Date of first submission	2026-05-16
Date of acceptance of article for publication after review	2026-06-25
Date of publication/publication	2026-07-25

SECURE DEVSECOPS FRAMEWORK FOR CLOUD INFRASTRUCTURE PROTECTION

Kateryna Oblakevych
ORCID: https://orcid.org/0009-0001-2927-1045
Master of Science in Computer Science,
Odessa National Polytechnic University, Ukraine
Software Development Engineer / Software Engineer,
Centific Global Solutions, Inc., US

Abstract. The article is devoted to the development of a secure DevSecOps framework for cloud infrastructure protection. The purpose of the study is to substantiate the author's approach to building such a framework based on the integration of artificial intelligence-based cyber threat detection technologies and data leakage prevention mechanisms. The scientific research used general scientific methods of cognition, in particular analysis, synthesis, generalization, systematization and classification, as well as the Relative Importance Index to assess the priority of the author's development components. The results of the study show that cloud infrastructure protection covers at least six levels of architecture, each of which requires a separate set of control mechanisms, and the classes and models of cloud services form a different distribution of responsibility between the provider and the consumer. Modern security technologies are systematized, covering secure service networks, data categorization in transit, continuous integration pipeline certification, and AI-based vulnerability detection tools. Based on the analysis, a proprietary secure DevSecOps framework is proposed that combines behavioral anomaly assessment, automated SIEM event correlation, built-in secure development controls, project-based data leakage prevention, and cloud infrastructure hardening. An assessment of the framework components by the relative importance index showed that automated SIEM event correlation and behavioral anomaly assessment have the highest priority, while secure development controls, data leakage prevention, and infrastructure hardening play a supporting but necessary role. The practical significance of the research lies in the possibility of using the proposed framework by organizations implementing cloud services to build a holistic system for detecting and preventing cyber threats at all stages of the software development life cycle.

Keywords: cloud infrastructure, DevSecOps, cybersecurity, artificial intelligence, data leakage prevention.

Introduction

Organizations are moving to the cloud faster than their security practices are evolving. According to industry research [1], about 80% of organizations have experienced at least one cloud security incident in the past year, and the global market for cloud infrastructure security solutions is expected to exceed $100 billion by 2030, according to analysts. At the same time, an increasing number of solution providers are relying on artificial intelligence as a tool to reduce incident response times, which is directly consistent with the direction of this study.

The scale of the potential consequences of insufficient cloud infrastructure security is confirmed by high-profile incidents in recent years. The personal data breach of 533 million Facebook users, according to Liang, X., & Xu, Y. A 2025 study found that 106 countries had settled claims with the US Federal Trade Commission for $5 billion, while the unauthorized upload of 700 million LinkedIn users' profiles affected 93% of the platform's total accounts [9].

ISSN: 2787-9364

Both cases demonstrate that scaling cloud services without commensurately strengthening access controls poses systemic risks to the reputation and financial stability of organizations. The State of IT Management study found that cloud computing is the largest IT investment for organizations, and cloud security is among the top ten management concerns, with 87% of information security professionals identifying it as a priority [9]. The situation is complicated by the fact that, according to industry analysts, by 2025, more than 95% of new digital workloads will be deployed in the cloud, while cloud resource misconfiguration remains the cause of more than 80% of significant security incidents [8]. Another example is the SUNBURST incident, which affected more than 18,000 organizations due to the compromise of a single element of the software supply chain [8]. The data presented confirms that traditional perimeter defense mechanisms do not match the dynamics of cloud environments, and disparate threat detection tools do not provide sufficient speed of response. There is a need for a holistic framework that combines DevSecOps principles, automated cyber threat detection based on artificial intelligence, and data leakage prevention technologies into a single cloud infrastructure protection system, which is what shapes the relevance of this study.

Literature Review

The issue of building a secure DevSecOps framework for protecting cloud infrastructure is not widely covered in the scientific literature. Nevertheless, some components of this issue are considered by scientists.

