCADA System to IaaS Clouds – A Case Study", *J. Cloud Comput. Adv. Syst. Appl.*, vol. 6, no. 11, pp. 1–12, June 2017.
[22] Y. Chen, J. Chen and J. Gan, "Experimental Study on Cloud Computing Based Electric Power SCADA System", *ZTE Communications*, vol. 13, no. 3, pp. 33–41, September 2015.
[23] *Integrated Service Networks for Utilities*. CIGRÉ Technical Brochure TB 249, WGD2.07, 2004.
[24] B. Zhu, A. Joseph and A. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", In Proceedings of the International Conference on Internet of Things and the 4th International Conference on Cyber, Physical, and Social Computing. IEEE, 2011, pp. 380–388.
[25] Z. El Mrabet, N. Kaabouch, Has. El Ghazi and Ham. El Ghazi, "Cyber-Security in Smart Grid: Survey and Challenges", *Comput. Electr. Eng.*, vol. 67, pp. 469–482, April 2018.
[26] W. Gao, T. Morris, B. Reaves and D. Richey, "On SCADA Control System Command and Response Injection and Intrusion Detection", In Proceedings of the 2010 eCrime Researchers Summit. IEEE, 2010, pp. 1–9.
[27] A. Sajid, H. Abbas and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges", *IEEE Access*, vol. 4, pp. 1375–1384, April 2016.
[28] B. A. Akyol, "Cyber Security Challenges in Using Cloud Computing in the Electric Utility Industry", Technical Report PNNL 21724, Pacific Northwest National Laboratory, 2012. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-21724.pdf (accessed February 05, 2019).
[29] M. Stojanović, V. Aćimović-Raspopović and S. Boštjančič Rakas, "Security Management Issues for Open Source ERP in the NGN Environment", In *Enterprise Resource Planning: Concepts, Methodologies, Tools, and Applications*, vol. II, M. Khosrow-Pour, Ed. New York: IGI Global, 2013, pp. 789–804.
[30] K. Stouffer, J. Falco and K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82 Rev. 2, 2015.
[31] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, et. al, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems", *Comput. Secur.*, vol. 56, pp. 1–27, February 2016.
[32] N. Hossain, A. Hossain, T. Das and T. Islam, "Measuring the Cyber Security Risk Assessment Methods for SCADA System", *Glob. J. Eng. Sci. Res. Manag.*, vol. 4, no. 7, pp. 1–12, July 2017.
[33] A. Ahmed and A. S. Sabyasachi, "Cloud Computing Simulators: A Detailed Survey and Future Direction", In Proceedings of the 2014 IEEE International Advance Computing Conference (IACC). IEEE, 2014, pp. 866–872.
[34] M. Kamal, ICS Layered Threat Modeling, SANS Institute – Information Security Reading Room, March 2019. https://www.sans.org/reading-room/whitepapers/ICS/ics-layered-threat-modeling-38770 (accessed April 02, 2019).
[35] Y. Gui, A. S. Siddiqui and F. Saqib, "Hardware Based Root of Trust for Electronic Control Units", In Proceedings of the SoutheastCon 2018. IEEE, 2018, pp. 1–7.