International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

# Micro segmentation And Zero Trust Architecture For Adaptive Security Enforcement In Cloud Networks

*Akula Rajitha[1], Dr. S.G. Santhi[2]*
*[1]Research Scholar, Department of Computer Science Engineering, Annamalai University Chidambaram, Tamil Nadu*
*[2]Associate Professor, Department of Computer Science Engineering, Annamalai University Chidambaram, Tamil Nadu*
***Emails:*** *Akularajitha32@gmail.com[1]*

***Abstract***
*The rising use of cloud computing has also provided exposure to the enterprise networks to advanced cyber threats, especially lateral movement attacks and insiders abuse, which the traditional perimeter-based security model does not adequately address. Zero Trust Architecture (ZTA) has become an exciting concept because it eradicates the unwritten trust in the paradigm by imposing a never-ending identity validation and the least-privilege access. Nevertheless, the use of Zero Trust without internal traffic control on a fine level is prone to the spread of east-west attacks. In an attempt to overcome this drawback, this paper presents an adaptive Zero Trust-enabled architecture of microsegmentation that can be implemented in the cloud network involving identity-based access control and network isolation (workload) remedies. The offered methodology uses the continuous risk assessment of the data based on identity attributes, contextual data, and real-time telemetry to dynamically implement micro-perimeters and limit the unauthorized communication between workloads. A policy decision, risk assessment, and adaptive segmentation is formulated mathematically to have a scalable and rigorous implementation. Based on experimental assessment on a cloud testbed, the suggested framework would significantly decrease the rate of lateral movement success, enhance attack containment, and decrease the rate of policy violation with a low level of enforcement latency. These findings confirm the usefulness and efficiency of implementing Zero Trust and adaptive microsegmentation in securing the modern cloud environments.*

***Keywords:*** *Zero Trust Architecture, Microsegmentation, Cloud Network Security, Lateral Movement Mitigation, Identity-Aware Access Control, Adaptive Security Enforcement, Software-Defined Networking*

## 1. Introduction

The mass-use of cloud computing has radically changed the way organizations implement, run and expand digital services. Cloud computing supports the ability to on-demand resources, international accessibility, and economical infrastructure administration. Nonetheless, this high velocity shift has also come with its own security challenges especially because of the dynamic, multi-tenant and highly intertwined characteristics of cloud environments. Conventional perimeter-based security paradigms that are based on implicit trust in internal networks are becoming useless in the face of current cyber threats like lateral movement attacks, insider threats and advanced persistent threats (APTs). Traditional cloud security models have it that once a party gets access into the network perimeter, it usually has wide internal access. This is an implicit trust model, which enables the attackers to perform lateral movement among workloads once initially compromised, resulting in massive breach of data and service disruption. It is also worsened by the increased sophistication of east west traffic in cloud data centers, since most of the internal communications are not effectively monitored and controlled. As a result, a high level of urgency to develop security models that presuppose the default of breach and provide the constant verification of all access points is crucial. Zero Trust Architecture (ZTA) has already appeared as a potential solution to such shortcomings by eradicating implicit trust and applying the measure of never trust, always verify. Zero Trust focuses on identity-centric security,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

continuous authentication, least-privilege access, and adaptive policy implementation among the users, devices, applications, and workloads. Although ZTA is a very powerful tool to strengthen access control mechanisms, its efficiency is low when used without network isolation (in fine grain). Zero Trust in itself does not limit unauthorized subsequent lateral communication between cloud workloads once the access has been granted. Micro segmentation is used together with Zero Trust to provide workload-level isolation of networks in cloud infrastructure. Micro segmentation creates the least-privilege communication by splitting the network into small, logically restricted segments and reducing the attack front. A micro-perimeter is applied to each workload, and only specifically authorized traffic is passed through it. Nevertheless, the current micro segmentation solutions tend to use hard and fast rules, system configuration or infrastructure-based mechanisms to restrict scalability and flexibility in dynamic cloud environments. The paper will argue that micro segmentation and Zero Trust should be implemented together in the quest to attain effective cloud security. Based on this, we postulate a new integrated model that integrates the concepts of Zero Trust and adaptive micro segmentation of cloud networks. The suggested solution uses identity-based access control and software-defined networking, as well as context-based policy implementation to dynamically protect inter-workload communication. With identity verification done again and again and fine-grained segmentation, the framework is very effective in limiting lateral movement and breach radius in case of a compromise. The main contributions of this paper are summarized as follows:

