SOCAR Proceedings

Computer-aided engineering and information technology

journal home page: http://proceedings.socar.az

APPLICATION PROBLEMS OF CLOUD-BASED SCADA SYSTEMS IN THE OIL AND GAS INDUSTRY

R. G. Alakbarov, M. A. Hashimov*

Institute of Information Technology, Ministry of Science and Education of the Republic of Azerbaijan, Baku, Azerbaijan

A B S T R A C T

SCADA (Supervisory Control and Data Acquisition) systems play an important role in the oil and gas industry providing real-time monitoring, control and data acquisition of critical infrastructure. Unlike traditional SCADA systems based on local hardware and software, cloud-based SCADA systems take advantage of cloud computing technologies for real-time data collection and management. Cloud-based SCADA systems offer many advantages due to their scalability, flexibility and cost-effectiveness. To take advantage of these advantages, it is required to solve a number of problems related to the application of cloud-based SCADA systems in the oil and gas industry. One of the most important application challenges is the cybersecurity issues arising in cloud-based SCADA systems, which are a significant concern due to the critical nature of the infrastructure they control. Thus, the systems face various vulnerabilities and threats that can destroy the data integrity and the system's availability. This article outlines the current cyber-attacks that can compromise the security of cloud-based SCADA systems. Threats and vulnerabilities in using cloud-based SCADA systems are analyzed, and suggestions are made that partially help to solve them. Some security mechanisms are recommended to ensure the security of cloud-based SCADA systems. These mechanisms will help increase the reliability and security of cloud-based SCADA system operations in the oil and gas industry.

Keywords: SCADA systems; cloud computing; cloud-based SCADA systems; SCADA security; cloud security.

© 2023 «OilGasScientificResearchProject» Institute. All rights reserved.

Introduction

SCADA systems are critical infrastructure systems for industrial enterprises that allow real-time data collection and management. SCADA systems refer to a type of industrial control systems that allow users to monitor and control industrial processes locally or remotely through sensors and actuators [1]. Traditional SCADA systems are very expensive, inflexible, difficult to scale, consequently many problems present in data collection, transmission and processing. The application of cloud-based SCADA systems can be considered a promising solution in solving these problems. A cloud-based SCADA system has several advantages over traditional ones. Cloud-based SCADA systems reduce the cost of purchasing, maintaining and upgrading physical servers, eliminating the need for extensive on-premise hardware and infrastructure. Adding new equipment to the system is easily ensured when needed or required. It costs a company less to buy, install, and run software and hardware. Cloud-based SCADA systems allow remote monitoring and control of industrial processes from anywhere with an internet connection. This is particularly useful for the oil and gas industry with geographically dispersed operations. Cloud service providers often perform system updates and maintenance tasks. This ensures that the SCADA system runs on the latest software versions without significant manual intervention.

Although cloud-based SCADA systems offer a number of advantages, its implementation in the oil and gas industry may face special challenges and risks. Many oil and gas industries have SCADA systems based on old technologies. Integrating these legacy systems with cloud-based solutions can be problematic, requiring updates or modifications to existing infrastructure.

The oil and gas sector often covers remote and geographically dispersed locations. Data transfer between these locations and the cloud can pose latency, potentially impacting real-time monitoring and management capabilities. Reliability of cloud services is crucial for SCADA systems, as any interruption can cause the operation to fail. Reliance on Internet connectivity and cloud provider infrastructure can pose a risk of operational disruptions to critical processes in the oil and gas industry.

Management programs of SCADA systems used to monitor critical infrastructure are deployed in the internal infrastructure of the organization and special software within the perimeter of the infrastructure protects its security. Organizations do not use the Internet to manage SCADA systems for security reasons. When SCADA systems were in their infancy, standard protocols and wired communications were used. At that time, the system only monitored and managed processes as a management system. After migrating these systems to a cloud computing environment, they became more vulnerable to cyber threats and attacks. When migrating SCADA applications to the cloud, security risks

