2023 5th International Conference on Problems of Cybernetics and Informatics (PCI) | 979-8-3503-1906-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/PCI60110.2023.10325946

Development of Security Mechanisms in Cloud Based SCADA Systems

Rashid Alakbarov
Institute of Information Technology,
Ministry of Science and Education
Republic of Azerbaijan
Baku, Azerbaijan
t.direktor_muavini@iit.science.az

Mammad Hashimov
Institute of Information Technology, Ministry of Science and
Education Republic of Azerbaijan
Baku, Azerbaijan
mamedhashimov@gmail.com

***Abstract*—Moving SCADA (Supervisory Control and Data Acquisition) applications used to monitor critical infrastructure to the cloud can reduce costs, rise scalability and make it more beneficial for organizations (users) in terms of technical support. While cost reduction and efficiency gains are key to business, security is one of the most important issues. The article analyzes the threats and vulnerabilities that can interfere with the security of cloud SCADA systems. Several cybersecurity mechanisms have been developed to secure cloud SCADA systems.**

Keywords—SCADA systems, Cloud computing, cloud-based SCADA systems, SCADA security, Cloud security.

I. Introduction

SCADA systems are critical infrastructure systems for industrial enterprises that allow real-time data collection and management. SCADA systems refer to industrial control systems that enable users to display and regulate industrial processes in the vicinity or at distant by means of sensors and actuators [1]. They gather information in real time and accomplishes local or remote control. Comprehensive real-time performance monitoring is realized by the systems. They also ensure vital data for production, control and administration. They are mainly applied by industries such as power systems, oil production and refinery, natural gas distribution, water and wastewater treatment, as well as transportation structures [2]. 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 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 [3]. On the other hand, if any device with an IP address connects to the Internet, it is vulnerable to cyber-attacks which can arise in this IP-based medium. Thus, the absence of security measures in classic SCADA systems, migrating these systems to cloud makes favorable conditions for possible 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.

II. Related Works

The article [3] analyzed the most common attacks and cybersecurity challenges faced in cloud-based SCADA systems. It also performs a security risk assessment of the analyzed attacks. Finally, it suggests the appropriate detection and prevention techniques available to mitigate the impact of cyber-attacks on these critical control systems. [4] highlights security issues as the main complications arising when integrating the SCADA systems to cloud. In such a medium, security risks such as keeping confidential information out of the organization’s control are estimated to be higher. [1] focuses on cyber security as the main risk factor during the migration of SCADA systems to the cloud environment. In this regard, further research and gradual implementation of migration is required. The study shows some progress made in this area, but also some challenges still remain unsolved. [5] explores security issues in the field of data storage in cloud servers and proposes a method to prevent unauthorized access to user (organization) data by cloud administrators. Along with the changes made in modern SCADA architectures, [6] mentions some following problems to be solved: a) providing large-scale control through multiple sensors; b) minimizing the time required to prevent any attack or incident detected; c) ensuring interoperability between SCADA systems in order to prevent incidents. In this regard, it is proposed to use sensor clouds to monitor large-scale and interdependent critical infrastructures. [7] extensively analyzes the architecture of traditional and modern SCADA systems. It classifies the attacks against SCADA systems. Several studies provide recommendations for the security of SCADA systems and information on the most effective practices in this area. [8] analyzes the attacks against SCADA systems, and as a result, explores existing security vulnerabilities that could hinder the operation of the industrial SCADA system in cloud environment.

III. Attacks Involving Cloud-Based SCADA Systems

Migrating traditional SCADA systems’ applications to cloud medium 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. 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.

Below are the reasons why cloud-based SCADA systems are more vulnerable to cyber-attacks [3]:

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

Traditional SCADA system is created as in the form of closed control system without the Internet connection. When SCADA system is migrated to cloud, data becomes unprotected from threats in compound network mediums that provide communication between SCADA systems and cloud services. When using public cloud services, security threats increase.

Shared infrastructure generates security risks in the equipment of other enterprises connected to the network infrastructure. Specifically, the identical physical server can be used by other participants, businesses or users, and using these resources can lead to various threats that will affect cloud-based SCADA systems running in vital and real-time applications. Malevolent insiders are the most destructive danger to any system, particularly for critical SCADA.

Malevolent insiders may include any previous personnel, system administrators, or cloud service providers. Unauthorized access can lead to various security threats, including data leakage and unsanctioned control of industrial SCADA system sensors.

Other reasons making cloud SCADA systems to be exposed may include the absence of authentication and encryption mechanisms. Poor authentication and encryption can result in such a situation where communication protocols such as Modbus enable attackers to easily obtain personal information, e.g., IP addresses, usernames, passwords when using cloud.

There are many management weaknesses in the cloud-based SCADA systems emerged in network environments. Some of them that may hinder SCADA systems running, which are mentioned below [9 - 13]:

1. The use of identical cloud resources (servers) by diverse 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 amount of equipment linked to cloud-based SCADA systems, its boundary is expanded, consequently, a wider scope becomes a target of attackers. Increasing the risks as well. Hence, security measures should always be taken by organizations.

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. Data migration to cloud may also cause 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).

IV. 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 cloud. With the increased number of threats in this field, which is regarded as a vital problem, the number and scope of incidents have also expanded.

