THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENSURING THE CYBER SECURITY OF SCADA SYSTEMS

Rashid Alakbarov and Mammad Hashimov

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

ABSTRACT

One of the vital systems for the management of industrial infrastructure is SCADA (Supervisory Control and Data Acquisition). They are extensively applied in different industrial processes, particularly or energy, water, and transportation networks. These systems are principally efficient and unfailing when united with Artificial Intelligence (AI) technologies. The application of AI technologies in traditional SCADA systems creates many new opportunities. These technologies provide more accurate monitoring of processes, more effective control, increased security, and optimization of operations. But, due to their integration with modern Information Technologies and the Internet, these systems are more and more unprotected from cyber threats. Outdated security procedures are often unsatisfactory against these attacks. AI has emerged as a promising solution to enhance SCADA cybersecurity through anomaly detection, automated threat response, and predictive risk assessment. This article explores the applications of AI-driven cybersecurity in SCADA systems, highlighting the benefits and future research directions. Integrating artificial intelligence into SCADA security is crucial to ensuring resilience, reliability, and protection against both known and emerging cyber threats.

KEYWORDS

Artificial intelligence, Cyber security, SCADA systems.

1. INTRODUCTION

The oil and gas industry are one of the main sectors that meet global energy needs and plays an important role in economic development. This industry is the main source of raw materials for transport, electricity generation and the chemical industry. It covers the exploration, production, processing and transportation of oil and gas. Due to technological innovations, production and processing processes became more efficient and safer. One of the crucial and significant problem in the advanced management system of the oil and gas industry includes the use of information technology. Obviously, the development rate of scientific and technical progress has created favorable conditions for the use of new management and control models that meet more advanced and modern standards in the oil and gas industry.

SCADA systems are applied in the oil and gas industry to monitor and control operations remotely, optimize production and ensure safety. SCADA systems are distributed control systems applied for managing comprehensive operations in oil and gas industries. They syndicate hardware and software mechanisms for the ease of links between field devices and central control systems [1]. These innovative platforms empower real-time monitoring, control, and optimization, as the main pillar of contemporary industrial procedures. SCADA systems have become essential tools to meet the growing demands of the industry to improve environmental

DOI:10.5121/ijaia.2025.16301

performance, safety, and efficiency. The global SCADA market cost for the oil and gas industry was projected to reach $4.52 billion by 2021, growing at a compound annual growth rate (CAGR) of 5.8% from 2021 to 2026 [2]. The need for real-time decision-making capabilities, the industry's change towards digital transformation, and the increasing complexity of operations are the key factors driving this growth. Emergence of of the Industrial Internet of Things is due to the industry 4.0 and the integration of Internet of Things devices into Cyber-Physical Systems. It provides real-time monitoring of machine state, affords instant response to workers, and simplifies quicker processes in manufacturing. Modernized SCADA systems have become highly advanced and complex technological systems. The adoption of open standard protocols has significantly increased their productivity and profitability. These systems are vital in the oil and gas industry as they enable real-time monitoring, control, and automation of different procedures.

In upstream, midstream, and downstream operations SCADA systems are applied as follows [3]:

- Upstream: SCADA systems assist exploration and production activities by monitoring drilling operations, well performance, and reservoir management. They offer real-time data on pressure, temperature, and flow rates by optimizing production procedures.
- Midstream: SCADA systems improve pipeline monitoring, leak detection, and transportation efficiency. They help automate compressor stations, regulate flow rates, and ensure the integrity of storage facilities.
- Downstream: In processing and distribution, SCADA systems facilitate process automation, quality control, and inventory management. They optimize processing, enhance safety measures, and simplify logistics in fuel distribution networks. SCADA systems offer numerous advantages in oil and gas operations, some of which are listed below [4]:
- Real-time monitoring: qualifies worker to track limitations such as pressure, flow rate, and temperature.
- Operational Efficiency: automates processes to optimize resource utilization and reduce human intervention.
- Security and Reliability: enhances leak detection, emergency shutdowns, and predictive maintenance.
- Cost Reduction: minimizes manual inspections, improves asset management, and reduces downtime.

Despite the above-mentioned advantages, SCADA systems face numerous cybersecurity challenges. SCADA systems increase the efficiency of industrial processes by offering remote control, real-time monitoring, and automatic control capabilities. However, these networked systems are exposed to cybersecurity threats. Unencrypted communication, authentication failures, and insider threats put the sustainability of SCADA systems at risk. Artificial intelligence technologies play an important role in addressing these challenges.

