PROCEEDINGS

of the

7th International Conference on

CONTROL AND OPTIMIZATION WITH INDUSTRIAL APPLICATIONS

Volume II

26-28 August, 2020
Baku, Azerbaijan

On some particularities of the wave propagation in the inhomogeneously pre-stressed hollow cylinder contained a compressible inviscid fluid . . . . . *S.D. Akbarov, G.J. Valiyev* 53

Torsion problem for the radially inhomogeneous sphere of small thickness . . . . . *S.B. Akbarova, S.A. Gasanova* 56

Asymptotic analysis of the torsion problem for the three-layer cylinder of small thickness with soft aggregate . . . . . *N. Akhmedov* 59

Conformational profiles of carnosine . . . . . *G.A. Akverdieva, I.N. Alieva, Z.I. Hajiyev, S.D. Demukhamedova* 62

Security issues of SCADA systems in cloud computing environment . . . . . *R.G. Alakbarov, M.A. Hashimov* 65

Constructing of optimal regulators for liquid damper's oscillatory systems . . . . . *F.A. Aliev, N.A. Aliev, N.A. Ismailov, Y.V. Mamedova* 68

Discretization method on movement equation of the oscillating system with liquid dumpers with variable coefficients . . . . . *F.A. Aliev, M.M. Mutallimov, E.H. Mammadhasanov, S.Y. Gasimov* 71

The dependence of full radiation flux on temperature in $\lambda > 912\mathring{A}$ region of central stars of planetary nebulae . . . . . *A.H. Alili, K.I. Alisheva* 74

Conception of neural network based adaptive e-governance system using aggregated opinions of public observers . . . . . *E.R. Aliyev, R.R. Rzayev, Kh.Kh. Abdullayev* 77

Combined energy management system . . . . . *I.M. Aliyev, O.M. Mirzayev* 80

The role of balance sheet in ensuring the financial stability of industrial enterprises . . . . . *R.M. Aliyev* 83

Advancement of court proceeding as a guarantee for the effective protection of human rights . . . . . *S.I. Aliyev, R.S. Rzayev* 86

Analysis of cybersecurity indicators: a case of Azerbaijan . . . . . *T. Aliyeva, A. Guliyeva, U. Rzayeva, G. Guliyeva* 89

Azerbaijan's economic policy is a sustainable person from capital to human progress . . . . . *D.I. Allahverdiyev* 92

Solution of the gas flowmeter selection problem for information-measuring system . . . . . *E.N. Allahverdiyev* 95

The 7th International Conference on Control and Optimization with Industrial Applications, 26-28 August, 2020, Baku, Azerbaijan

SECURITY ISSUES OF SCADA SYSTEMS IN CLOUD COMPUTING ENVIRONMENT

R.G. ALAKBAROV[1], M.A. HASHIMOV[1]

[1]Institute of Information Technology of ANAS, Baku, Azerbaijan
e-mail: rashid@iit.ab.az, mamedhashimov@gmail.com

ABSTRACT. The article examines the security issues of cloud-based SCADA (Supervisory Control and Data Acquisition) systems, which are widely used in monitoring and management of the oil and gas industry. It outlines the advantages of cloud-based SCADA systems over traditional SCADA systems. It analyzes the security issues that may arise when using SCADA system applications in the cloud environment.

1. INTRODUCTION

The SCADA system is widely used in the management of technological processes in the oil and gas industry. SCADA systems are industrial control and management systems that centrally manage and control geographically distributed technical devices. SCADA system collects data in real-time, performs local or remote control. The system provides comprehensive monitoring for production operation in real-time. With the help of the system, important reference information for production, control, and management is provided [9].

The amount of data generated by the automation of systems in the oil and gas industry and the deployment of various new sensors can be measured in millions of gigabytes. Traditional SCADA systems is not able to perform the requirements for big data analysis, accelerated processing, delays and network scalability. The usage of cloud-based SCADA systems in solving these problems can be considered a prospective solution.

2. MIGRATION TO CLOUDS AND SECURITY ISSUES

Cloud technologies are widely used to solve complicated problems based on computer networks and to create distributed computing systems for the management of technological processes. The systems with high computing and memory resources are created based on computer networks with high-speed communication channels. Utilizing high-speed communication channels, the usage of cloud computing services is more efficient for users of various organizations and enterprises [1]. Recently, cloud computing technologies are widely used in the management of various sectors of the oil and gas industry. Cloud computing technologies offer cloud services that provide data collection, storage, and processing for seismic exploration, drilling, production and management of other sectors.These services provides the creation and usage of computer technology infrastructure and software directly in a network environment.Through this technology, data is stored in cloud systems, processed, the running of processing programs and the review of results is provided [10]. Cloud computing technology provides group activity and distant visualization at the office of the oil company, its branches, and even remote areas. Recently, the amount of data generated in the oil and gas exploration and production sector has increased

significantly. Seismic data generated by seismic sensors is considered big data [11]. The study of seismic data is considered an important part of effective drilling management. An effective system for managing seismic data, as well as a high-productivity and large-capacity storage is required. Oil companies using cloud services can apply high-performance virtual machines to answer these requirements.

Thus, cloud-based SCADA systems play an important role in the effective management of the oil and gas industry. The cloud-based SCADA system has the following advantages comparing with traditional SCADA systems [2, 4]:

(1) The adding of new devices is provided to the system if required or needed. For the company, the obtaining, installing and running of software and hardware cost cheap.
(2) Users can easily obtain the additional resources they need on a cloud server without installing an additional device.
(3) Updating existing applications and adding new applications to the system is implemented easily.
(4) Easy access to memory resources for the storage of big data generated in system management.
(5) Ensuring system reliability and security by creating reserve servers in the cloud.
(6) The users access to data hosted on cloud servers connected to the Internet in real-time.
(7) Cloud-based SCADA systems allow for efficient use of resources, low energy consumption, also provide rapid deployment of new services and reduction of overall costs.