In particular, the classes and models of cloud infrastructure were studied by P. Mell and T. Grance [10], who in the normative document NIST SP 800-145 [10] identified five essential characteristics of cloud computing, three service models and four deployment models. These authors systematized the differences between SaaS, PaaS and IaaS in terms of the distribution of management control between the provider and the consumer. Developing this topic, T. Erl, R. Puttini and Z. Mahmood [5] investigated the economic and architectural prerequisites for the transition to cloud models, in particular, the proportionality of costs, the elasticity of resources and the risks associated with expanding the boundaries of trust between the organization and the provider.

As for the essence of cloud infrastructure protection and vulnerability classification, this issue has been studied by several authors. Among them, it is worth highlighting K. Hashizume, D. G. Rosado, E. Fernández-Medina and E. B. Fernandez [7], who systematized vulnerabilities and threats according to the SPI model (SaaS, PaaS, IaaS) based on a systematic review of scientific sources. X. Liang and Y. Xu [9] applied the Design Science Research methodology to summarize technological contributions to cloud security by architectural levels: data, identity and access management, applications and software, host and virtualization, trust and privacy, and compliance. R. Kapoor and S. Verma [8] proposed a taxonomy of cloud vulnerabilities and a four-tiered Cloud Security Posture Management (CN-SPM) model that encompasses security by design, continuous monitoring, identity management, and incident response.

Modern cloud infrastructure security technologies and DevSecOps practices have been studied primarily by specialists from the US National Institute of Standards and Technology. R. Chandramouli [2] described DevSecOps implementation mechanisms for microservice architecture applications using service networks in the NIST SP 800-204C [2]. In a subsequent paper, R. Chandramouli [3] explored strategies for integrating software supply chain security into continuous integration and deployment pipelines, including attestation of code build processes. R. Chandramouli and W. Hales [4] investigated approaches to categorization and data protection in cloud applications based on WebAssembly modules operating in a service network proxy. M. Fu, J. Pasuksmit and C. Tantithamthavorn [6] conducted a systematic review of the application of artificial intelligence to DevSecOps tasks, covering 99 scientific papers and identifying 12 critical security tasks at different stages of the development lifecycle. M. Waseem,

ISSN: 2787-9364

P. Liang and M. Shahin [11] further investigated the practices of implementing microservice architecture within DevOps, which forms the technological foundation for further integration of security tools.

The review shows that existing research is mostly focused on individual components of cloud infrastructure protection, while holistic frameworks that combine behavioral anomaly detection, event correlation automation, and data leakage prevention within a single DevSecOps cycle remain underdeveloped. The author's contribution to this study is the systematization of approaches to cloud infrastructure protection by architecture levels, the classification of modern protection technologies, and the development of a secure DevSecOps framework with an assessment of the priority of its components by the index of relative importance. To achieve the set objectives, methods of analysis, synthesis, systematization, classification, and comparison were used.

Methods and Materials

The study is based on general scientific methods of cognition. Analysis and synthesis were used to process regulatory documents of the US National Institute of Standards and Technology and scientific publications on cloud security issues. The method of systematization and classification was used to organize the levels of cloud infrastructure architecture, classes of cloud services and modern protection technologies. The comparative method was used to compare the approaches of different authors to building models of cloud environment security management.

To assess the priority of the components of the author's secure DevSecOps framework, the Relative Importance Index (RII) was used [1]. Each component of the framework was evaluated according to three criteria on a five-point scale: impact on the speed of threat detection, the level of process automation and the complexity of integration into the existing CI/CD pipeline. The index is calculated using the formula $RII = \Sigma W / (A \times N)$, where W is the sum of scores for individual criteria, A is the highest score on the scale ($A = 5$), N is the number of criteria ($N = 3$). The obtained values are interpreted at five levels: critical, high, medium-high, medium and low. The use of this methodology is an element of scientific novelty of the study, as it allows moving from a qualitative description of the framework components to their quantitative ranking.

Purpose of the Article

The goal of the study is to develop and substantiate a secure DevSecOps framework for cloud infrastructure protection based on the integration of cyber threat detection technologies using artificial intelligence and data leakage prevention mechanisms. To achieve the goal, the following tasks will be performed during the study: 1) to reveal the essence of cloud infrastructure protection and systematize approaches to it by architecture levels; 2) to characterize the classes and models of cloud infrastructure; 3) analyze and classify modern technologies for protecting cloud infrastructure; 4) develop an author's secure DevSecOps framework and assess the priority of its components according to the index of relative importance.