2. CONCEPTUAL MODEL OF SCADA SYSTEM

The conceptual model of SCADA systems shows how various components operate in an integrated manner and work in a coordinated manner to control industrial processes. SCADA systems consist of complex software and hardware tools that provide remote control and monitoring of industrial processes. SCADA systems provide effective control and monitoring of processes in industrial enterprises and infrastructures. These systems make possible the real-time monitoring of processes, data collection and analysis, as well as the automation. SCADA systems aim to increase performance, reduce costs, and ensure operational safety in industrial enterprises. This model mainly consists of four main parts: field devices, communication infrastructure, control center, and human-machine interface (HMI). Figure 1 presents the conceptual model of

SCADA systems [5-7]:

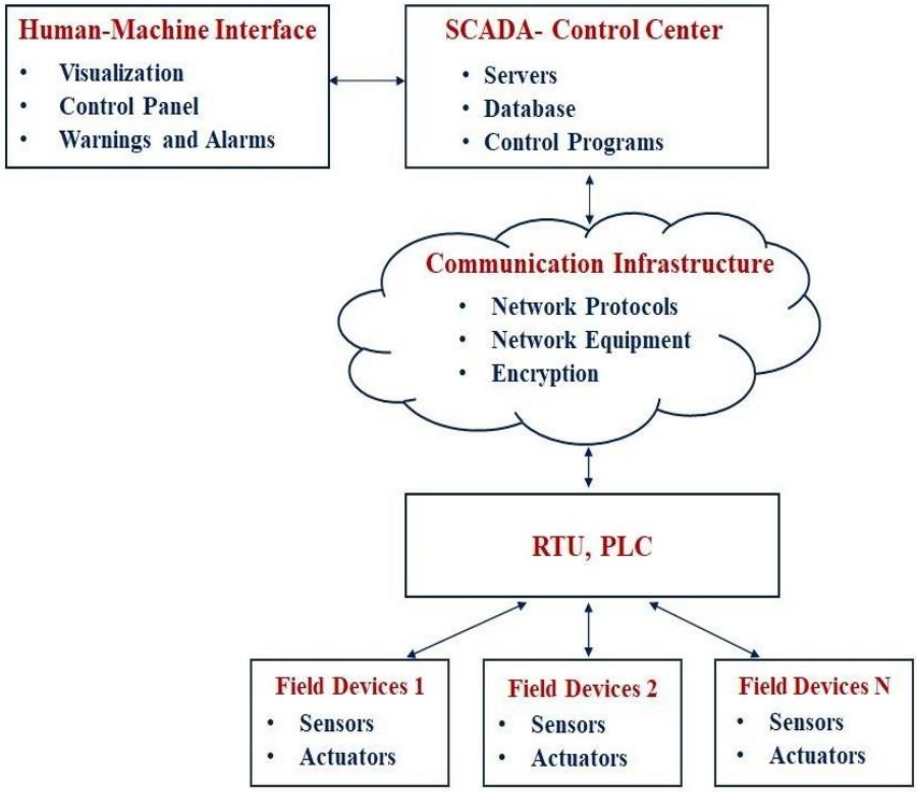

Figure 1. Conceptual model of a SCADA system

Field Devices - Located at the lowest level of SCADA systems and are used for direct monitoring and control of processes. These devices include various sensors, actuators, RTU (Remote Terminal Unit) and PLC (Programmable Logic Controller) elements such as:

- Sensors: They are applied to sense temperature, pressure, level, flow and other parameters.
- Actuators: Act as valves, motors and other mechanical devices that directly affect processes.
- RTU and PLC: They gather data from equipments in the field and perform management instructions. PLCs are programmable devices for process automation, while RTUs communicate with devices located at remote locations.

Communication infrastructure - a network system that provides data sharing between field devices and the control center. This system uses various protocols and network technologies.

- Network Protocols: Modbus, DNP3, IEC 60870-5-104 and other industrial protocols are used for data transmission.
- Network Equipment: Here, secure and right data transmission is implemented through routers, switches, firewalls and other network devices.
- Encryption: Encryption technologies are used to ensure confidentiality and integrity during data transmission.

Control Center - The central control part of SCADA systems collects and analyzes data and controls commands.