E-mail: mamedhashimov@gmail.com

http://dx.doi.org/10.5510/OGP20230400928

must be considered in advance. The elimination of security flaws of a cloud-based system is impossible by taking advantage of the capabilities of available SCADA protocols. For example, Modbus and DNP3 protocols, which are widely used in current SCADA systems, do not support authentication and encryption or do not implement them at all [2]. On the other hand, if any device with an IP address connects to the Internet, it is vulnerable to cyberattacks that can occur in this IP-based environment. Thus, due to the lack of security measures in classic SCADA systems, migrating such systems to the cloud opens the door to potential security threats. Organizations should determine how robust they are to the aforementioned risks and then decide whether to migrate the system to a cloud infrastructure or not. Taking the above into consideration, the presented article examines the attacks, vulnerabilities, and ambiguities in cloud-based SCADA systems. Certain offers and mechanisms are developed for solving cyber security problems of cloud-based SCADA systems.

Security mechanisms prevent unauthorized persons from accessing the cloud-based SCADA system, data acquisition and manipulation by unauthorized entities, on the other hand, early detection of cyber security threats in SCADA systems, and elimination of potential threats in real time. This enables the minimization of damage, timely prevention of threats and quick recovery of operations. A properly implemented security strategy not only protects against potential threats, but also allows maximization of the benefits offered by cloud-based SCADA systems in the oil and gas industry.

Attacks involving cloud-based SCADA systems

Migrating traditional SCADA systems' applications to the cloud environment reduces costs, increases scalability and makes it more attractive for organizations (users) in terms of technical support. Moreover, it may reduce costs incurred due to the purchase, installation, maintenance of hardware and software for monitoring and management systems and lessen the number of technical staff [3]. Although reducing costs and increasing efficiency are key business conditions, ensuring security is one of the more important issues. Thus, data loss or theft, loss of control over the system must be balanced with the advantages of cloud-based SCADA systems.

Reasons why cloud-based SCADA systems are more vulnerable to cyber-attacks [2]:

- use of cloud services by SCADA systems;
- shared infrastructure;
- malicious insiders;
- security of SCADA protocols.

The traditional SCADA system was created as a closed control system without the Internet connection. When SCADA system is migrated to the cloud, data is exposed to threats in complex network environments that provide communication between SCADA systems and cloud services. Security threats increase when using public cloud services.

Shared infrastructure generates security risks in the equipment of other enterprises connected to the network infrastructure. Specifically, the same physical server can be shared with other competitors, companies or users, and sharing such resources will lead to many threats that will affect cloud-based SCADA systems running in critical and real-time applications.

Malicious insiders are considered to be the most destructive threat to any system, especially critical SCADA systems. Malicious insiders can be any former employees, system administrators, or cloud service providers. Unauthorized access can lead to various security threats, including data leakage and unauthorized control of industrial SCADA system sensors.

Another factor making cloud SCADA systems vulnerable is the lack of authentication and encryption mechanisms. As a result of poor authentication and encryption, communication protocols such as Modbus enable attackers to easily obtain personal information such as IP addresses, usernames and passwords when using the cloud.

Security-related attacks to cloud-based SCADA systems can be classified as common, software and internal attacks.

Common attacks. There are four main factors making cloud-based SCADA systems more vulnerable to insider attacks than traditional SCADA systems [4, 5]:

- using the same infrastructure resources with unknown external users can cause various threats to such systems;
- attackers can use vulnerable network connection between the SCADA system and the cloud to disrupt the management of the entire industrial enterprise;
- some SCADA protocols (Modbus and DNP3) do not support authentication and encryption;
- using unlicensed security solutions for SCADA systems causes various threats when SCADA systems are connected to cloud.

Software attacks. APTs (Advanced Persistent Threat), lack of data integrity, MITM (Man in The Middle) attacks and Denial-of-Service attacks (DoS) are the main software attacks on cloud SCADA systems. Attackers use other malware to create threats to accessibility (DDoS attacks), integrity (malware injection), and privacy (infrastructure data discovery) [6]:

- *Advanced Persistent Threat (APTs).* APTs are network attacks in which an unauthorized person attempts to gain access to a system using zero-day attacks to steal data instead of damaging it [7]. APTs can be performed when an attacker or a group of attackers gain unauthorized access to the system network to obtain highly sensitive data. A zero-day attack is a hardware or software vulnerability that is unknown to the party responsible for fixing the vulnerability.

