IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices

Dhruv Patel
Independent Researcher
dp270894@gmail.com

Abstract: *The Security issues become more complicated as a result of organizations using cloud-native architectures since cyberattacks are becoming more frequent and sophisticated. This research investigates Zero Trust Security integration together with DevSecOps application to reach higher security levels for cloud-native environments. The proposed study uses an improved security architecture that applies the core security principles of Zero Trust least privilege access and ongoing authentication, and dynamic policy enforcement across the DevSecOps pipeline to current agile development lifecycles. The analysis identifies security challenges of cloud-native environments that stem from microservices and containers, as well as orchestration systems using Kubernetes, while providing recommended solutions for all development periods. Continuous monitoring combined with automated vulnerability assessments and adaptive security measures forms the basis for this paper, which insists on implementing security measures right from application inception. This research presents complete guidelines for organizations that implement Zero Trust together with DevSecOps to guarantee that security becomes a core component of their cloud-native infrastructure.*

Keywords: Zero Trust Security (ZTS), DevSecOps, Cloud-Native Environments, Cybersecurity Framework, Shift-Left Security, Microservices Security

I. INTRODUCTION

Zero Trust functions as digital defense system, ensuring constant user and system protection and authentication. Through ongoing verification processes that align with the organizational principles of DevSecOps, this security measure functions beforehand. It should work on the tenet that until appropriate validation is finished, nothing should be confirmed. By putting Zero Trust Security into practice, a company may improve security [1]. Initiatives for digital modernization and transformation result in organizational adjustments to infrastructure and operations as well as cultural changes. Every initiative's execution requires a strategic framework that outlines the vision, goals, and objectives in addition to the elements and priorities. Three main concerns are shared by modern strategies: cybersecurity, cloud computing, and artificial intelligence (AI).

Additionally, they both strive for innovation, efficiency, agility, and evolution. To accomplish these strategic objectives and priorities, the defense and industry are utilizing two security models: DevSecOps and Zero Trust. Enterprises should be aware of both models, how they complement one another to enhance cybersecurity, and how they need to change to integrate them into their workflows and procedures [2]. Provide a high-level summary of the actions in these steps of a DevSecOps pipeline. In this system, the context for creating an application is provided by a mission thread. Finding the Zero Trust considerations that businesses need to make when completing the seven DevSecOps phases is their main goal [3].

Security is paramount in cloud-native environments because it involves distributed, dynamic systems with various interconnected services, making them inherently vulnerable to attacks. To safeguard data, apps, and infrastructure from risks and threats, cloud-native application and infrastructure security calls for a proactive, comprehensive strategy that considers the full lifecycle, from development to runtime [4].

Fortunately, the latest advancements and successes in the fields of AI, cloud computing, and microservices age offer

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

telecom providers optimism. A cognitive network that can coexist and adjust to network and vertical changes is made possible by the new accomplishments. A new idea known as the Cloud Native Environment (CNE) is created by telecom's shift to the micro-service paradigm [5].

There are suggestions for best practices in each of these frameworks. The requirements of business clouds are ease of use, adaptability, compliance with best practices, and support from extensive experiments like penetration testing to verify the proposals' robustness. However, there are no specifics regarding the actual use of these proposals or any convincing evidence of their adoption. It is in fact improbable that such frameworks will become operational without such a distinct "line of sight" between idea and execution. Additional simulations and tests are needed to confirm the suggested security framework's resilience and efficacy. This encourages us to combine their CCAF architecture by offering a comprehensive strategy that combines OpenStack security, multilayered security, and service integration to improve commercial cloud security. Multilayered security is implemented in corporate clouds using an integrated security architecture, and extensive penetration testing and experiments are conducted to confirm the resilience and efficacy of their methodology [6].

To achieve best practices in Zero Trust and DevSecOps, focus on continuous monitoring, secure coding, automating security, and educating developers about security concerns, while implementing tools for early vulnerability detection and robust access controls. Decided to investigate several facets of Coast in DevSecOps experimentally. Their initial goal was to categories and identify the difficulties that practitioners in this field confront. One possible explanation for the concerns that have been noted is a lack of proper knowledge of these difficulties. In order to facilitate Coast, they also sought to determine the best cooperation strategies that practitioners suggested [7].