Results and Discussions

Cloud infrastructure protection is a set of technical, organizational and procedural measures aimed at ensuring the confidentiality, integrity and availability of resources located in a distributed computing environment. Unlike the traditional perimeter model, the cloud environment is characterized by the absence of a clear physical boundary, multi-tenancy of resources and dynamic scaling, which significantly expands the attack surface [7]. Responsibility for security in such an environment is divided between the provider and the

ISSN: 2787-9364

consumer, and it is the boundary of this division that most often becomes a source of vulnerabilities.

Systematization of approaches to protecting cloud infrastructure by architectural levels allows us to see that each level requires a separate set of control mechanisms (see Table 1). These layers cover information protection, identity management, application security, virtualization, trust between parties, and regulatory compliance.

Table 1 – Classification of approaches to cloud infrastructure security by architectural layer

Architecture level	Description of the security approach
Data protection [9]	encryption, classification, and access control to ensure the confidentiality and integrity of data at rest and in transit
Identity and access management [9]	authentication, authorization, and segregation of user and service privileges in a distributed environment
Application and software protection [7]	vulnerability management at the SaaS level, compliance with web application security guidelines, and isolation of multi-tenant environments
Host and virtualization protection [7]	hypervisor isolation, control of virtual machine images, and mitigation of risks associated with shared resources
Trust and privacy [9]	establishment of transparent relationships between consumers and providers regarding data processing and storage procedures
Regulatory compliance [9]	alignment of security practices with the standards and regulations governing cloud data processing

Note: compiled by the author based on sources [7; 9]

As can be seen from Table 1, the greatest technical complexity is represented by the levels of data and application protection, since they are the ones that directly contact the business logic of the cloud service. At the same time, the level of compliance with regulatory requirements determines the limits of permissible technical solutions for the remaining levels, and therefore actually performs a coordinating function. This distribution of approaches by architectural levels creates the basis for further analysis of classes and models of cloud infrastructure, since it is the chosen model that determines which of the above levels is controlled by the provider and which by the consumer.

The classification of cloud infrastructure is carried out according to two independent criteria: the type of service provided to the consumer and the method of resource deployment. The regulatory definition of cloud computing distinguishes three service models. The SaaS model involves the use of ready-made applications from the provider, while the consumer's responsibility is limited to the configuration of user settings. The PaaS model provides the consumer with a platform for deploying their own applications without managing the underlying infrastructure. The IaaS model, on the other hand, leaves the consumer with control over the operating systems, storage, and deployed applications, while the provider is responsible only for the physical layer [10].

A separate feature of the classification is the deployment model, which determines the range of consumers and the level of resource isolation (see Fig. 1). A private cloud serves a single organization, a community cloud serves a group of organizations with common requirements, a public cloud serves an unlimited number of users, and a hybrid cloud combines several models through standardized data portability mechanisms [10].