- Servers: High-performance computers used for data collection, storage and processing.
- Database: Database systems used for long-term storage and analysis of data.
- Control Programs: Special software for controlling and monitoring processes.

Human-Machine Interface (HMI) - visual interfaces to enable operators to communicate with SCADA systems.

- Visualization: Graphical representations of processes and visual representation of their status.
- Control Panel: A panel used by operators to intervene in processes and issue control commands. • Warnings and Alarms: Warning and alarm systems used to inform operators in emergency situations.

3. RELATED WORKS

Article [8] explores the integration of Artificial Intelligence (AI) with SCADA systems to improve operational efficiency. Large amounts of data can be processed in real time with SCADA systems, device failures can be forecasted, energy consumption optimized, and ecological effects minimized. The study highlights the transformative potential of AI in industrial automation, presenting both the opportunities and challenges associated with AI. In [9], the integration of machine learning models within modern SCADA systems is explored, and the chief competences of machine learning models, as well as upgraded anomaly detection, predictive maintenance, and optimized system performance are highlighted. [10] proposes a new approach for identifying alarms using Fuzzy Logic based on data collected by SCADA. The alarms generated in this situation can be grouped in two categories: orange alarms, which correspond to faults that require preventive maintenance intervention, and red alarms, which correspond to critical conditions that may lead to system failure. It is aimed to handle the indicators sensed by the SCADA system from a different perspective. [11] offers various solutions to recover the lost data of important SCADA parameters using linear and nonlinear AI algorithms. [12] examines how to use the data presented by a pipeline-based SCADA system to attempt self-error identification, self-correction, and self healing functions using machine learning (ML) models. [13] provides a comprehensive review of machine learning and deep learning applications in SCADA system security. The research focuses on the past five years, showing the latest applications of Deep Learning methods in Intrusion detection system (IDS). The article analyses the newest studies on building robust IDSs through Deep Learning (DL) algorithms, as well as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Stacked Autoencoders (SAE), and Deep Belief Networks. Each algorithm is concluded to have own advantages and shortcomings. In [14], the authors use machine learning algorithms such as Decision Trees, K-means, etc. to detect anomalies in a SCADA dataset from a Mississippi gas pipeline. The dataset was tested with several machine learning algorithms and it was found that Decision Trees and K-nearest Neighbors algorithms outperformed K-means clustering when analyzing different types of attacks. [15] evaluates the effectiveness of Machine Learning (ML) for detecting unauthorized access in SCADA systems. A dataset from a gas pipeline is used and two classification algorithms, namely Random Forest and Support Vector Machine, are applied. [16] reviews various existing system solutions to secure SCADA systems, and recommends a new security approach using AI. An intrusion detection system (IDS) is built to struggle with cyberattacks through deep learning algorithms and machine learning algorithms. Different methods and algorithms are evaluated to achieve the best results in attack detection. The results show that the Bi-LSTM IDS technique provides the highest intrusion detection (ID) performance compared to previous methods to secure SCADA systems. In [17], an intrusion detection algorithm is proposed. The proposed Genetic Seeded Flora Transformer Neural Network (GSFTNN) algorithm completely differs from the signature-based method used by traditional

intrusion detection systems. In terms of accuracy and efficiency, the algorithm offered performs better that the traditional ones, such as Residual Neural Networks (ResNet), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM). [18] explores the effectiveness of six machine learning (ML) methods for detecting DDoS attacks. [19] uses two laboratory-scale SCADA systems (water storage tank and gas pipeline systems) to collect data and real-world data sets, including various cyberattacks. Some ML and deep learning techniques, including support vector machine (SVM), XGB, and RF, are studied to detect attacks on these systems.

4. THE MAIN ADVANTAGES OF APPLYING AI TECHNOLOGY TO SCADA SYSTEMS

Application of AI technology in traditional SCADA system provides many new opportunities. This technology ensures more accurate monitoring of processes, more effective management, increased safety and optimization of operations. The integration of AI in SCADA systems enables the creation of more intelligent and flexible control systems that meet modern requirements in the industrial environment. Application of AI technology to SCADA systems has great advantages in terms of automation and optimization of industrial processes. These advantages help SCADA systems to be managed more efficiently, safely and effectively. Management of SCADA systems through traditional methods is accompanied by some limitations. Application of modern technologies, particularly AI technology, plays an important role in overcoming these limitations and increasing the functionality of SCADA systems. AI technology enables more efficient and automated management of SCADA systems through machine learning, big data analysis, predictive models and other advanced methods. Through these technologies, systems become smarter, more flexible, and more efficient, optimizing operations and improving security.