A. Structure of the Paper

The paper is organized into several sections. Section II, Understanding Cloud-Native Security, introduces cloud-native computing principles, highlighting challenges like scalability and security. Zero Trust is defined in Section III Zero Trust Security Model in Cloud-Native Environments, along with its essential elements, including IAM, network segmentation, and ongoing monitoring. Section IV Security Frameworks for Cloud-Native Zero Trust and DevSecOps explores how DevSecOps integrates with Zero Trust to enhance security, referencing frameworks like NIST and MITRE ATT and CK. Section V, the Best Ways to Apply DevSecOps and Zero Trust in Cloud-Native Settings. Sections VI and VII Literature Review, previous studies on Zero Trust and DevSecOps, and the conclusion and future work.

II. UNDERSTANDING CLOUD-NATIVE SECURITY

Cloud-native Security is concerned with protecting apps and infrastructure built for cloud environments, emphasizing application-focused security, automated controls, and a change from conventional network-based defenses to a more flexible, adaptable approach [8]. The software methodology used to develop, implement, and oversee modern apps in Environments that use cloud computing is called "cloud native [9]." Developing applications that are highly scalable, flexible, and reliable is the aim of contemporary companies in order to enable them to be promptly updated to satisfy client needs. They do this by utilizing contemporary instruments and methods that naturally make developing cloud infrastructure applications easier.

A. Key Principles of Cloud-Native Computing

The fundamental ideas behind cloud-native computing focus on designing, building, and running scalable and resilient applications in dynamic cloud environments [10]. Here's a concise explanation of the core principles:

- **Automation:** Automating tasks such as building, deploying, and managing infrastructure to accelerate application development and improve operational efficiency.
- **Microservices:** Architecting applications as collections of small, self-contained, and loosely connected services with separate development, deployment, and scaling capabilities.
- **Containerization:** Packaging applications with their dependencies into containers, enabling reliable and effective implementation in a variety of contexts.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

- **Scalability:** Designing systems to scale up or down dynamically depending on workload requirements, guaranteeing cost and performance optimization [11].

B. Challenges in Cloud-Native Application

Cloud-native applications leverage microservices, containers, dynamic orchestration, and continuous deployment. While these bring numerous benefits like agility and scalability, they also introduce significant organizations must overcome these obstacles to guarantee dependability, performance, and security [12]. Cloud-native applications (CNAs) face several unique challenges, including:

Complex Architecture

Complex Architecture Applications designed for the cloud are often microservices-based, which creates a number of challenges for managing a large number of discrete and relatively independent services. Implementing good communication between these services, managing dependencies on other services and synchronizing the execution of these components is not a trivial task especially when the environment is dynamic as is in the cloud.

Scalability and Performance

Scalability and Performance This is a result of the concept of scalability, which is a fundamental characteristic of cloud-native systems, though it is difficult to come by in an efficient manner. Load balancing management, state management in stateless architecture, and managing the network latency between the various components are major challenges [13][14].

Security

One of the issues that must be addressed in applications designed for the cloud-native environment is security. Security must be extended at different layers thus other important steps include enforcing proper authentication and authorization controls, proper protection of data that is at rest, and multiple attacks due to multiple microservices and API calls [12].

III. ZERO TRUST SECURITY MODEL IN CLOUD-NATIVE ENVIRONMENTS

Traditional security methods are based on In response to the antiquated notion that every entity within a company's network should be trusted, Forrester Research developed Zero-Trust Protection. Various industry norms describe the Zero-Trust Security framework. ZTS, which includes defense-in-depth controls, is essentially a layered cybersecurity strategy. It makes it possible for a robust, reliable, and adaptable strategy to reduce threat risks that can arise as a result of abnormalities and sophisticated assaults [15]. The tenet of "never trust, always verify" is the foundation of the discipline [16].

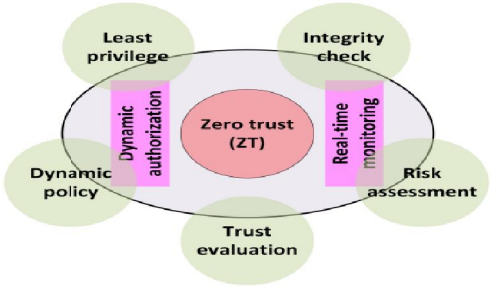

Fig. 1.Key Zero Trust Principles for Information Security [17]

A. Principles of Zero Trust (ZT)

The special U.S. NIST paper 800-27 lays forth the fundamental principles of ZT. Figure 1 outlines and clarifies the key concepts of ZT.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