Typically, when someone discovers a potential security problem in a program, they notify the software company about it so that action can be taken before it's too late. In this case, the software vendor can fix the fault code in a short time and distribute it in the updated software, and even if a potential attacker is aware of the vulnerability, he can no longer exploit it. However, sometimes a hacker may be the first to discover a vulnerability. Since the vulnerability is not known in advance, there is no way to avoid such situations. APTs are often executed when an intruder is in standby mode and exploits zero-day vulnerabilities in the system. Zero-day vulnerabilities occur shortly after system or software development and installation, enabling a successful attack without detection.

- *Lack of data integrity*. Data integrity is lost when the original data is destroyed and this is done by any means such as physical interference or interception.
- *MiTM attacks.* An attacker can launch attacks after positioning himself between the cloud user and the cloud application using two methods. Attacks are carried out in

two ways: spoofing attack and sniffing attack. In a spoofing attack, an attacker gains access to cloud-based SCADA systems using the name of other cloud users to bypass security and gain access to control systems or steal data. In a sniffing attack, an attacker can intercept data packets in a cloud-based SCADA system network and monitor them, thereby capturing sensitive data such as passwords and personal information [8].

• *DoS attacks* make the intended service unavailable to users by using two methods: flooding the targeted system with traffic, sending data that causes a crash in the targeted system [9].

• *Ransomware attacks* can encrypt critical data in the SCADA system and charge for a decryption key. This effectively blocks the system and prevents access to important information.

• *Phishing attacks* can trick users (by sending a fake email) to get sensitive information such as usernames, passwords or access codes. An attacker can gain unauthorized access to SCADA systems through obtained data and use it to manipulate operations.

Internal attacks. SCADA system managers are often unable to maintain a high level of data privacy due to limited security capabilities. Therefore, other cloud users take advantage of security vulnerabilities and get unauthorized data [10]. Due to the increase in the number of devices connected to cloud SCADA systems, there is an increase in the number of access points without effective authentication mechanisms, which leads to data capture in enterprise networks, enterprise confidence disclosure, illegitimate access and interventions in the enterprise system [11].

There are many management vulnerabilities in the cloud-based SCADA systems emerged in network environments. Some of them that may hinder the operation of SCADA systems are mentioned below [12-16]:

1. The use of the same cloud resources (servers) by different customers creates an opportunity for intrusions.

2. Since the network connection between the SCADA systems and the cloud is implemented via the Internet, data in the communication channels may be subject to attacks.

3. Many SCADA systems use commercially available off-the-shelf security solutions instead of exclusive ones.

4. Cloud applications of SCADA systems can be easily found by attackers and used for malicious purposes.

5. Cloud-based SCADA system applications can be easily intercepted and misused by attackers.

6. Due to the increased number of equipment connected to cloud-based SCADA systems, its perimeter is expanded, and as a result, attackers can be provided with a wider scope. In this case, the risks also increase. Therefore, organizations should always take security measures.

7. Providing access from any point of the world makes it vulnerable to malicious attacks such as a Distributed Denial-of-Service (DDoS) attack.

8. Migration of data to the cloud may also lead to the loss of direct control over them.

9. SCADA systems integrated into cloud technologies may have all the risks of cloud infrastructure.

10. Since cloud-based SCADA systems are more public, system commands and data can be changed, lost or copied during communication.

The aforementioned vulnerabilities are the basis of cloud-based SCADA systems being exposed to threats that adversely affect their performance. Many efforts have been made in terms of security solutions, protection mechanisms and security approaches to prevent SCADA systems from the aforementioned threats (vulnerabilities).