ISSN: 2787-9364

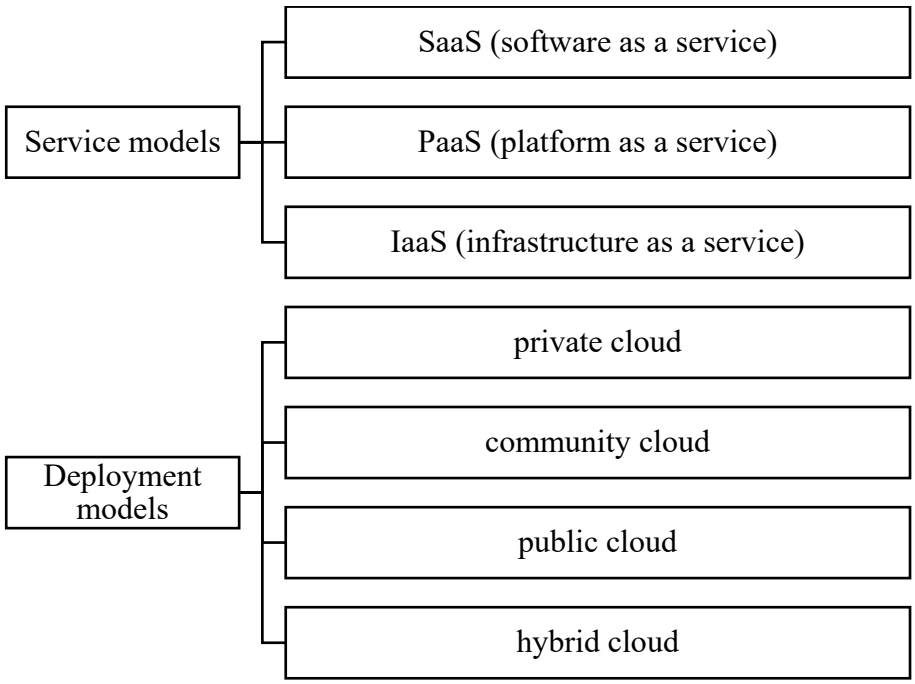

Fig. 1. Classes and models of cloud infrastructure
Note: compiled by the author based on the source [10]

The practical value of such a distribution is confirmed by economic calculations, according to which the transition from capital to operating costs and the ability to pay only for actually used resources are the main economic motive for choosing the IaaS model for organizations with variable loads [5]. At the same time, the deeper the level of abstraction of the model, the less technical control remains with the consumer and the more responsibility for security shifts to the provider [5]. This provision is directly consistent with the approaches given in Table. 1: In the SaaS model, the provider controls almost all six layers of the architecture, while in the IaaS model, the consumer must independently implement data, application, and partially virtualization protection. Understanding this dependency is a necessary prerequisite for choosing modern protection technologies, which are discussed in the next section.

The development of cloud infrastructure protection technologies in recent years has been determined by three parallel trends: the transition to service-based network architectures, automation of software supply chain security, and the introduction of artificial intelligence for threat detection and classification. Each of these trends forms a separate class of technological solutions that complement each other within a single DevSecOps cycle.

- The first class of technologies is associated with secure service networks, in which a proxy component placed next to each microservice or at the node level ensures that security checks cannot be bypassed [2].
- The second class includes data categorization modules that run in WebAssembly format directly in the proxy and are capable of detecting personal data, payment card data, and log fragments in real time that should be masked or blocked [4].
- The third class consists of continuous integration pipeline attestation tools that capture the origin of build artifacts and prevent the delivery of unauthorized code [3].
- The fourth class combines deep learning models that detect vulnerabilities at the line-of-code level and classify their type with an accuracy that exceeds the performance of traditional static analysis [6].

Table 2 – Classification of modern cloud infrastructure protection technologies

ISSN: 2787-9364

Technology category	Functional purpose
Secure service meshes [2]	standardized configuration templates and traffic segregation between microservices through sidecar or ambient proxies
Data classification in transit [4]	real-time detection and masking of sensitive data in web traffic, APIs, logs, and large language model data streams
CI/CD pipeline attestation [3]	verification of build artifact integrity, signature validation, and source code provenance control before deployment
AI-driven vulnerability detection [6]	application of deep learning models for the detection, classification, and automated remediation of code vulnerabilities

Note: compiled by the author based on sources [2; 3; 4; 6]

The discussion among researchers regarding the priority of these technological classes remains open. If R. Chandramouli [2; 3] emphasizes the primacy of control over the code delivery pipeline as the point of least resistance for an attacker, then M. Fu, J. Pasuksmit and C. Tantithamthavorn [6] argue that the main potential for increasing the effectiveness of protection lies precisely in the development stage, where AI-oriented tools can reduce the time for detecting and eliminating vulnerabilities by several times. The above comparison of approaches shows that no single technology covers the entire DevSecOps cycle on its own, and therefore it is advisable to combine them in a single framework, the author's version of which is considered in the next subsection.

Based on the architecture levels, cloud infrastructure classes, and technological solutions systematized in the previous sections, an author's secure DevSecOps framework is proposed, which combines the principles of secure software engineering, cloud-native DevSecOps practices, automation of SIEM workflows, and anomaly detection using artificial intelligence. The framework is implemented in the form of five sequential, but interconnected stages (see Fig. 2).

