connection intensity, the distribution of traffic sources, request frequency, and the nature of server responses. A combination of atypical indicators can trigger an alert; however, confirming an attack requires accounting for the possibility of a legitimate surge in load.

Another important area is the detection of port scanning. During network infrastructure reconnaissance, an attacker might sequentially access various ports on a single node or check the availability of multiple devices. A machine learning model can detect an atypical increase in the number of such requests, unusual connection sequences, and a high rate of failed connection attempts. Artificial intelligence can also be used to detect signs of data exfiltration. For example, a workstation that typically transmits small amounts of information might suddenly start sending large volumes of data to an external server at an unusual time. The system can identify such an anomaly based on data transmission volume, connection duration, and the device network activity history. However, confirming a data leak requires further verification of the connection destination, access rights, and the nature of the transmitted data. One more example is the detection of infected devices establishing regular connections with external command-and-control nodes. Even if individual connections show no obvious signs of danger, their frequency, unusual duration, or combination with other suspicious events may indicate the presence of malware.

Protecting Internet of Things (IoT) devices is a critical area of focus. Such devices often have limited computing resources, utilize standard network protocol sets, and do not always support robust security measures. Consequently, they can become targets for attacks or be used to form botnets. Network behavior analysis makes it possible to identify devices that suddenly alter their communications patterns, connect to unknown servers, or generate atypical traffic volumes. In cloud-based and distributed information systems, intelligent analysis can be performed simultaneously across multiple layers: network, server, and application. Aggregating information from various sources enables a better understanding of the interrelationships between events and the detection of attacks that might otherwise go unnoticed if analyzed at individual nodes in isolation.

References

1. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: NIST, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.

2. National Institute of Standards and Technology. Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. Gaithersburg: NIST, 2022. DOI: https://doi.org/10.6028/NIST.SP.1270.

3. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

4. MITRE. MITRE ATT&CK: Enterprise Matrix. URL: https://attack.mitre.org/ (дата звернення: 13.10.2026).

5. Scikit-learn developers. Novelty and Outlier Detection. Scikit-learn User Guide. URL: https://scikit-learn.org/stable/modules/outlier_detection.html (дата звернення: 13.10.2026).

6. National Institute of Standards and Technology. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2023. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.AI.100-2e2023.

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.

4. Development and standardization of information security policies in cloud environments: current state and prospects.

УДК 004.056:681.518

КІБЕРЗАХИСТ СИСТЕМ SCADA: АКТУАЛЬНІ ЗАГРОЗИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Євген Губницький

Миколаївський національний аграрний університет, м. Миколаїв, Україна

Науковий керівник: Л. О. Борян,
старший викладач Миколаївський національний аграрний університет

Інтенсивна цифровізація виробничих процесів, індустріальна автоматизація та впровадження концепції Індустрії 4.0 зумовили глибоку інтеграцію інформаційних технологій (IT) та операційних технологій (OT). Центральне місце в цій екосистемі займають диспетчерські системи управління та збору даних Supervisory Control and Data Acquisition (SCADA). Вони забезпечують безперервний моніторинг, збір телеметричної інформації та керування складними технологічними об'єктами в реальному часі: від енергетичних мереж і гідроелектростанцій до агропромислових комплексів, систем зрошення та переробки [1]. Однак історично архітектура SCADA-систем розроблялася з розрахунку на ізольованість і фізичну безпеку, а не на протидію цілеспрямованим кібератакам із боку злочинних угруповань чи держав-агресорів [4]. Перехід до використання стандартних мережевих протоколів (Modbus, Profibus, DNP3 поверх TCP/IP), підключення промислових мереж до глобальної мережі Інтернет та використання хмарних сховищ перетворили критично важливі об'єкти країни на вразливі мішені. Відтак, забезпечення надійного кіберзахисту SCADA є питанням безпеки й життєдіяльності держави.