Threats and vulnerabilities of cloud-based SCADA systems

Organizations must continuously monitor for security vulnerabilities to protect SCADA applications and ensure performance. Consequently, very little time is spent on eliminating the vulnerabilities mentioned in the management and control systems. Risk assessment should encourage the decision-making process of migrating SCADA applications to the cloud. One of the main challenges in this area is that as threats have increased, both the number and scope of attacks have expanded. These attacks are mainly targeted at security systems. Obviously, if we look at the attack vector, we can see how breaches occur and how hackers get access to the system. In some cases, failures in ensuring security of cloud-based SCADA environment connections occur as a result of access to multiple equipment and systems by employees using those systems. Typically, such cases arise when system employees are aimed by attackers through their own laptops or phone devices. Once the organization decides to migrate the system to cloud, a service provider must be appointed. Every cloud service provider must be able to meet security control requirements. For SCADA applications, it is also important to ensure a high level of security mechanisms and processes. In fully cloud-based SCADA systems, applications are completely hosted in cloud. This application generates traffic and sends it to the controllers located at the customer's premises for further processing. There are two main security risks in this type of architecture [1, 17]:

1. While being transmitted from SCADA system devices to the cloud, real-time data or commands are seized, read, falsified, denied, or changed into various forms depending on the skill of the attacker.

2. An internal connection is established through a network gateway by sending commands from the cloud-based application to the on-site devices of the internal SCADA environment. This required connection opens the way to the internal network, which is considered unacceptable, since it enables hackers to find their way into the network.

When migrating traditional SCADA systems to cloud infrastructure, equipment and communication protocols used in them suffer from security issues. This creates problems in system management. Therefore, the infrastructure of cloud-based SCADA systems needs to be constantly improved. SCADA system networks can be improved in three ways, taking into account the main problems, as shown below [18, 19]:

1. Security of SCADA systems within the network can be improved by using intrusion detection systems and keeping firewalls up to date, thereby keeping system performance under constant control.

2. Security management of SCADA systems can be improved by conducting regular risk assessments and enhancing security plans and their implementation.

3. Access control for SCADA systems can also be improved. The first step in securing any system is to prevent unauthorized access to the system.

When organizations use cloud-based SCADA systems,

users should consider some of the following issues [15, 20, 21]:

Lack of control. Since cloud-based SCADA systems are hosted on remote servers, the organization has limited control over the physical security of the infrastructure. By migrating data to the cloud, the organization's ownership on that data is transferred to the cloud service provider.

Data breach. Cloud-based SCADA systems store sensitive data such as process and system configuration on remote servers. If these servers are compromised, attackers can access and manipulate this data, damaging the production processes.

Lack of authentication. Some SCADA protocols do not support or implement authentication. If these systems use the cloud via weak communication protocols such as Modbus, an attacker can easily gain access to IP addresses, usernames, and other personal credentials due to weak authentication and encryption.

Internal threats. Employees or contractors with access to cloud-based SCADA systems can harm the organization by intentionally or unintentionally accessing or altering sensitive data.

Malware attacks. Cloud-based SCADA systems can suffer from malware attacks, which can lead to unauthorized access and control of industrial processes.

Interoperability issues. Cloud-based SCADA systems often involve the integration of different components from different vendors, which can result in compatibility issues and vulnerabilities.

Lack of encryption. Just as authentication, any type of encryption essential for data protection are not supported by SCADA protocols. Modbus and DNP3 protocols also do not support any type of encryption, making the traffic more vulnerable to MiTM attacks.

Inadequate security controls. Cloud-based SCADA systems require robust security controls to prevent unauthorized access and protect sensitive data. Failure to implement these controls can result in vulnerabilities that can be exploited by attackers.

Lack of transparency. When using cloud-based SCADA systems, it can be difficult to gain complete information about the security status of the system due to the distributed character of the infrastructure. This lack of transparency can make it difficult to detect and respond to security incidents.

To ensure the security of cloud-based SCADA systems, the methods and techniques such as log analysis, network traffic analysis, using tools to detect routine malicious activities, implementing regular vulnerability testing, conducting continuous monitoring and analysis, implementing file integrity and executing proxy solutions should be required [22].

When evaluating the capabilities of a cloud provider offering the creation of cloud-based SCADA systems, the followings should be taken into account [1, 23]:

1. Determining the extent to which customers control the changes made to the provider's network infrastructure: for example, customers must be constantly notified when updates are made to internal infrastructure.