Thus, the transfer of traditional SCADA systems applications to the cloud environment allows us to reduce costs, increase the scalability and make it more attractive to users in terms of hardware. At the same time, the costs of obtaining, installing, maintaining the hardware and software required for monitoring and management systems are decreased by the reduction of technical staff. Despite the above-mentioned advantages, cloud-based SCADA systems have serious security risk factors. Overtime, out dated technologies in various fields are replaced by new ones, but unfortunately, only existing versions of available SCADA systems are improved to adapt to the capabilities of both old and new technologies. The combined use of both technologies puts the security of SCADA systems at risk. Forth is reason, as a result of the integration of satellite systems into the cloud concept, integrated SCADA systems have become more vulnerable to cyberthreats than the conventional SCADA systems.

Various articles [3, 7, 8] identifies security issues as a major problem in the integration of SCADA systems to the cloud.In this type of environment, we observe higher security risks, such as keeping confidential information out of the control of the organization.Cloud-based SCADA systems are exposed to the same cybersecurity risks as other cloud-integrated systems. Cyberattacks against SCADA systems can be classified as follows: hardware attacks, software attacks, and communication system attacks. The SCADA control center operates on the basis of information received from controllers (control devices). Attacks that make threats to process control are aimed at altering control data or obstructing data transmission. The following security risks exist in cloud-based SCADA systems [5, 6]:

(1) Due to cloud communication, SCADA systems are more public, thus the system commands and data can be modified, leaked, lost or copied during communication.

(2) Virtually as long as each cloud service provider stores the data on its own server, they are located on a common server used by hundreds or even thousands of other clients. In this case, the data is shared with others, intentionally or unintentionally.

(3) Since the network connection between SCADA systems and the cloud is implemented over the Internet, the data on communication channels may be compromised.

(4) SCADA systems integrated into cloud technologies may have all the same risks as in the cloud infrastructure.

(5) SCADA system applications used in the cloud can be easily found and used byattackers.

(6) Although SCADA systems use different protocols for management and automation purposes, some of these protocols have a number of security vulnerabilities. For example, Modbus and DNP3, the most common SCADA protocols, do not support authentication and encryption.

Open cloud migration requires the transmission of control over data, as well as control over components of the system that were previously under the direct control of the organization, to the control of the cloud provider. In this case, organizations that transfer data with high-security requirements to the cloud should determine together with the provider how that data will be managed and stored securely. Security risk management is a periodic process consisting of several stages: the analysis of risks by identifying vulnerabilities and threats, the estimation of risks, the decision-making on risk level, the identification and implementation of measures to reduce risks.

3. Conclusion

The use of cloud-based SCADA systems increases in order to automate systems, grow efficiency and income opportunities in the oil and gas industry.There arise various problems in data collection, transmission, and processing because of traditional SCADA systems being very expensive, inflexible, and complicated scalability. The transferring of the SCADA system's applications to the cloud environment reduces costs and improves scalability. Cloud-based SCADA systems have significant advantages and are vulnerable to security concerns. For this reason, its implementation is still not fully possible. With the right architecture and security, organizations can not only take advantage of cloud technology, but also increase it ssecurity. To this end, there is a need for additional research and gradual implementation of cloud migration.

4. Acknowledgment

This work was financed by the Scientific Fund of the State Oil Company of the Republic of Azerbaijan - Grant -No.03LR.

Keywords: Oil and Gas Industry, SCADA Systems, Cloud Computing, Security.

AMS Subject Classification: 68Mxx.

References

[1] Alguliyev R., Alekperov R., Cloud computing: modern state, problems and prospects, *Telecommunications and Radio Engineering*, Vol.73, No.3, 2013, pp.255-266.

[2] Church P., Mueller H., Ryan C., Gogouvitis S.V., Goscinski A., Haitof H., Tari Z., SCADA Systems in the Cloud, *Handbook of Big Data Technologies*, 2017, pp.691-718.

[3] Howard P.D., A Security Checklist for SCADA Systems in the Cloud, GCN, 2015.

[4] Is Moving Your SCADA System to the Cloud Right For Your Company, Cloud-Based SCADA Systems: The Benefits Risks, *White Paper*, 2011.

[5] Piggin R.S.H., Securing scada in the cloud: managing the risks to avoid the perfect storm, IET ISA 60th *International Instrumentation Symposium,* 2014.

[6] Sajid A., Abbas H., Saleem K., Cloud-assisted IoT-based SCADA systems security: a review of the state of the art and future challenges, *IEEE Access*, Vol.4, 2016, pp.1375-1385.

[7] Stojanovic M.D., Bostjancic Rakas S.V., Markovic-Petrovic J.D., Scada systems in the cloud and fog environments: migration scenarios and security issues, *Electronics and Energetics*, Vol.32, No.3, 2019, pp.345-358.

[8] Slay J., Miller M.M., A security architecture for SCADA networks, *17th Australasian Conference on Information Systems,* 2006.

[9] Yadav G., Paul K., Archutecture and security of SCADA systems: a revew, 2020. https://arxiv.org/abs/2001.02925

[10] Zhang Q., Cheng L., Boutaba R., Cloud computing: state-of-the-art and research challenges, *Journal of Internet Services and Applications*, Vol.1, 2010, pp.7-18.

[11] Zhifeng Y., Fei H., Xuehui F., Qi Y., Zhen C., Yidan Z., Cloud computing and big data for oil and gas industry application, *Journal of Computers*, Vol.14, No.4, 2019, pp.268-282.