У контексті агропромислового виробництва використання таких технологій відкриває можливості для створення цифрових двійників цілих технологічних ліній (наприклад, елеваторних комплексів чи ліній переробки сировини). Q. Qi та співавтори доводять, що інтеграція технології Digital Twins з системами аналізу Великих даних здатна підвищити загальну ефективність обладнання (OEE) на 15–20 % за рахунок оптимізації режимів роботи [4].

Отже, впровадження цифрових двійників в автоматизовані інформаційні системи моніторингу формує принципово новий рівень управління кіберфізичними системами [1]. Це дозволяє здійснити перехід до обслуговування обладнання за фактичним станом, що мінімізує фінансові втрати від непередбачених простоїв та підвищує експлуатаційну безпеку підприємства [2].

Список використаних джерел

1. Grieves M., Vickers J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. Transdisciplinary perspectives on complex systems. Springer, Cham, 2017. P. 85–113.

2. Tao F., Zhang H., Liu A., Nee A. Y. C. Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics. 2019. Vol. 15, № 4. P. 2405–2415.

3. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital Twin in manufacturing: A categorical literature review and classification. IFAC-PapersOnLine. 2018. Vol. 51, № 11. P. 1016–1022.

4. Qi Q., Tao F., Hu T., Anwer N., Liu A., Wei Y., Wang L., Nee A. Y. C. Enabling technologies and tools for digital twin. Journal of Manufacturing Systems. 2021. Vol. 58. P. 3–21.

УДК 004.056:004.7

DEVELOPMENT OF ADAPTIVE ACCESS CONTROL POLICIES FOR MULTI-CLOUD ENVIRONMENTS IN DISTRIBUTED INFORMATION SYSTEMS

Dmytro Hleba

Institute of Special Communications and Information Protection,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

Abstract. This paper investigates the challenges and prospects of developing adaptive access control policies for distributed information systems operating in multi-cloud environments. It analyzes key information security threats associated with cloud migration, as well as the limitations of traditional static access control models. The advantages of transitioning to dynamic attribute-based models (ABAC) and Zero Trust architecture are identified. Particular attention is paid to mechanisms for continuous monitoring of user context, automated policy updating, and enhancing the overall resilience of the infrastructure against modern cyberattacks.

Keywords: multi-cloud environments, cybersecurity, access control, adaptive policies, distributed information systems, Zero Trust, ABAC, identity management.

Research Relevance: The current stage of corporate information technology development is characterized by a massive transition to multi-cloud architectures. Organizations simultaneously use resources from various providers (e.g., AWS, Azure, Google Cloud) to optimize costs and ensure the uninterrupted operation of distributed systems. However, such infrastructure fragmentation leads to an expanded attack surface, loss of centralized control, and difficulties in managing access rights. Traditional static Role-Based Access Control (RBAC) models are no longer capable of effectively protecting data in conditions of highly dynamic connections, Bring Your Own Device (BYOD) practices, and remote work. The relevance of this research stems from the urgent need to develop and implement adaptive access control mechanisms capable of responding in real time to context changes and risk levels within multi-cloud ecosystems.

Research Objective: The aim of this study is to analyze the principles of building adaptive access control policies in multi-cloud environments, develop approaches for integrating dynamic risk assessment

into the authorization decision-making process, and identify architectural solutions to ensure continuous security of distributed information systems.

Distributed information systems in multi-cloud environments consist of microservices, databases, APIs, and user interfaces hosted on various providers' platforms. The main security problem in such environments is the lack of a single perimeter. Each cloud provider has its own Identity and Access Management (IAM) tools, which often leads to policy inconsistencies, over-provisioning of privileges, and the emergence of "blind spots" in security auditing. Furthermore, the dynamic nature of containerized applications and serverless computing introduces ephemeral workloads that require instantaneous access provisioning and de-provisioning, further complicating traditional security management.

Adaptive Access Control is an evolutionary step in cybersecurity that abandons one-time authentication upon system entry. Instead, it is based on the principles of Zero Trust Architecture (ZTA), where trust is never granted by default but is continuously evaluated. At the core of adaptive policies lies the Attribute-Based Access Control (ABAC) model, which considers not only the user's role but also the context of the request. This contextual awareness is often operationalized through the Continuous Adaptive Risk and Trust Assessment (CARTA) framework, which ensures that security postures dynamically evolve in tandem with emerging threats.

The decision-making process regarding access authorization in adaptive systems relies on the analysis of a multidimensional set of metrics. These metrics include: user location (IP address, geolocation), time of day, endpoint security posture (presence of antivirus, OS updates), type of network connection, and user behavior history. For instance, if an employee who typically works from the Kyiv office using a corporate laptop suddenly attempts to access a confidential cloud database from an unknown mobile device abroad, the system must automatically detect this anomaly.