2. Ensuring that the cloud provider regularly encrypts the user's data.

3. Ensuring the distribution of the software vulnerabilities among users once they are eliminated by the supplier.

4. Opportunities to take necessary measures immediately after detecting a vulnerability.

5. Ability to collect and analyze all log data and detect, respond to and analyze threats, incidents, and abnormal activity in real time.

6. Awareness of the provider about its obligation to immediately correct all identified vulnerabilities.

7. Determining the availability of adequately trained, dedicated security personnel.

8. Ensuring reliable customer service to be provided.

The most effective means of securing a cloud-based SCADA application is to establish an effective, mutual service-level agreement between the user and the provider covering the abovementioned issues.

Thus, migrating SCADA applications to the cloud is a new management strategy that requires caution. While the savings and increased efficiency are undeniable, organizations must ensure that their critical data is secured by cloud providers.

Security mechanisms in cloud-based SCADA systems

Given the increased security risks when migrating SCADA to the cloud, any organization should take a number of measures to ensure the its data security. The following mechanisms and recommendations are proposed to solve the security problems that arise during threats to cloud-based SCADA systems [15, 20, 24, 25]:

- Access control. These mechanisms should be implemented to ensure that only authorized personnel access the SCADA system. This includes password policies, the use of multi-factor authentication to ensure authenticity. It is recommended to use strong passwords and change them regularly to prevent unauthorized access.
- Encryption. This can protect the confidentiality and integrity of data transmitted over a network. For this, the use of secure protocols such as SSL/TLS (Secure Sockets Layer / Transport Layer Security) and the use of strong encryption algorithms are recommended.
- Symmetric encryption. It is recommended to use AES (Advanced Encryption Standard) symmetric encryption algorithms, which use a single key for both encryption and decryption, ensure fast and efficient data protection.
- Asymmetric Encryption. These algorithms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are used to ensure data security. This algorithm uses a pair of public and private keys for encryption and decryption, respectively. Although asymmetric encryption is slower than symmetric encryption, it offers better security and management capabilities.
- Homomorphic encryption. This allows to perform calculations (operations) on encrypted data without the need for decryption, ensuring secure data processing in multi-use cloud environments.
- Secure communication protocols. These protocols are essential for protecting the data sharing between the various components of a cloud-based SCADA system. In this regard, it is recommended to use the popular TLS protocol, which provides secure data transmission over networks by encrypting data and ensuring authentication, integrity and confidentiality.
- Intrusion detection and prevention systems. It is recommended to use the IDPS protocol to detect and prevent unauthorized access and malicious intrusions (activities) within a cloud-based SCADA system.
- Security information and incident management. The proposed SIEM (Security Information and Event Management)

protocol collects and analyzes security events and logs from various sources within a cloud-based SCADA system, providing real-time threat detection, incident response and compliance reporting.

• Protection systems against critical threats and cyber-attacks. It is recommended to use intrusion detection system (IDS – Intrusion Detection System) and intrusion prevention system (IPS – Intrusion Prevention System) to protect against critical threats and cyber-attacks. Examples of these are machine learning-based IDS, deep learning-based IDS, artificial neural networks-based IDS, etc. can be shown [24].

• Log analysis. Activity logs (log files) are stored by almost all computer programs and devices. Tracking through these logs can identify and manage many attacks. Such log analysis is typically supported by a host-based IDS.

• Continuous monitoring. Continuous monitoring of a SCADA system identifies potential security threats and mitigate them before they can be exploited by attackers.

• File integrity monitoring. File integrity analysis checks the integrity of some software and operating systems. The cryptographic verification method is the most commonly used verification method. File integrity can be easily determined using checksum methods of malicious files (blacklists) and authorized files (whitelists).

• Network segmentation. Network segmentation isolates important parts of a system from less important ones. This limits the impact of a security incident and can prevent attackers from gaining access to critical systems.

• Using vulnerability detection tests. Unknown errors in cloud systems are easily detected with continuous monitoring and vulnerability testing. These tests can be applied either to the entire system or to specific system components. Over time, tests should be performed regularly, as new threats are discovered during analysis.