- Design of a micro segmentation-enabled Zero Trust security architecture for cloud networks
- Development of an adaptive policy enforcement mechanism based on identity and contextual attributes
- Comprehensive security analysis addressing lateral movement and insider threat scenarios
- Experimental evaluation demonstrating improved attack containment and policy enforcement efficiency

The remainder of this paper is organized as follows. Section II reviews related work on Zero Trust and micro segmentation in cloud environments. Section III presents the proposed system architecture and policy framework. Section IV discusses the experimental setup and performance evaluation results. Finally, Section V concludes the paper.

## 2. Literature Survey

Zero Trust Architecture (ZTA) has become the new paradigm in the field of enterprise and cloud security by removing implicit trust and implementing relentless verification of each access request. ZTA principles were put down in writing in the National Institute of Standards and Technology (NIST) Special Publication SP 800-207 that provides a list of logical components including the policy engine, policy administrator, and policy enforcement point [1]. The model focuses on identity-based access control, posture checking of devices and dynamism of policy analysis instead of fixed network boundaries. A number of studies have applied the NIST ZTA model to cloud and hybrid platforms and have shown a better resilience to credential theft and insider threats [2]. Yet, the majority of current ZTA deployments are concentrated on north south traffic authentication and authorization schemes, and the east west traffic in the cloud environments is not sufficiently secured. It has also been noted that ZTA implementations that lack internal traffic controls are susceptible to attacks of lateral movement after the access has been approved [3]. Micro segmentation has been suggested as a useful method to mitigate the attack surface in cloud and virtualized systems by imposing workload-level isolation that is finer-grained. Compared to the conventional methods of network segmentation, including VLANs, subnet-based controls, micro segmentation provides a policy enforcement at application or workload level, restricting unauthorized communication channels [4]. Recently, the literature has addressed software-defined networking (SDN) as a scalable framework that can be used to support micro segmentation in cloud data centers. Frameworks based on SDN make access policy dynamically between workloads and virtual machines and allow flexible and programmable segmentation [5]. Research in multi-tenant clouds environments has demonstrated that

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

micro segmentation is an effective way of isolating infected load and limiting the spread of attacks [6]. In spite of these benefits, there are numerous current micro segmentation products based on fixed rules and hand-written policy setup, which restricts the ability to be flexible in the strongly dynamic and elastic cloud environments. Even though Zero Trust Architecture reinforces the identity verification and access control, it does not necessarily limit the subsequent lateral communication between workloads following authorization. When attackers gain access, they may continue to take advantage of implicit trusting relationships within the internal network. Micro segmentation on the other hand, provides a good control measure over lateral movements but tends not to have identity awareness or real-time verification. Segmentation policies, in which contextual identity validation is not performed, have been demonstrated to allow unauthorized access in case the valid credentials have been compromised [7]. A number of survey research papers have found that the implementation of both Zero Trust and micro segmentation alone offers partial security coverage and gap in cloud protection systems [8], [9]. With cloud native systems that have short-lived workloads and flexible communication patterns, it is easy to find that the static segmentation policies become outdated almost immediately, leading to the risk of improper configuration, and policy drift. In order to address the critiques of standalone security models, recent works have examined how Zero Trust principles can be combined with micro segmentation. Micro segmentation has been suggested to be a vital enforcement tool to Zero Trust the networks, especially to manage east west traffic in cloud systems [10]. Micro segmentation that is identity conscious, such as the use of authentication and authorization cues in segmentation policies, have shown better containment of lateral attacks [11]. Recent frameworks have suggested Zero Trust-based cloud security architecture based on SDN and policy-based segmentation mechanisms [12]. Although these methods help to minimize the unauthorized access, they frequently use predefined or fixed policies and do not have the adaptive improvement with respect to the real-time analysis of the risk [13]. In the same way, the studies concentrating on cloud-native and Kubernetes-based applications of Zero Trust concepts using network policies and service meshes also indicate issues with policy sprawl, operational complexity, and scalability [14], [15].