- **Zero Trust:** There is no such thing as a trustworthy network asset or function; this includes all devices, computer resources, and the network's services. This implies that all communications have to follow the same third-party security guidelines [18].
- **Trust/Risk Evaluation:** Each request for access undergoes a thorough examination of trust and risk. Continuous and dynamic evaluations are performed [14].
- **Least Privilege:** If permission is given, it should be with the fewest possible rights. Depending on the resource's sensitivity, the access is only valid for that resource; it cannot be used for any other resource.
- **Dynamic Policy:** The choice to provide access requires a policy that may be changed as needed. Security status (credentials, software version/patches, location, etc.), subject behavioral traits, and network assets are the main deciding considerations.
- **Integrity Check:** The Continuous, ideally real-time, monitoring is done on the condition of all network resources' security and request themes. The device's and the network asset's security posture is assessed by an automated system or user's behavior patterns for compliance with security policy requirements [19].

B. Core Components of Zero Trust

The fundamental elements of a ZTA infrastructure are IAM, Network Segmentation (also known as micro-segmentation), and the maxim "never trust, always verify"[20], Device Security, Data Protection, and Continuous Monitoring and Verification. An enterprise-level ZTA implementation consists of several logical parts. It has the option of running these components on-premises or in the cloud [21].

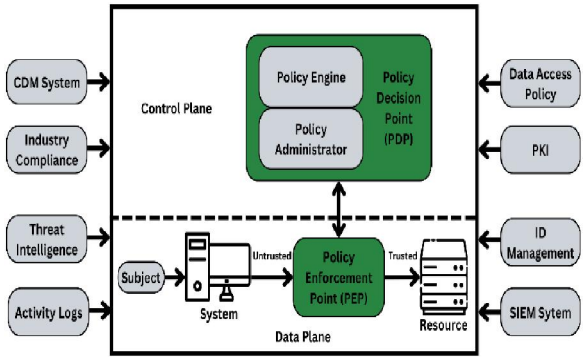

Fig. 2. Core Components and Logical Architecture of Zero Trust Security

Figure 2 shows the two wings, or planes, that make up the rational framework of a paradigm for zero trust security. Central to the process are the inputs from many sources, including CDM systems, which are processed by the Policy Engine, Policy Administrator, compliance standards, threat intelligence, and logs are all part of the Policy Decision Point (PDP), which is where access decisions are made [22]. In the Data Plane, it'll find the Policy Enforcement Point (PEP), which guards against people or systems gaining unauthorized access to the target resource. The concept embodies Zero Trust's guiding principle of "never trust, always verify" by enforcing access based on identity verification, dynamic risk assessments, and stringent data access regulations [23].

C. Implementing Zero Trust in Cloud-Native Infrastructure

The traditional perimeter security measures are inadequate to protect today's cloud infrastructures; Zero Trust has made network security its central tenet, particularly for cloud deployments. It may establish micro-segmentation and set network access controls with the help of AWS's Private Link tools, Network ACLs, and VPC Security Groups. Among the network security features offered by Azure are private connections, firewalls, and NSG [24][25]. The GCP offers VPC Service Controls and IAP as an alternative for enforcing access controls at the network layer. The biggest problem is in implementing consistent network policies across many clouds, even though all cloud environments have good security tools. Cisco Umbrella, Palo Alto Prisma Cloud, and Scalar are some of the third-party solutions that are necessary for implementing network segmentation and ZTNA in AWS, Azure, and GCP settings [26]. Since cloud-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

native settings no longer rely on perimeter-based security, Zero Trust has become an absolute necessity:

- **AWS:** Allows for micro-segmentation and enforces least privilege access via Private Link, Network ACLs, and Virtual Private Cloud Security Groups.
- **Azure:** Azure Firewall, Private Link, and Network Security Groups (NSGs) are used to enforce policies.
- **GCP:** Facilitates access management and the use of Identity-Aware Proxy (IAP) and VPC Service Controls to implement Zero Trust principles [27].