• Using virtual private clouds. Cloud service providers do not guarantee that the hardware infrastructure will not be shared with other users. Resource sharing can cause many disruptions for critical and real-time applications. This problem can be solved by creating virtual private clouds.

• Protection of virtual machines. Security mechanisms must be implemented to protect the virtual machines used in the SCADA system from security threats. These may include the use of antivirus software, intrusion detection and prevention, and vulnerability detection.

• Distributed Denial of Service (DDoS) Attacks. Cloud-based SCADA systems are also vulnerable to DDoS attacks, which can overload the network with unnecessary traffic and make it inaccessible to required data. This can have serious implications for critical infrastructure systems. Prevention of these attacks requires the use of techniques such as traffic rate limiting and filtering.

• Ensuring cloud infrastructure availability. Cloud infrastructure failure can make it unavailable for a long time. Such an event can be disastrous for any service-using enterprise, especially for SCADA control systems. In order to prevent such cases, it is suggested to save data backup options in a certain region.

• Blockchain-based security mechanisms. Blockchain technology is a decentralized, tamper-resistant technology used to increase the security of cloud SCADA systems. Blockchain-based solutions improve data integrity, access control, and auditability [25].

• Data backup and recovery. SCADA system data should be regularly backed up and stored in a secure location. This enables an organization to recover its data in case of a disaster or cyber-attack.

• Ensuring safety training. Employees should be trained in best security practices and how to recognize potential security threats. This may prevent human-related security incidents.

• Organization of physical security measures. Only authorized personnel should be allowed physical access to the SCADA system. Physical security measures such as access control, surveillance cameras, and alarms should be realized to prevent unauthorized access to the system.

• Conducting security audits. Regular security audits can be performed to ensure the system security and effective work of all security mechanisms. Security audits can also identify any security breaches in the system.

• Disaster recovery and performance continuity. Disaster recovery and performance continuity plans should be developed so that the organization can recover from any security incidents or disasters. These measures may include regular backup of critical data and systems, offsite backups, and regular testing of disaster recovery and business continuity plans.

• Third-party risks: Cloud-based SCADA systems often rely on third-party service providers, such as cloud providers, network providers, and software providers, to operate. Organizations must ensure that these third-party providers have robust security measures in place and adhere to industry standards and regulations.

Along with the methods proposed above, in order to ensure a high level of security of cloud-based SCADA systems, it is necessary to regularly use and update intrusion detection and prevention systems, antivirus programs, and bring up-to-date attack patterns in the database.

Conclusion

To protect organizations' SCADA software, they must continuously monitor it for security, keep track of recorded vulnerabilities, and regularly make suggestions for their elimination. Unlike most IT systems, SCADA systems require a different approach, and there is less time to remediate vulnerabilities. In cloud-based SCADA systems, the presence of risks should be minimized to zero. The results of these risk assessments should be ensured by providers to help organizations make the right decision to migrate their SCADA applications to the cloud. If the information security risk is evaluated in the same way as the criteria of cost, efficiency and reliability, then the decision to migrate the system to the cloud will be right. Once the organization decides to migrate to the cloud system, it must identify a service provider. Any cloud provider should be able to satisfy the user's security requirements. The provider must have strong security mechanisms to ensure the security of the SCADA applications to be deployed in cloud.

This work was supported by the Science Foundation of the State Oil Company of the Azerbaijan Republic (Contract No.3 LR-AMEA).

References

1. Stojanović, M. D., Boštjančič Rakas, S. V., Marković-PetroviC, J. D. (2019). Scada systems ın the cloud and fog envıronments: mıgratıon scenarıos and securıty ıssues. *Electronics and Energetics*, 32(3), 345–358.

2. Alshehry, F. F., Wali, A. M. (2022). Analysis of security challenges in cloud-based SCADA systems: A survey. *TechRxiv. Preprint.*

3. Alakbarov, R. K., Hashimov, M. A. (2020). Migration issues of SCADA systems to the Cloud Computing Environment (review). *SOCAR Proceedings*, 3, 155-164.