## 3. Proposed Methodology

In this case, the architecture proposed combines the Zero Trust Architecture (ZTA) and adaptive micro segmentation to achieve fine-grained and identity-aware security enforcement within the cloud networks. It is an architecture with a policy-oriented design that is modular and continuously assesses trust, implements least-privilege access and dynamically limits lateral movement across cloud workloads as represented by figure1.

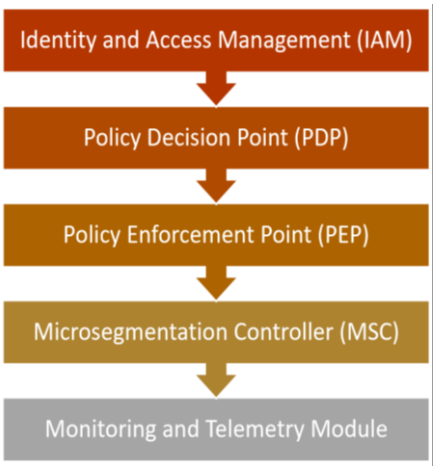


**Figure 1 Proposed Methodology**

### 3.1.Identity and Access Management (IAM)

Identity and Access Management (IAM) is the underlying layer of trust of the proposed zero trust-enabled micro segmentation approach. Without the implicit network trust, every access control is made on the basis of verifiable digital identities and contextual attributes. The IAM module performs the tasks of authenticating, authorizing, and constantly validating users, devices, services, and workloads communicating in the cloud environment. The entities are given individual cryptographic identities, which can be a certificate or token, fixed to a collection of security attributes such as role, level of privilege, tenant domain, and type of workload. Multi-factor authentication (MFA) and short-lived credential are used as strong authentication measures

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

to mitigate the threat of credential compromise and replay attacks. These identities are verified each time of access so that the principle of never trust, always verify is adhered to as a Zero Trust principle.The IAM module provides real-time identity attributes to the Policy Decision Point (PDP) to assist in enforcing fine grained policies. Such attributes are the strength of authentication, device posture score, compliance status, and historical trust level. The IAM module facilitates the process of access control by providing attribute-based access control (ABAC) and least-privilege access control by exposing identity metadata instead of hard-coded credentials over cloud workloads. The identity trust contribution for an entity s is represented as:

$$T_{id}(s) = \sum_{k=1}^{n} \omega_k \cdot a_k(s) \text{-----1}$$

Tthe value of ak(s) is normalized identity attributes (e.g., MFA status, role confidence, posture score) and the weight of the same is 9. This is an identity trust score that is later combined with contextual and behavioral factors during the process of risk evaluation. The IAM module also implements the lifecycle of identity validation in the session. There is periodic revalidation of credentials and access privileges may be dynamically revoked on the occurrence of anomalies or policy violations. Identity isolation is also provided on a tenant basis in multi-tenant cloud environments to ensure that identities are not reused across domains to avoid unauthorized cross-tenant access. The IAM module allows providing secure, scalable, and adaptive access control, creating the foundation of the suggested Zero Trust and micro segmentation methodology by establishing strong identity verification, rich attribute exposure, and continuous validation.