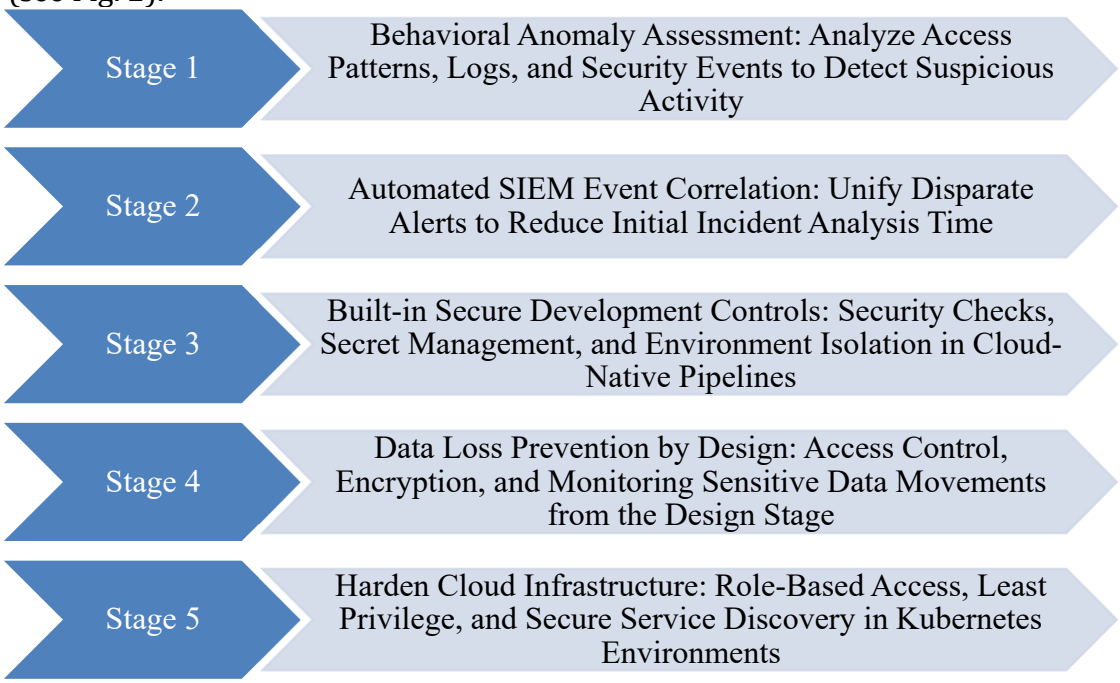

Fig. 2. Stages of the author's secure DevSecOps framework for protecting cloud infrastructure
Note: compiled by the author

ISSN: 2787-9364

The key difference between the proposed framework and the CN-SPM model [8] is that behavioral anomaly assessment and SIEM event correlation are considered not as a separate monitoring layer, but as an end-to-end mechanism integrated into each of the other four components. This makes it possible to detect deviations not only in network traffic, but also in the behavior of the CI/CD pipeline and in the dynamics of data access simultaneously.

To assess the priority of the five components of the framework, a relative importance index was used according to three criteria: impact on the speed of threat detection (C1), level of automation (C2), and complexity of integration into the existing CI/CD pipeline, where a higher score corresponds to simpler integration (C3) (see Table 3).

Table 3 – Evaluation of components of the author's DevSecOps framework by relative importance index

Framework component	C1	C2	C3	RII	Level
Behavioral anomaly assessment	5	4	3	0.80	High
Automated SIEM event correlation	5	5	3	0.87	High
Integrated secure development controls	3	4	4	0.73	Medium-high
Privacy by design	4	3	3	0.67	Medium-high
Cloud infrastructure hardening	3	3	5	0.73	Medium-high

Note: Compiled by the author. Each component is rated on three criteria on a five-point scale. The relative importance index is calculated using the formula RII = ΣW / (A × N), where A = 5, N = 3 [1]

As can be seen from Table 3, the highest priority is given to automated SIEM event correlation (RII = 0.87), since it is this component that most reduces the time from signal detection to the start of response and is the easiest to automate among all five elements. Behavioral anomaly assessment (RII = 0.80) takes second place: it significantly affects the speed of threat detection, but requires more complex integration due to the need to accumulate historical data on normal system behavior. Built-in controls for secure development and cloud infrastructure hardening received the same index (RII = 0.73), although they achieved it in different ways: the former are stronger in terms of automation, the latter in terms of ease of integration thanks to ready-made role-based access mechanisms. Data leakage prevention by project received the lowest index among the considered components (RII = 0.67), which is explained by the high complexity of configuring data classification rules for a specific business context. The obtained values confirm that the core of the proposed framework is the pair "detection – correlation", while the remaining components perform a supporting, but necessary function, without which the detected anomalies are not transformed into specific protective actions.