4. Alakbarov, R. K., Hashimov, M. A. (2018). Application of the internet of things in oil-gas industry. In: *6th International Conference on Control and Optimization with Industrial Applications.*

5. Nazir, S., Patel, S., Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70, 436-454.

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

7. Bere, M., Muyingi, H. (2015). Initial investigation of industrial control system (ICS) security using artificial immune system (AIS). In: *International Conference on Emerging Trends in Networks and Computer Communications (ETNCC).*

8. Cagalaban, G., Kim, T., Kim, S. (2008). Improving SCADA control systems security with software vulnerability analysis. In: *12th WSEAS International Conference on Automatic Control, Modelling & Simulation.*

9. Davis, C., Tate, J., Okhravl, H., et al. (2006). SCADA cyber security testbed development. In: *38th North American Power Symposium.*

10. Kang, U., Chau, D., Faloutsos, C. (2012). Pegasus: mining billion-scale graphs in the cloud. In: I*EEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Kyoto, Japan.*

11. Shen, J., Xu, J., Cai, K., Ji, Y. (2021). Access point authentication scheme of Scada system based on cloud computing technology. *Journal of Physics: Conference Series, IOP Publishing,* 1748(2), 1-6.

12. Alakbarov, R. Q., Hashimov, M. A. (2014). Possibilities and prospects of using cloud technologies in the electronic government. In: *First Republic Scientific-Practical Conference on E-Science Problems.*

13. Piggin, R. S. H. (2014). Securing SCADA in the cloud: managing the risks to avoid the perfect storm. In: *IET & ISA 60th International Instrumentation Symposium.*

14. Kyle,W. (2013). SCADA in the cloud a security conundrum?. *Trend Micro Incorporated Research Paper*. https://blog. trendmicro.com/trendlabs-security-intelligence/scada-in-the-cloud a-security-conundrum/

15. Alakbarov, R., Hashimov, M. (2022). Security issues of cloud-based SCADA systems. *NATO Science for Peace and Security Series - D: Information and Communication Security,* 62, 1-8.

16. Alakbarov, R. K., Hashimov, M. A. (2020). Security issues of SCADA systems in cloud computing environment. In: *7th International Conference on Control and Optimization with Industrial Applications.*

17. Fernandez, J., Fernandez, A. (2005). SCADA systems: vulnerabilities and remediation. *Journal of Computing Sciences in Colleges*, 20(4), 160-168.

18.Nazir, S., Patel, Sh., Patel, D. (2020). Cloud-based autonomic computing framework for securing SCADA systems /in book: Innovations, Algorithms, and Applications in Cognitive Informatics and Natural Intelligence. *IGI Global.*

19. Igure, V., Williams, R. (2006). Security and SCADA protocols. In: *5th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC HMIT).*

20. Alakbarov, R., Hashimov, M. (2020). Security issues in cloud-based SCADA systems. *Information Technology Problems*, 2, 3-12.

21. Wang, Y. (2012). SCADA: Securing SCADA infrastructure communications. *International Journal of Communication Networks and Distributed Systems*, 6(1), 59-78.

22. Alakbarov, R. (2021). Cloud-based electronic government system: state-of-the-art, problems and security issues. *Information Society Problems*, 1, 18-31.

23. Howard, P. A. (2015). Security checklist for SCADA systems in the cloud. https://gcn.com/cloud-infrastructure/2015/06/ a-security-checklist-for-scada-systems-in-the-cloud/287164/

24. Ferrag, M. A. Babaghayou, M. Yazici, M. A. (2020). Cyber security for fog-based smart grid SCADA systems: solutions and challenges. *Journal of Information Security and Applications*, 52, 102500.

25. Cui, L., Xie, G., Qu, Y., et al. (2018). Security and privacy in smart cities: challenges and opportunities. *IEEE Access*, 6, 46134–46145.