### 3.2.Policy Decision Point (PDP)

Policy Decision Point (PDP) is the key element of the decision-making of the proposed Zero Trust-based micro segmentation framework. It mainly serves to examine every request to access based on checked identity attributes, contextual data, and risk that is calculated dynamically and produce fine-grained access control determinations that implement least-privilege access in cloud networks. For each access request

$$R = s, d, a, t, c \text{ ----2}$$

the PDP receives the following inputs:

- Identity trust score from IAM: Tid(s)
- Context vector: x=[x1,x2,…,xm]
- Telemetry-derived anomaly score: A(s,d)
- Workload sensitivity level: S(d)S(d)S(d)

The PDP computes a unified risk score by combining identity, context, and behavioral indicators:

$$R(\mathcal{R}) = \alpha_1\left(1 - T_{id}(s)\right) + \alpha_2 \cdot |x| + \alpha_3 \cdot A(s,d) + \alpha_4 \cdot S(d) \text{-----3}$$

where

$$\alpha i = 1 \sum_{i=1}^{4} \alpha_i \text{-----4}$$

The corresponding trust score is defined as:

$$\tau(\mathcal{R}) = 1 - R(\mathcal{R}) \text{---5}$$

The PDP enforces Zero Trust using an attribute-based access control (ABAC) decision function:

$$ABAC(s,d,a,c) = \mathbb{1}[role(s) \in \Pi(d,a) \wedge posture(s) \geq \delta \wedge compliance(s) = 1] \text{----6}$$

where Π(d,a) represents permitted roles and δ is the minimum acceptable posture score.

To enforce continuous verification, the PDP periodically re-evaluates active sessions:

$$\tau_t(\mathcal{R}) = \beta\tau_{t-1}(\mathcal{R}) + (1-\beta)\tau_{inst}(\mathcal{R}) \text{-----7}$$

If

$$\tau_t(\mathcal{R}) < \theta(d,a) \text{----- 8}$$

the PDP triggers immediate policy revocation or restriction via the Micro segmentation Controller.

### 3.3. Policy Enforcement Point (PEP)

Policy Enforcement Point (PEP) enforces the runtime policy of authorization decisions made by the Policy Decision Point (PDP). Working in the data plane, the PEP will make sure that all authorized communications are within the Zero Trust constraints and micro segmentation rules. Both north-south and east-west traffic are enforced at finer granularity as well and updated continuously on a session lifetime basis. For an authorized request R, the PEP enforces a rule set:

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

$$\mathcal{E}(\mathcal{R}) = \{\mathcal{C}_{port}, \mathcal{C}_{proto}, \mathcal{C}_{time}, \mathcal{C}_{rate}, \mathcal{C}_{path}\}\text{----}$$
9

where each Ck is a constraint derived from PDP outputs and micro segmentation directives. Only explicitly permitted ports and protocols are allowed:

$$\mathcal{C}_{port}: \quad p \in \mathcal{P}_{allow}(d,a)\text{----}10$$

Any packet with p∉Pallow is denied.

Access may be limited to an approved time window:

$$\mathcal{C}_{time}: \quad t \in [t_{start}, t_{end}]\text{----}11$$

If t violates this interval, the PEP revokes the session regardless of prior authorization. To mitigate scanning, brute force, and data exfiltration:

$$\mathcal{C}_{rate}: \quad \lambda_{sd}(t) \le \lambda_{max}(d,a)\text{---}12$$

Where λsd(t) is the observed packet or request rate from s to d Let the segmentation adjacency matrix be A(t). The PEP enforces:

$$\mathcal{C}_{path}: \quad A_{sd}(t) = 1\text{Cpath: }Asd(t) = 1\text{----}13$$

If the Micro segmentation Controller updates Asd(t)=0, the PEP immediately terminates the flow. During an active session, trust is re-evaluated periodically:

$$\tau_t(\mathcal{R}) = \gamma\tau_{t-1}(\mathcal{R}) + (1-\gamma)\tau_{inst}(\mathcal{R})\text{----}14$$

Each enforcement action produces telemetry T:

$$\mathcal{T} = \{(s,d,p,\pi,\lambda,t,\text{action})\}\text{----}15$$

which is forwarded to the Monitoring Module to update risk estimates and trigger adaptive policy refinement.