SCADA systems produce significantly more data. For example, a decade ago, an offshore oil platform could generate only 10–15 gigabytes of data per day; today, this figure varies between 1–2 terabytes [20]. The abundance of data has driven the development of sophisticated analytics capabilities, with artificial intelligence and machine learning becoming increasingly important in extracting useful information. The main advantages of applying AI technology to SCADA systems in various fields are shown below [21-23]:

- **Early detection of failures**: AI algorithms predict upcoming equipment failures, which ensures timely implementation of preventive maintenance measures. AI algorithms can analyze historical and real-time data to detect anomalies, trends and patterns that may indicate potential equipment failures.
- **Optimization of resource use**: AI technology predicts resource use more accurately, which warrants more efficient use of energy and other resources. It reduces resource shortages and waste by predicting future demands.
- **Decision making**: AI technology support professionals to make more accurate decisions by analyzing data with deep analytics and models.
- **Maintenance planning**: AI algorithms forcast the possibility of device fails providing appropriate operation of maintenance and restoration work.
- **Energy management**: AI enhances setpoints and tracks parameters in real-time, due to which the system functions at extreme effectiveness, minimizing waste and energy usage.
- **Automated control**: AI technology provides automation of processes, reducing human intervention and ensuring more accurate and faster implementation of operations.
- **Deep data analysis**: AI technology enables better understanding of system performance by analyzing large data sets through deep analytics.

Despite the above-mentioned advantages, there are some difficulties associated with the

application of AI technologies in SCADA systems. Some of them are shown below [21-23]:

- Training AI models in SCADA environments is difficult because high-quality, labeled data covering confidential and rare events is scarce and limitedly available.
- Training and deploying complex AI models in SCADA systems is difficult because the limited computing power and resources of these systems cannot meet the high computational demands.
- For operators in critical infrastructures to trust AI-based security alerts, it is essential that the models' decisions are transparent and explainable.
- Because AI systems have vulnerabilities that can be manipulated by adversaries, they themselves can be targets of cyberattacks.
- Integrating modern AI solutions with legacy SCADA systems and protocols is difficult because these systems have non-standard, resource-constrained, and non-upgradable architectures.
- AI systems can generate false positive or negative signals, and since this affects the reliability of the system, additional filtering, human supervision, and adaptive learning mechanisms are required to manage such cases.

5. ADVANTAGES OF USING AI TO ENSURE SECURITY IN SCADA SYSTEMS

As SCADA systems are unified and associated to larger networks, they become more exposed to cyberattacks. Such attacks can cause serious consequences for the oil and gas sector, ranging from production disruptions to environmental disasters. According to recent research, the number of cyberattacks targeting SCADA and other industrial control systems has increased by 110% annually over the past three years. According to the study, 73% of these attacks targeted the energy industry, with oil and gas corporations being the hardest hit. Enterprises are investing heavily in cybersecurity solutions to counter these attacks. According to the survey, cybersecurity spendings on SCADA systems by large oil and gas corporations have increased by 18% annually since 2018 [3]. The dynamic nature of cyberthreats remains challenging despite these growing costs. Some of the security risks in SCADA systems are listed below [24, 25]:

- **Unauthorized Access**: Weak authentication mechanisms are captured by cybercriminals to take control on the main infrastructure.
- **Cyberattacks:** Cybercriminals target SCADA networks with malware to disrupt operations. Malicious actors mainly focus on the systems to corrupt, employ, or disorder data to cause operational failures. Momentous risks are mainly posed by man-in-the-middle (MITM), ransom ware, and malware.
- **Insider threats:** Employees with privileged access to SCADA systems can intentionally or unintentionally interfere with critical data, which can result in data corruption or loss.
- **System vulnerabilities**: Older SCADA system soften have outdated software, insecure communication protocols, or vulnerabilities that increase the risk of data breaches. Interception and manipulation of sensitive data can be implemented with the use of uncertain communication protocols.
- **Data integrity:** Refers to the accuracy, consistency, and reliability of data throughout its lifecycle. In SCADA systems, providing data integrity is of great importance in terms of operational efficiency and security. Dangerous data can result in false readings, which can lead to poor operational decisions. For instance, manipulated sensor data may lead to failure of detect a pipeline leak detection or a valve misadjusting, possibly causing an environmental or safety incident.
- **Third-party risks:** To ensure system maintenance oil and gas corporations usually count on external suppliers or contractors, wich rises the risk of third-party data breaches.