Проблемы применения облачных SCADA-систем в нефтегазовой отрасли

Р. Г. Алекперов, М. А. Гашимов
Институт Информационных Технологий, Министерство Науки и Образования
Азербайджанской Республики, Баку, Азербайджан

Реферат

Системы SCADA (Supervisory Control and Data Acquisition) играют важную роль в нефтегазовой отрасли, обеспечивая мониторинг, контроль и сбор данных критической инфраструктуры в режиме реального времени. В отличие от традиционных систем SCADA, основанных на локальном аппаратном и программном обеспечении, облачные системы SCADA используют преимущества технологий облачных вычислений для сбора данных и управления ими в реальном времени. Облачные системы SCADA предлагают множество преимуществ благодаря своей масштабируемости, гибкости и экономической эффективности. Чтобы воспользоваться этими преимуществами, необходимо решить ряд задач, связанных с применением облачных SCADA-систем в нефтегазовой отрасли. Одной из наиболее важных проблем применения являются проблемы кибербезопасности, возникающие в облачных системах SCADA, которые вызывают серьезную озабоченность из-за критического характера инфраструктуры, которую они контролируют. Таким образом, системы сталкиваются с различными уязвимостями и угрозами, которые могут нарушить целостность данных доступность системы. В данной статье описаны текущие кибератаки, которые могут поставить под угрозу безопасность облачных систем SCADA. Проанализированы угрозы и уязвимости при использовании облачных систем SCADA и предложены некоторые решения. Для обеспечения безопасности облачных систем SCADA рекомендуются некоторые механизмы безопасности. Эти механизмы помогут повысить надежность и безопасность работы облачных SCADA-систем в нефтегазовой отрасли.

Ключевые слова: SCADA-системы; облачные вычисления; облачные SCADA-системы; SCADA-безопасность; облачная безопасность.

Bulud əsaslı SCADA sistemlərinin neft-qaz sənayesində tətbiqi problemləri

R. Q. Ələkbərov, M. A. Həşimov
İnformasiya Texnologiyaları İnstitutu, Azərbaycan Respublikası
Elm və Təhsil Nazirliyi, Bakı, Azərbaycan

Xülasə

SCADA (Supervisory Control and Data Acquisition) sistemləri kritik infrastrukturun real vaxt rejimində monitorinqini, idarə edilməsini və məlumatların əldə edilməsini təmin etməklə neft-qaz sənayesində mühüm rol oynayır. Lokal aparat və proqram təminatına əsaslanan ənənəvi SCADA sistemlərindən fərqli olaraq, bulud əsaslı SCADA sistemləri real vaxt rejimində məlumatların toplanması və idarə edilməsi üçün bulud hesablama texnologiyalarından istifadə edirlər. Bulud əsaslı SCADA sistemləri miqyaslılığı, çevikliyi və qənaətcilliyi sayəsində bir çox üstünlüklər təklif edir. Bu üstünlüklərdən yararlana bilməsi üçün bulud əsaslı SCADA sistemlərinin neft-qaz sənayesində tətbiqi ilə bağlı bir sıra problemlərin həll edilməsi tələb olunur. Tətbiqlə bağlı ən əsas problemlərdən biri isə bulud əsaslı SCADA sistemlərində yaranan kibertəhlükəsizlik məsələləri onların nəzarət etdikləri infrastrukturun kritik xarakterinə görə əhəmiyyətli narahatlıq doğurur. Çünki sistemlər məlumatların bütövlüyünü, sistemin əlçatanlığını poza biləcək müxtəlif zəifliklər və təhdidlərlə üzləşirlər. Məqalədə də bulud əsaslı SCADA sistemlərinin təhlükəsizliyinə mane ola biləcək mövcud kiberhücumlar göstərilmişdir. Bulud əsaslı SCADA sistemlərinin istifadəsində meydana çıxan təhdidlər və boşluqlar analiz edilmiş, onların həllinə qismən kömək edən təkliflər verilmişdir. Bulud əsaslı SCADA sistemlərinin təhlükəsizliyini təmin etmək üçün bəzi təhlükəsizlik mexanizmləri tövsiyyə edilmişdir. Bu mexanizmlər neft-qaz sənayesində bulud əsaslı SCADA sistemlərinin əməliyyatlarının etibarlılığını artırmağa və təhlükəsizliyini təmin etməyə kömək edəcək.

Açar sözlər: SCADA Sistemləri; Bulud hesablamaları; Bulud əsaslı SCADA Sistemləri; SCADA təhlükəsizliyi; bulud təhlükəsizliyi.