IV. SECURITY FRAMEWORKS FOR CLOUD-NATIVE ZERO TRUST AND DEVSECOPS

To achieve effective security in cloud-native environments, DevSecOps is indispensable. Integrating ZTA into DevSecOps workflows enhances security by enforcing consistent security controls across all stages from development to production, ensuring a robust and adaptable security posture. It is necessary to have a security architecture that is visibility-centric and can capture, process, and store important packets since massive attack activity can quickly deplete storage, server, and networking resources. Deploying in the cloud often involves nesting virtual machines and containerized environments according to service needs and operational standards [28][29]. The idea of zero trust security is one possible way to safeguard cloud-native edge settings' intricate networking across several environments. All entities are considered potentially untrustworthy according to the underlying Zero Trust concept. Consequently, DevSecOps teams need to keep a close eye on the system and make sure that all access requests and activities are being properly controlled [30].

A. NIST Zero Trust Architecture (ZTA)

The NIST defines ZT as a set of guiding principles that impose exact access decisions for every request in order to decrease or remove implicit trust in digital systems. This is done under the assumption that the network may already be compromised [31]. The corresponding general system architecture that underpins this security concept is known as ZTA. PEP and PDP manage authorization and authentication through an abstraction of zero-trust access. These elements make sure that access is only allowed when requirements specified by the policy are fulfilled by enforcing decisions on access control based on contextual factors and device security posture. NIST outlines seven foundational tenets of ZTA, which together support a fully secure and dynamic access model [32].

CISA Zero Trust Maturity Model

To assist companies with the CISA created the Zero Trust Maturity Model to help with the shift to ZT. ("Improving the Nation’s Cybersecurity") Zero Trust is given top priority as a national security necessity under Executive Order 14028, which prompted the introduction of the concept (CISA, 2021). The model evaluates maturity across five domains:

- Identity
- Device
- Network/Environment
- Application Workload
- Data

The capabilities in governance, automation, orchestration, transparency, and analytics support each area. Three stages of maturity are evaluated: Optimal, Advanced, and Traditional. While the model is comprehensive in its technological scope, it lacks emphasis on adapting Zero Trust principles to organizational processes and human factors [33].

B. Mitre ATT and CK for Cloud Security

A well-respected behavior-based model of adversarial in Plans, strategies, and the MITRE ATT&CK paradigm is grounded in observations from the actual world. Unlike threat models based solely on vulnerability reports, ATT&CK catalogues actual behaviors used by threat actors, including malware and red team simulations [34][35]. The documentation for each technique in ATT&CK details its operational mechanism, together with its real-world deployment reasons as well as detection and mitigation guidelines. The structure and documentation of ATT&CK enable defenders and forensic analysts to properly target critical activities for monitoring and reconstruct attacks to manage security risks successfully [36].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

V. BEST PRACTICES FOR IMPLEMENTING ZERO TRUST AND DEVSECOPS IN CLOUD-NATIVE ENVIRONMENTS

This section explains the vital techniques for cloud-native system protection through Zero Trust integration with DevSecOps. The approach focuses on protecting identity systems with MFA as well as implementing RBAC and ABAC access policies while deploying Kubernetes best practices and service mesh for infrastructure protection and using code analysis to secure CI/CD pipelines together with secrets management as well as implementing continuous threat detection and automated responses and conducting security training for team collaboration. The stated practices enable security protection of cloud-native deployments in a scalable and continuous fashion with resilience across their complete lifecycle [37].

A. Identity-Centric Security

The core starting point for Zero Trust security exists in identity procedures, which treat every user and machine as non-trustworthy. The implementation of Multi-Factor Authentication (MFA) with biometric technologies for authentication confirms access permission only for verified system identities. MFA improves safety by making users prove their identity through a combination of knowledge-based authentication, like passwords, and possession-based verification through devices and biometric authentication. The security system benefits from access control improvements achieved by a utilitarian approach; Permissions are granted according to work duties using ABAC and RBAC, as well as dynamic security factors such as device wellness or position. Such combined access management strategies define restrictive policies that analyze both fine-grained elements and situational factors.

B. Secure CI/CD Pipelines

The cloud-native settings, the CI/CD pipeline has to have strong security mechanisms in place. Because they protect production systems from cybersecurity threats. The automatic vulnerability detection is performed by Code analysis tools, including SCA, SAST, and DAST. Critical to secure system operations is proper management of secrets [38][39], which includes API keys and credentials; PaciCorp Vault and AWS Secrets Manager tools protect secrets from leaking through environment variables or version control systems. Adopting Policy-as-Code embeds security and compliance rules directly into the development pipeline, ensuring policies are applied consistently and automatically [40].