AI application is vital for providing the security of SCADA systems. AI technologies improve

various aspects of cybersecurity, making systems more reliable and secure. The application of AI technologies creates a number of new opportunities in traditional SCADA systems and increases their functionality. The main advantages of using AI in ensuring security are explained below [26-29]:

- Anomaly detection: AI technology enables early detection of uncommon activities and security incidents in SCADA systems, allowing for timely action. Machine learning approaches are essential for recognizing anomalies to identify insider threats in SCADA systems. Models can detect deviations from the norm that may be indicative of malicious activity by learning from typical system behavior. Unsupervised learning techniques, such as Autoencoders, Gaussian mixture models, or single-class SVMs, can be used to detect anomalies and flag suspicious behavior.

An example of anomaly detection based on AI technologies is the research work [30]. Various ML algorithms were used to detect anomalies based on a dataset of a Gas Pipeline SCADA system created by the SCADA laboratory at Mississippi State University. This work was divided into two classifications: binary classification and categorical classification. Two attack types (Command Injection and Response Injection) were investigated within the framework of binary classification. Eight different ML algorithms were applied and the results obtained were compared. Light GBM and Decision Tree classifiers achieved higher performance compared to other applied models. Seven (7) attack types in the dataset were analyzed using six different ML classifiers within the framework of categorical classification task. Light Gradient Boosting Machine (LGBM) showed superior results compared to all other classifiers in detecting attack types.

Real-time analysis: AI technologies can analyze events occurring in SCADA systems in real time. This allows for immediate detection of unusual activities and potential attacks. AI technologies analyze data in real time and detect anomalies through machine learning algorithms. It provides early detection of failures and abnormal behavior. This detects and prevents attacks at an early stage.

Deep data analysis: AI algorithms identify anomalies by analyzing large volumes of data. This detects and prevents attacks at an early stage. For example, Natural Language Processing [NLP] can offer important insights to detect insider threats in SCADA systems. They use NLP techniques handle and analyze this textual data, extract applicable information, and sense possible attack indicators.

Predictive analytics: AI technologies can predict future security threats based on previous data. This allows preventive measures to be taken to avoid potential threats. By analyzing network traffic patterns, AI can predict DDoS attacks and take preventive measures to protect SCADA systems.

Cyber-attack detection: AI technologies can detect malicious activities and cyber-attacks. AI algorithms learn various behavioral patterns and threats to recognize and prevent attacks. Traditional security solutions often fail to address these insider risks. Machine Learning [ML] based Insider Intrusion Detection Systems [IDS] have appeared as a possible method to advance the discovery and prevention of insider attacks in SCADA systems.

Malware recognition: AI technologies analyze malicious programs and their behavior, identify potential threats, and prevent malicious activities. For example, deep learning models such as Bidirectional Long Short-Term Memory (Bi-LSTM) and methods such as Random Forest have demonstrated high effectiveness in detecting intrusions in SCADA environments.

Automated security audits: Security audits and monitoring can be automated through AI technologies. This minimizes human intervention and allows for more efficient and faster implementation of security measures.

Decision automation: AI algorithms can automatically make decisions about security threats. This ensures immediate responses to attacks and threats.

Data interpretation: AI technologies analyze large volumes of data fast and accurately, interpreting security information more effectively. This helps cybersecurity teams make more informed decisions.

Risk analysis and assessment: AI technologies improve the risk assessment process. Algorithms can assess potential threats and their impacts more accurately. AI technologies develop and implement effective strategies to minimize risks. This helps to implement security measures in a more systematic and expedient manner.

Automated Incident Management: AI technologies provide automatic incident management. This allows security incidents to be resolved faster and more efficiently.

Suspicious Activity Detection: AI methods are used to detect cyber-attacks and suspicious activities in real time and automate response measures. Machine learning algorithms can recognize small anomalies and identify abnormal actions that deviate from established standards by learning patterns and behaviors from data.