Instead of rigid Allow/Deny blocking, adaptive policies allow for flexible response mechanisms. Depending on the calculated transaction risk level, the system may require additional Multi-Factor Authentication (MFA), restrict access rights to a "read-only" mode, or permit access only to non-confidential data. Additionally, session termination or step-up authentication can be triggered mid-session if a sudden shift in behavior is detected, ensuring that an initially secure connection remains secure throughout its entire lifecycle. This approach minimizes the impact on legitimate users while simultaneously blocking potential threats.

Implementing adaptive policies in a multi-cloud environment requires the use of Cloud Access Security Brokers (CASB) or centralized cloud security posture management platforms (CSPM, CIEM). These tools enable abstraction from the specifics of a particular cloud provider and apply unified standardized access policies across the entire distributed infrastructure. Data from various cloud platforms, event logs, and network traffic is consolidated and normalized. Moreover, integrating API gateways and service meshes into this architecture allows for granular policy enforcement, ensuring secure machine-to-machine (M2M) communication across different cloud boundaries. This centralized visibility also simplifies compliance with stringent regulatory frameworks, such as GDPR or HIPAA, by providing a unified trail of access logs.

Machine learning and artificial intelligence algorithms play a crucial role in developing adaptive policies by enabling User and Entity Behavior Analytics (UEBA). Models detect hidden correlations and anomalies that may indicate credential compromise or insider abuse attempts, automatically adjusting the user's "trust score" in real time. By utilizing both supervised learning for known threat signatures and unsupervised learning for novel anomaly detection, these intelligent systems can proactively isolate compromised accounts before significant data exfiltration occurs.

Thus, the development and implementation of adaptive access control policies are critical for protecting modern distributed information systems. The integration of dynamic context assessment, attribute-based access models, and behavior analytics allows for the creation of a resilient architecture that effectively counters cyber threats in complex multi-cloud ecosystems.

References

1. National Institute of Standards and Technology. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207.

2. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing. URL: https://cloudsecurityalliance.org/ (accessed: 14.10.2026).

3. National Institute of Standards and Technology. Attribute Based Access Control (ABAC) Definition and Considerations. NIST SP 800-162. Gaithersburg: NIST, 2014. DOI: https://doi.org/10.6028/NIST.SP.800-162.

УДК 004.8:681.5

DATA MINING AND MACHINE LEARNING IN AUTOMATED PROCESS CONTROL SYSTEMS

Olena Polonska

Institute of Special Communications and Information Protection,
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

Language advisor: Zhytska S. A., Senior Lecturer
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute»

Modern critical infrastructure encompasses energy, water supply, chemical industry, and other strategically important sectors, the stable operation of which depends on the efficiency of automated process control systems (APCS). As the number of industrial devices, sensors, and monitoring systems grows, so does the volume of process data, creating a need for intelligent data processing methods. One promising avenue is the integration of Big Data, Data Mining, and Machine Learning technologies, which enable a shift from traditional monitoring to predicting deviations and enhancing process control efficiency[1]. This approach is underpinned by the Big Data concept, characterized by large data volumes (Volume), high rates of data ingestion and processing (Velocity), and a diversity of formats (Variety). In APCS environments, this data may include historical records of temperature, pressure, resource consumption, equipment operating modes, and industrial network events. Data reliability and the ability to derive practical value from analysis are also crucial, as errors, omissions, and information noise can compromise the accuracy of analytical models[2].

Data Mining or intelligent data analysis serves as a key tool for uncovering hidden patterns within vast datasets of processed information. Its application makes it possible to identify interrelationships between process parameters, detect anomalous equipment operating modes, pinpoint the causes of malfunctions, and identify opportunities for optimizing resource utilization[3]. The primary methods include classification, clustering, association analysis, and forecasting. Specifically, classification helps distinguish between normal and potentially critical states; clustering identifies typical equipment operating modes; and association analysis detects combinations of events linked to the occurrence of process deviations. Within APCS architecture, data mining can be used to analyze data accumulated in historical repositories (Industrial Historian) and transmit the resulting insights to analytical systems and decision-support tools. Unlike standard SCADA functions such as filtering, data aggregation, and trend visualization, intelligent analysis enables detection of complex relationships that are not always apparent during routine monitoring. This makes it an effective complement to existing automation infrastructure, without requiring the replacement of core components[4].

Machine learning is a key area of development in intelligent analysis; it enables the construction of models for forecasting and pattern recognition based on data. While data mining focuses primarily on discovering and interpreting relationships, machine learning allows training of models that apply these relationships to new data. For instance, supervised learning methods such as logistic regression and random forests can be used to classify equipment states[5], whereas unsupervised learning methods such as K-means can be employed to group operational modes and detect anomalous behavior. Combining data mining and machine learning creates opportunities to analyze both historical data and real-time information streams. Such historical data may include thermal, hydrodynamic, mechanical, and electrical parameters, as well as