C. Infrastructure and Network Hardening

Securing infrastructure and networks is a critical element of zero trust. Using best practices for Kubernetes security, such as restricting privilege escalation, using network policies, and isolating workloads, helps reduce the attack surface. Service Meshes like Istio or Linkerd enable encrypted service-to-service communication, enforce access controls, and monitor traffic between microservices. For deeper network visibility and control, cloud-native firewalling combined with ebb (extended Berkeley Packet Filter) allows fine-grained, high-performance traffic filtering and behavior monitoring at the kernel level [41].

D. Monitoring and Incident Response

Continuous monitoring is essential for real-time threat identification and response. Tools such as XDR and SIEM gather and analyses data from several systems in order to identify anomalies and threats. Once threats are detected, automated incident response solutions often leverage SOAR (Security Orchestration, Automation, and Response) to trigger predefined actions to contain and remediate attacks. Meanwhile, continuous audit and compliance monitoring ensure that systems adhere to corporate policies and regulatory requirements, lowering the possibility of noncompliance [42].

E. Cultural and Organizational Practices

A strong security culture is vital for the effective application of DevSecOps and Zero Trust. Security Champion Programs embed security advocates within development teams to promote best practices and act as liaisons to security experts. Regular security training and awareness sessions ensure all team members understand security risks and how to mitigate them. Finally, promoting cross-functional. A shared security responsibility is established by cooperation

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

between the operations, security, and development teams. It makes it possible to resolve vulnerabilities and events more quickly [43].

VI. LITERATURE REVIEW

In this section, previous research on DevSecOps and Zero Trust in Cloud-Native Environments with Security Frameworks is summarized. Table I highlights the combination of cryptography frameworks and Zero Trust principles, automated testing, and dynamic defense mechanisms in cloud-native environments. Collectively, they underscore the significance of DevSecOps practices and security frameworks in enhancing trust, efficiency, and resilience against evolving cyber threats.

Amaral and Gondim (2021) suggested that A cyber supply chain employs a Zero Trust design. This study's primary contribution is a domain-specific security control configuration for a cyber supply chain that makes use of Zero Trust architectural concepts to improve cyber supply chain security. Component vulnerabilities that were previously thought to be secure because of relationships of perceived trust are being taken advantage of. One strategy to reduce this type of cyber risk is to use a Zero Trust architecture. Attacks with advanced capabilities have targeted the cyber supply chain [44].

Deepika et al. (2022) proposed a framework for accessing data in a cloud environment that is security-enabled (SEFAI), which uses a variety of safe encryption methods to protect data while it is being accessed from the cloud. The approach suggested in this study increases data security in cloud environments and keeps information from being accessed by unauthorized individuals. When using the cloud to access information, security concerns are crucial. Using cryptographic methods, a novel framework is created to address the security issue. Compared to the previous framework, the created framework, "Security Algorithms for Cloud Computing (SACC)," takes less time to encrypt and decode data [45].

Jayakody et al. (2019) provide a method for automating security testing and vulnerability scanning using a cloud-native technology that offers a standalone environment that requires only a single click to boot up the scanners and set up settings. Standards and security scanners have been developed by security groups. Online security testers are spending a lot of time manually assessing the security of web applications because the environments and configurations they set up take a lot of time [46].

Lim and Kim (2021) provide service function chaining in a single cloud system that uses network functions selected by the classifier based on the service categorization result of the traffic to handle VNF and CNF. Nonetheless, the VNF and CNF combo will endure for a very long time under actual working conditions. To supply network services, VNF and CNF create a chain. A distinct network is needed to connect VNF and CNF, which were installed utilizing a cloud system. Additionally, the network function that controls traffic according to service type in a container environment is somewhat different even when the same network service is offered [47].

Sojan et al. (2021) created a replicable solution that tracks the cloud-native infrastructure and application level, based on the well-liked microservice architectural style, to close this gap. Cloud-native settings are being adopted by software development and operations more and more. One of the factors contributing to this shift is the growing popularity of development methodologies like DevSecOps. Monitoring is seen as a crucial DevSecOps practice, and there are already many different tool options on the market to handle this new change [48].

Wu et al. (2022) latent persistent threats to cloud environments show that the NFV-based cloud environment and the dynamic defense concept are very consistent and complementary. Thus, when the two sets of security threats meet, a lot of emphasis has been paid to figuring out how to prevent the unpredictability of cloud security due to complex manufacturing relationships and untrustworthy hardware and software suppliers. Next, it is suggested that NFV-based clouds be aligned with intrinsic cloud security (iCS), It provides a smooth transition and mutually beneficial growth between NFV-based clouds and security by imitating defense and the MTD paradigm [49].