6. CONCLUSION

SCADA systems are an integral part of modern industry and infrastructure. These systems play an important role in increasing operational efficiency, automating processes, managing resources, and ensuring safety and savings. Over time, these systems have evolved from being just monitoring tools to being equipped with more intelligent and flexible management capabilities. The integration of AI technologies into SCADA systems has significant potential in terms of optimizing industrial processes and increasing the level of security. Machine learning, deep learning, neural networks and other AI algorithms create wide opportunities for analyzing big data, detecting anomalies and taking preventive measures. These technologies also provide automated solutions for faster and more accurate detection and response to security incidents.

However, there are also a number of challenges in this area. In particular, the lack of high-quality and labeled data, the need to adapt legacy SCADA architectures to modern AI models, resource constraints, the need for decision explainability and the management of false positives/negatives are among the main challenges. In addition, the fact that AI systems themselves are potential targets for cyberattacks creates additional security risks.

The purpose of this review article is to analyze the application of AI technologies in the cybersecurity of SCADA systems, to examine the existing problems in this area and their possible solutions, as well as to identify the main directions for future research. Within the framework of the study, it was investigated how machine learning, deep learning and other AI methods can be applied to increase the level of cybersecurity in SCADA systems. Using AI methods such as machine learning, deep learning and neural networks, the development of new methods and algorithms for anomaly detection in SCADA systems, prediction of cybersecurity threats and timely detection of attacks such as malware is a future research direction. Research in these areas will not only strengthen the role of AI in the cybersecurity of SCADA systems, but will also contribute to safer and smarter management of industrial processes.

ACKNOWLEDGEMENTS

This work is supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 01LR-EF/2024).

REFERENCES

[1] G. Yadav, K. Paul, (2021) "Architecture and security of SCADA systems: A review", International Journal of Critical Infrastructure Protection, Vol. 34, 100433.
[2] Marketsand Markets, "SCADA Market in Oil & Gas - Global Forecast to 2026," 2021.
[3] V. H. Khisty, (2024) "SCADA Systems in Oil and Gas: Driving Innovation and Efficiency in the Digital Age", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 12, issue 8, pp. 96-107.
[4] How SCADA Systems Revolutionize the Gas & Oil Industry. https://www.htt.io/learning-center/how scada-systems-revolutionize-the-gas-oil-industry
[5] R. G. Alakbarov, M. A. Hashimov. (2020) "Migration Issues of SCADA Systems to the Cloud Computing Environment (review). SOCAR Proceedings No.3, 155-164.
[6] A. Shahzad, S. Musa, A. Aborujilah, M. Irfan. (2014) "The SCADA Review: System Components, Architecture, Protocols and Future Security Trends", American Journal of Applied Sciences, Vol. 11, issue. 8, 1418-1425.
[7] J. Carson. What Are the Main Components of a https://pacificblueengineering.com/what-are-main-components-scada-systems/ SCADA System?
[8] M. Taha. (2024) "Integrating Artificial Intelligence with SCADA Systems: Enhancing Operational Efficiency, Predictive Maintenance, and Environmental Sustainability". P.23.
[9] I. Šenk, S. Tegeltija, L. Tarjan. (2024) "Machine Learning in Modern SCADA Systems: Opportunities and Challenges", 23rd International Symposium INFOTEH-JAHORINA (INFOTEH).
[10] T. Benmessaoud, A. P. Marugán, K. Mohammedi, F. P. G. Márquez, (2017) "Fuzzy Logic Applied to SCADA Systems". In International Conference on Management Science and Engineering Management (pp. 749-757). Springer, Cham.
[11] N. M. Khan, G. M. Khan, P. Matthews. (2020) "AI Based Real-Time Signal Reconstruction for Wind Farm with SCADA Sensor Failure. International Federation for Information Processing, Published by Springer Nature Switzerland AG 2020 I. Maglogiannis et al. (Eds.): AIAI 2020, IFIP AICT 584, pp. 207–218.
[12] B. C. Mugo. (2024) "Optimization of Industrial Conveyor based SCADA System using Machine Learning Techniques", International Journal of Computer Applications, Vol. 186, No. 29.
[13] A. Balla, M. H. Habaebi, MD. R. Islam, S. Mubarak. (2022) "Applications of deep learning algorithms for Supervisory Control and Data Acquisition intrusion detection system". Cleaner Engineering and Technology Vol. 9, 100532.
[14] B. Phillips, E. Gamess, and S. Krishnaprasad, (2020) "An evaluation of machine learning-based anomaly detection in a SCADA system using the modbus protocol," Proceedings of the 2020 ACM Southeast Conference, pp. 188–196.
[15] R. L. Perez, F, Adamsky, R, Soua, T, Engel. (2018) "Machine Learning for Reliable Network Attack Detection in SCADA Systems. 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).
[16] L. A. Aldossary, M. Ali, A, Alasaadi. (2021) "Securing SCADA Systems against Cyber-Attacks using Artificial Intelligence". International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)
[17] S. Y. Diaba, T. Anafo, L. A. Tetteh, M. A. Oyibo, A. A. Alola, M. Shafie-khah, M. Elmusrati. (2023) "SCADA securing system using deep learning to prevent cyber infiltration". Neural Networks. Vol. 165, pp. 321-332.
[18] G. Qaiser, S. Chandrasekaran, R. Chai, J. Zheng, (2023) "Classifying DDoS attack in industrial Internet of services using machine learning," in Proc. 15th Int. Conf. Comput. Autom. Eng, pp. 546–550.
[19] A. Tesfahun, D. L. Bhaskari, (2016) "A SCADA testbed for investigating cyber security