Users should always consider some of the following issues when businesses apply cloud-based SCADA systems [12, 14]:

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. Data migration to cloud lead to the organization's ownership on that data to be shifted to cloud service provider.

Data breach: SCADA systems based on cloud 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: Authentication may not be supported or implemented by some SCADA protocols. When these systems use cloud via weak communication protocols such as Modbus, an attacker can effortlessly access 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: SCADA systems based on cloud often involve the integration of different components from different vendors, which can result in compatibility issues and vulnerabilities.

Lack of encryption: Just as authentication, many encryption types essential for data protection are not supported by SCADA protocols. For example, Modbus and DNP3 protocols do not support any encryption forms, making the traffic vulnerable to MiTM (Man-in-the-middle).

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

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.

V. Security Mechanisms in Cloud-Based SCADA Systems

Given these increased safety risks when migrating SCADA to the cloud, any organization should take several measures to provide the its data safety. The following mechanisms and recommendations are proposed to solve the security problems that arise during threats to cloud-based SCADA systems [12, 14 - 16]:

- **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.

- **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.

- **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.

- **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.

- **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.

VI. 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. Taking into account the above mentioned, submitted article systematically highlights numerous weaknesses in the control of SCADA systems which are based on cloud and built in network environments. Organizations are recommended to consider security issues when using cloud-based SCADA systems. The article offers mechanisms, recommendations, and encryption software for organizations to address security issues when threats to cloud-based SCADA systems arise.

ACKNOWLEDGMENT

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

REFERENCES

[1] M. D. Stojanović, S. V. Boštjanĉiĉ Rakas, and J. D. Marković-PetroviC, "Scada systems ın the cloud and fog envıronments: mıgratıon scenarıos and securıty ıssues," Electronics and Energetics, vol. 32, no. 3, 2019, pp. 345-358.

[2] R. G. Alakbarov, and M. A. Hashimov, “Migration issues of SCADA systems to the cloud computing environment (REVIEW),” SOCAR Proceedings, no. 3. 2020, pp. 155-164.

[3] F. F. Alshehry, and A. M. Wali, "Analysis of Security Challenges in Cloud Based SCADA Systems: A Survey," TechRxiv. Preprint. – 2022, https://doi.org/10.36227/techrxiv.20291835

[4] Honeywell Process Solutions. Securing SCADA in the cloud, 2019. https://www.processonline.com.au/content/software-it/article/securing scada-in-the-cloud417777075

[5] Z. E. Mrabet, N. Kaabouch, and H. E. Ghazi, “Cyber-Security in Smart Grid: Survey and Challenges,” Computers & Electrical Engineering, vol. 67, 2018, pp. 469–482.

[6] B. D. Yosra, D. Yacine, R. Slim, and B. Noureddine, “A Novel Sensor Cloud Based SCADA infrastructure for Monitoring and Attack prevention,” MoMM '16: Proceedings of the 14th International Conference on Advances in Mobile Computing and Multi Media, November 2016, p. 45–49. https://doi.org/10.1145/3007120.3007169

[7] G. Yadav, and K. Paul, “Archıtecture and Securıty of Scada Systems: a Revıew // 2020. https://arxiv.org/abs/2001.02925

[8] F. Zakuan, J. Norziana, S. Q Qais, E. R Mohd, J. Norhamadi, D. Maslina, and H. HafizahChe, “A Study on Security Vulnerabilities Assessment and Quantification in SCADA,” Journal of Engineering and Applied Sciences, vol. 13, no. 6, 2018, pp. 1338–1346.

[9] R. Q. Alakbarov, and M. A. Hashimov, "Possibilities and prospects of using cloud technologies in the electronic government," The First Republic scientific-practical conference on e-science problems, Baku, 2014. p. 132-135.

[10] R. S. H. Piggin, “Securing scada in the cloud: managing the risks to avoid the perfect storm” IET & ISA 60th International Instrumentation Symposium, 2014, p. 1-6. doi: 10.1049/cp.2014.0535

[11] W. Kyle, “SCADA in the Cloud A Security Conundrum?,” Trend Micro Incorporated Research Paper, 2013, https://blog.trendmicro.com/trendlabs-security-intelligence/scada-in-the cloud a-security-conundrum/

[12] R. Alakbarov, and M. Hashimov, “Security Issues of Cloud-Based Scada Systems,” NATO Science for Peace and Security Series - D: Information and Communication Security. vol. 62, 2022, pp. 1-8. doi:0.3233/NICSP2200.

[13] R. K. Alakbarov, and M. A. Hashimov, "Security issues of SCADA systems in cloud computing environment," Proceedings of the 7th International Conference on Control and Optimization with Industrial Applications, 2020, p. 65-67.

[14] Y. Wang, “sSCADA: Securing SCADA infrastructure communications,” International Journal of Communication Networks and Distributed Systems, vol. 6, no. 1, 2012, pp. 59-78. https://doi.org/10.48550/arXiv.1207.5434

[15] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, “Cyber Security for Fog based Smart Grid SCADA Systems: Solutions and Challenges,” Journal of Information Security and Applications, vol. 52, 2020, pp. 1-14. https://doi.org/10.1016/j.jisa.2020.102500

[16] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and Privacy in Smart Cities: Challenges and Opportunities,” IEEE Access, vol. 6, 2018, pp. 46134 – 46145, doi: 10.1109/ACCESS.2018.2853985