TABLE I. Literature on Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks

Reference	Key Topic	Focus Area	Findings/Insights
Amaral and Gondim (2021)	Zero Trust in Cyber Supply Chains	Security Control Organization	Proposes the organization of security controls based on Zero Trust principles to secure cyber supply chains from sophisticated threats and eliminate implicit trust in

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

			components.
Deepika et al. (2022)	Secure Framework for Cloud Data Access	Cryptography-Based Security in Cloud	Introduces SEFAI framework using encryption algorithms to securely access cloud data, outperforming SACC in encryption/decryption efficiency while preventing unauthorized access.
Jayakody et al. (2019)	Automated Security Testing in Cloud-Native Environments	Vulnerability Scanning & Web App Security	Presents a cloud-native solution that automates vulnerability scanning setup, reducing the manual effort and time needed for secure configuration of web applications.
Lim and Kim, (2021)	Service Function Chaining with VNFs and CNFs	Network Security in Mixed Cloud Environments	Proposes traffic-based classifier for chaining VNFs and CNFs; addresses deployment and service differentiation challenges in hybrid (container and VM) cloud setups.
Sojan et al. (2021)	DevSecOps Monitoring in Microservices	Observability in Cloud-Native Infrastructure	Offers a microservice-based monitoring solution for both application and infrastructure layers, highlighting monitoring as a critical DevSecOps practice in cloud-native adoption.
Wu et al. (2022)	Intrinsic Cloud Security (iCS) with NFV	Dynamic Defense & Moving Target Security	Proposes iCS framework combining NFV and moving target defense to counter persistent threats, enabling adaptive and evolving cloud security strategies.

VII. CONCLUSION AND FUTURE WORK

In conclusion, cloud-native architectures that combine DevSecOps and Zero Trust security offer a robust framework for mitigating cyber risks and ensuring resilient security across the entire software development lifecycle. Organizations must make detailed security management solutions their highest priority because cloud-native technologies, together with microservices architecture, have become essential for adoption. The fundamental principle of Zero Trust security is "never trust, always verify" provides an optimal solution for protecting distributed cloud systems with their volatile nature. Organizations defending against changing cyber threats can achieve better protection through identity-centric security and monitored continuous access controls, together with CI/CD pipeline protection. In cloud-native settings, enterprises must leverage security while adopting Zero Trust frameworks that include NIST ZTA together with CISA's Zero Trust Maturity Model and MITRE ATT&CK for Cloud Security. These frameworks offer precise instructions and organizational standards that guide organizations to implement a Zero Trust infrastructure properly. An effective Zero Trust deployment demands both technological and organizational and procedural adjustments according to the analysis presented throughout this paper.

Future investigations about these areas should unify Zero Trust and DevSecOps platforms while optimizing them to manage current cloud-native complications. Advanced machine learning and artificial intelligence techniques that enable automatic responses and real-time anomaly detection, as well as tools to improve the feasibility of a flexible security framework across various cloud settings, must be the focus of the study. The assessment of Zero Trust benefits and practical difficulties. More research is needed in multi-cloud and hybrid cloud deployments because new technologies like edge computing and 5G networks come into play.

REFERENCES

[1] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," Sustainability (Switzerland). 2022. doi: 10.3390/su141811213.

[2] S. S. S. Neeli, "Optimizing Database Management with DevOps: Strategies and Real-World Examples," J. Adv. Dev. Res., vol. 11, no. 1, 2020.

[3] G. Sanders, T. Morrow, N. Richmond, and C. Woody, "Integrating Zero Trust and Devsecops," Softw. Eng. Inst., 2021.