vulnerabilities in critical infrastructures," Autom. Control Comput. Sci., Vol. 50, pp. 54–62.
[20] T. Halima et al. (2020) "Big Data Analytics for Oil and Gas Industry: Challenges and Opportunities," IEEE Access, Vol. 8, pp. 61183-61201.
[21] R. Canvas. (2023) "How AI/ML Complements SCADA Systems in Manufacturing.Available at: https://www.rapidcanvas.ai
[22] A. Ucar, M. Karakose, N. Kırımça. (2024) "Artificial Intelligence for Predictive Maintenance Applications: Key Components, Trustworthiness, and Future Trends", Appl. Sci. Vol. 14, 898.
[23] The Fusion of Artificial Intelligence and SCADA Industry 4.0: A Transformative Synergy. https://atvise.vesterbusiness.com/en/news/scada-with-applied-artificial-intelligence-industry/
[24] M. Alanazi, A. Mahmooda, M. J. M. Chowdhury. (2023) "SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues, Computers & Security, Vol. 125, 103028.
[25] S. Ghosh, S. Sampalli. (2019) "A Survey of Security in SCADA Networks: Current Issues and Future Challenges, IEEE Access, p. 99.
[26] N. Capuano, G. Fenza, V. Loia, C. Stanzione, (2022) "Explainable Artificial Intelligence in CyberSecurity: A Survey" IEEE Access, Vol. 10, pp. 93575 – 93600.
[27] M. Aliyari. (2021) "Securing Industrial Infrastructure against Cyber-Attacks Using Machine Learning and Artificial Intelligence at the Age of Industry 4.0.". Turkish Journal of Computer and Mathematics Education Vol.12 No.11. 6581-6594.
[28] A. J. Gonçalves de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, (2023) "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey", Electronics, Vol. 12, Issue 8, pp. 1-18.
[29] B. Al-Muntaser, M. A. Mohamed, A. Y. Tuama, I. A. Rana. (2023) "Cybersecurity Advances in SCADA Systems. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 8, pp. 318-328.
[30] E. K. Fiah. (2023) "Anomaly detection in SCADA systems using machine learning" Theses and Dissertations. 5824.

AUTHORS

Rashid Alakbarov graduated from Automation and Computer Engineering faculty of Azerbaijan Polytechnic University named after C. Ildirim. He received his PhD degree in 2006 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. His primary research interests incloude various areas in cloud computing, data processing, computer networks, virtual computing, particularly in the area of distributed computing. He is head of department at the Institute of Information Technology as of 2002. Since 2010, he has been leading the development of "AzScienceNet" infrastructure. In 2021, he was appointed a executive director of the institute by the decision of the Presidium of Azerbaijan National Academy of Sciences. He is the author of 98 scientific papers, inclouding 5 inventions.

Mammad A. Hashimov received his Master's degree in automation and control from Azerbaijan Technical University in Baku, Azerbaijan. He received his PhD degree in 2016 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. He is scientific researcher of Institute of Information Technology of Azerbaijan National Academy of Sciences. His primary research interests include various areas in internet of things, cloud computing, data processing, computer networks, virtual computing, particularly in the area of cloud technology applications. He is the author of 32 journal scientific papers and 23 proceedings.