Conclusions

The conducted research has shown that effective protection of cloud infrastructure cannot be ensured at the level of a separate technology, since the division of responsibility between the provider and the consumer, established by the chosen service model, directly determines which of the six levels of the security architecture require independent implementation of controls by the organization. That is why the proposed author's framework is not limited to any single technological class, but combines service networks, data

ISSN: 2787-9364

categorization, certification of code delivery pipelines and AI-oriented vulnerability detection into a single sequence of five stages.

The quantitative assessment of these stages confirmed what was already observed at the qualitative level when comparing the approaches of different researchers: event detection and correlation mechanisms constitute the semantic core of the protection system, while development controls, data leakage prevention and infrastructure hardening work as protective barriers derived from them. This aligns the position of proponents of the priority of a secure code delivery pipeline with the position of proponents of the priority of AI-oriented threat detection, showing that both approaches are not alternative, but complementary components of the same DevSecOps cycle.

The results obtained can be used by organizations implementing cloud services as a guideline for the sequence of deployment of protective mechanisms: from building basic anomaly monitoring and event correlation to further increasing development controls and preventing data leakage. Prospects for further research are associated with empirical verification of the proposed framework in real cloud environments and refinement of the weighting coefficients of the evaluation criteria for different industry contexts.

References

1. Boakye, M., Adanu, S. K., Adu-Gyamfi, C., Asare, R. K., Asantewaa-Tannor, P., Ayimah, J. C., & Agbosu, W. K. (2023). A Relative Importance Index Approach to On-Site Building Construction Workers' Perception of Occupational Hazards Assessment. Medycyna Pracy, 114(3), e2023024. DOI: https://doi.org/10.23749/mdl.v114i3.14240

2. Chandramouli, R. (2022). Implementation of DevSecOps for a Microservices-Based Application with Service Mesh. NIST Special Publication 800-204C. National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-204C. URL: https://www.nist.gov/publications/implementation-devsecops-microservices-based-application-service-mesh

3. Chandramouli, R. (2024). Strategies for the Integration of Software Supply Chain Security in DevSecOps CI/CD Pipelines. NIST Special Publication 800-204D. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-204D.ipd.pdf

4. Chandramouli, R., & Hales, W. (2024). A Data Protection Approach for Cloud-Native Applications. NIST Interagency/Internal Report 8505. National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.8505. URL: https://csrc.nist.gov/pubs/ir/8505/final

5. Erl, T., Puttini, R., & Mahmood, Z. (2013). Cloud Computing: Concepts, Technology & Architecture. Pearson Education. URL: https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/0133387526.pdf

6. Fu, M., Pasuksmit, J., & Tantithamthavorn, C. (2024). AI for DevSecOps: A Landscape and Future Opportunities. arXiv. URL: https://arxiv.org/abs/2404.04839

7. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An Analysis of Security Issues for Cloud Computing. Journal of Internet Services and Applications, 4(1), 5. URL: https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5

8. Kapoor, R., & Verma, S. (2025). An Exhaustive Analysis of Security Vulnerabilities in Modern Cloud Computing Environments: Taxonomy, Attack Surfaces, and Mitigation Frameworks. European Economic Letters. URL: https://www.eelet.org.uk/index.php/journal/article/view/3401

9. Liang, X., & Xu, Y. (2025). A Novel Framework to Identify Cybersecurity Challenges and Opportunities for Organizational Digital Transformation in the Cloud. Computers & Security, 151, 104339. DOI: 10.1016/j.cose.2025.104339. URL: https://doi.org/10.1016/j.cose.2025.104339

ISSN: 2787-9364

10. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

11. Waseem, M., Liang, P., & Shahin, M. (2020). A Systematic Mapping Study on Microservices Architecture in DevOps. arXiv. URL: https://arxiv.org/abs/2008.07729

ISSN: 2787-9364