[4] A. Immadisetty, "Edge Analytics vs. Cloud Analytics: Tradeoffs in Real-Time Data Processing," J. Recent Trends Comput. Sci. Eng., vol. 13, no. 1, pp. 42–52, 2016.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

[5] A. Boudi, M. Bagaa, P. Poyhonen, T. Taleb, and H. Flinck, "AI-Based Resource Management in Beyond 5G Cloud Native Environment," IEEE Netw., vol. 35, no. 2, pp. 128–135, Mar. 2021, doi: 10.1109/MNET.011.2000392.
[6] V. Chang, Y. H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Futur. Gener. Comput. Syst., 2016, doi: 10.1016/j.future.2015.09.031.
[7] R. Rajapakse, M. Zahedi, and M. A. Babar, "Collaborative Application Security Testing for DevSecOps," 2022, doi: 10.48550/arXiv.2211.06953.
[8] N. Patel, "Sustainable Smart Cities : Leveraging IoT and Data Analytics for Energy Efficiency and Urban Development," J. Emerg. Technol. Innov. Res., vol. 8, no. 3, 2021.
[9] A. Goyal, "Scaling Agile Practices with Quantum Computing for Multi-Vendor Engineering Solutions in Global Markets," Int. J. Curr. Eng. Technol., vol. 12, no. 06, Jun. 2022, doi: 10.14741/ijcet/v.12.6.10.
[10] A. Gogineni, "Novel Scheduling Algorithms for Efficient Deployment of Mapreduce Applications in Heterogeneous Computing," Int. Res. J. Eng. Technol., vol. 4, no. 11, 2017.
[11] S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," Int. Res. J. Mod. Eng. Technol. Sci., vol. 3, no. 12, Jan. 2021, doi: 10.56726/IRJMETS17782.
[12] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.
[13] R. Tarafdar and Y. Han, "Finding Majority for Integer Elements," J. Comput. Sci. Coll., vol. 33, no. 5, pp. 187–191, 2018.
[14] S. S. S. Neeli, "Transforming Data Management: The Quantum Computing Paradigm Shift," Int. J. Lead. Res. Publ., vol. 2, no. 8, 2021.
[15] S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," Int. J. Curr. Eng. Technol., vol. 12, no. 06, Jun. 2022, doi: 10.14741/ijcet/v.12.6.11.
[16] B. Ali, S. Hijjawi, L. H. Campbell, M. A. Gregory, and S. Li, "A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing," Secur. Commun. Networks, 2022, doi: 10.1155/2022/3178760.
[17] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN," Computer Networks. 2022. doi: 10.1016/j.comnet.2022.109358.
[18] A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.
[19] V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization AI for Cybersecurity Incident Investigations," Int. J. Res. Anal. Rev., vol. 3, no. 3, 2016.
[20] H. S. Chandu, "A Survey of Memory Controller Architectures: Design Trends and Performance Trade-offs," Int. J. Res. Anal. Rev., vol. 9, no. 4, pp. 930–936, 2022.
[21] K. Olson and E. Keller, "Federating trust: Network orchestration for cross-boundary zero trust," in Proceedings of the 2021 SIGCOMM 2021 Poster and Demo Sessions, Part of SIGCOMM 2021, 2021. doi: 10.1145/3472716.3472865.
[22] V. S. Thokala, "Efficient Data Modeling and Storage Solutions with SQL and NoSQL Databases in Web Applications," Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 470–482, Apr. 2022, doi: 10.48175/IJARSCT-3861B.
[23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
[24] A. Goyal, "Enhancing Engineering Project Efficiency through Cross-Functional Collaboration and IoT Integration," Int. J. Res. Anal. Rev., vol. 8, no. 4, pp. 396–402, 2021.
[25] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," ESP J. Eng. Technol. Adv., vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.
[26] A. A. Solanke, "Zero Trust Security Architectures for Multi-Cloud Environments: Implementation Strategies and Measurable Outcomes," World J. Adv. Eng. Technol. Sci., vol. 3, no. 2, pp. 122–134, Oct. 2021, doi: 10.30574/wjaets.2021.3.2.0054.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

[27] S. Pandya, "Innovative Blockchain Solutions for Enhanced Security and Verifiability of Academic Credentials," Int. J. Sci. Res. Arch., vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.
[28] K. M. R. Seetharaman, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/IJARSCT-6268B.
[29] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Inteligence and Machine learning in Cloud Computing Operations," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 7, no. 2, 2019.
[30] J. S. Shin and J. Kim, "Smartx Multi-Sec: A Visibility-Centric Multi-Tiered Security Framework for Multi-Site Cloud-Native Edge Clusters," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3115523.
[31] S. Pandya, "Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralised Voting System," Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 865–876, Aug. 2022, doi: 10.48175/IJARSCT-12467H.
[32] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access. 2022. doi: 10.1109/ACCESS.2022.3174679.
[33] M. Dawson, R. Bacius, L. B. Gouveia, and A. Vassilakos, "Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors," L. Forces Acad. Rev., 2021, doi: 10.2478/raft-2021-0011.
[34] K. Murugandi and R. Seetharaman, "A Study of Supplier Relationship Management in Global Procurement : Balancing Cost Efficiency and Ethical Sourcing Practices," Int. J. Adv. Res. Sci. Commun. Technol., vol. 2, no. 1, pp. 724–733, 2022, doi: 10.48175/IJARSCT-7744B.
[35] V. Singh, "Lessons Learned from Large-Scale Oracle Fusion Cloud Data Migrations," Int. J. Sci. Res., vol. 10, no. 10, pp. 1662–1666, 2021.
[36] C. Liu, A. Singhal, and D. Wijesekera, "Forensic Analysis of Advanced Persistent Threat Attacks in Cloud Environments," in IFIP Advances in Information and Communication Technology, 2020. doi: 10.1007/978-3-030-56223-6_9.
[37] G. Modalavalasa, "The Role of DevOps in Streamlining Software Delivery: Key Practices for Seamless CI/CD," Int. J. Adv. Res. Sci. Commun. Technol., vol. 1, no. 12, pp. 258–267, Jan. 2021, doi: 10.48175/IJARSCT-8978C.
[38] R. Patel and R. Tandon, "Advancements in Data Center Engineering: Optimizing Thermal Management, HVAC Systems, and Structural Reliability," Int. J. Res. Anal. Rev., vol. 8, no. 2, 2021.
[39] A. Gogineni, "Automated Deployment and Rollback Strategies for Docker Containers in Continuous Integration/Continuous Deployment (CI/CD) Pipelines," Int. J. Multidiscip. Res. Growth Eval., vol. 1, no. 5, 2020.
[40] Anju and A. V. Hazarika, "Extreme Gradient Boosting using Squared Logistics Loss function," Int. J. Sci. Dev. Res., vol. 2, no. 8, pp. 54–61, 2017.
[41] N. Malali, "Microservices In Life Insurance : Enhancing Scalability and Agility in Legacy Systems," Int. J. Eng. Technol. Res. Manag., no. 03, pp. 118–125, 2022, doi: 10.5281/zenodo.15176335.
[42] M. Felderer, M. Büchler, M. Johns, A. D. Brucker, R. Breu, and A. Pretschner, "Security Testing: A Survey," in Advances in Computers, 2016. doi: 10.1016/bs.adcom.2015.11.003.
[43] T. Rangnau, R. V. Buijtenen, F. Fransen, and F. Turkmen, "Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines," in Proceedings - 2020 IEEE 24th International Enterprise Distributed Object Computing Conference, EDOC 2020, 2020. doi: 10.1109/EDOC49727.2020.00026.
[44] T. M. S. do Amaral and J. J. C. Gondim, "Integrating Zero Trust in the cyber supply chain security," in 2021 Workshop on Communication Networks and Power Systems, WCNPS 2021, 2021. doi: 10.1109/WCNPS53648.2021.9626299.
[45] Deepika, R. Kumar, and Dalip, "Security Enabled Framework to Access Information in Cloud Environment," in 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, COM-IT-CON 2022, 2022. doi: 10.1109/COM-IT-CON54601.2022.9850906.
[46] J. A. D. C. A. Jayakody, A. K. A. Perera, and G. L. A. K. N. Perera, "Web-Application Security Evaluation as a Service with Cloud Native Environment Support," in 2019 International Conference on Advancements in Computing (ICAC), IEEE, Dec. 2019, pp. 357–362. doi: 10.1109/ICAC49085.2019.9103414.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 3, January 2023

[47] H. Lim and Y. Kim, "A Design of Service Function Chaining with VNF and CNF on Cloud Native Environment," in International Conference on ICT Convergence, 2021. doi: 10.1109/ICTC52510.2021.9620867.
[48] A. Sojan, R. Rajan, and P. Kuvaja, "Monitoring Solution for Cloud-Native DevSecOps," in Proceedings - 2021 IEEE 6th International Conference on Smart Cloud, SmartCloud 2021, 2021. doi: 10.1109/SmartCloud52277.2021.00029.
[49] Q. Wu, R. Wang, X. Yan, C. Wu, and R. Lu, "Intrinsic Security: A Robust Framework for Cloud-Native Network Slicing via a Proactive Defense Paradigm," IEEE Wirel. Commun., 2022, doi: 10.1109/MWC.001.2100251.