### 3.4. Micro segmentation Controller (MSC)

The Micro segmentation Controller (MSC) is in charge of coordinating workload-based network isolation, fine-grained by transforming results of Zero Trust authorization into enforceable segmentation policies. The MSC exists between the Policy Decision Point (PDP) and distributed Policy Enforcement Points (PEPs) to ensure east west traffic in cloud networks is explicitly based on least-privilege principles and dynamically responds to changing risk conditions.

The cloud environment is modeled as a directed graph:

$$G(t) = (V, E(t))\text{----}16$$

where
V = w1, w2, …, wn

represents workloads (VMs, containers, microservices), and E(t)⊆V×V denotes allowed communication paths at time t. Upon receiving a PDP decision for request R the MSC updates segmentation rules using:

$$\Phi: (\mathcal{R}, \tau(\mathcal{R})) \to A_{sd}(t)\text{-----}17$$

To support adaptive security, the MSC maintains a communication risk score between workloads wi and wj:

$$r_{ij}(t) = \alpha r_{ij}(t-1) + (1-\alpha)\text{----}18$$

Where rij(t) is instantaneous risk derived from telemetry (anomalies, violations), and α∈(0,1) controls responsiveness. The MSC aims to minimize both security exposure and over-connectivity by solving:

$$\min_{A(t)} \left(\lambda_1 \textstyle\sum_{i,j} A_{ij}(t) \cdot r_{ij}(t) + \lambda_2 |A(t)|_0\right)\text{----}19$$

where

- the first term minimizes cumulative communication risk,
- the second term (‖A(t)‖0) enforces sparsity (least privilege),
- λ1,λ2 balance security and service availability.

Before deploying updated rules, the MSC validates segmentation consistency:

$$\forall (i,j): A_{ij}(t) = 1 \Rightarrow \exists \text{ valid PDP authorization-}$$
$$\text{--}20$$

This prevents stale or conflicting policies and ensures that all allowed paths are explicitly authorized.

### 3.5. Monitoring and Telemetry Module

Monitoring and Telemetry Module has the ability to give visibility, feeds, and situational awareness throughout the proposed Zero Trust-enabled micro segmentation architecture. As per the principle of continuous verification of Zero Trust, this module

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

will ensure that the trust is not assumed but constantly measured allowing the assessment of the risk dynamically and response of the policy. Let the telemetry stream at time t be defined as:

$$\mathcal{T}(t) = \{\tau_1(t), \tau_2(t), \ldots, \tau_k(t)\} \text{----21}$$

where each telemetry record τk(t) captures security-relevant observations such as:

- inter-workload traffic flows,
- authentication and authorization logs,
- policy enforcement actions,
- anomaly and intrusion alerts,
- session duration and frequency.

Each telemetry record is represented as:

$$\tau_k(t) = s, d, p, \pi, \lambda, t, \eta \text{ ----22}$$

where
s,d= source and destination identities,
p = port, π\piπ = protocol,
λ = observed traffic rate,
t = timestamp,
η = enforcement outcome (allow/deny/limit).
For each workload pair (i,j), a baseline behavior profile is maintained:

$$\mu_{ij} = E[\lambda_{ij}], \quad \sigma_{ij} = \mathrm{Var}[\lambda_{ij}] \text{---23}$$

The behavioral deviation score is computed as:

$$D_{ij}(t) = \frac{|\lambda_{ij}(t) - \mu_{ij}|}{\sigma_{ij} + \epsilon} \text{---24}$$

where ϵ avoids division by zero.
A deviation is flagged if:

$$D_{ij}(t) > \delta_d * Z \text{---25}$$

where δd is a deviation threshold.

### 3.6. Evaluation Metrics

To fully evaluate the efficiency of the suggested methodology, the security-centric and performance-centric metrics are considered. This is a ratio of unauthorized lateral movement attempts which achieve unintended workloads:

$$\mathrm{LMSR} = \frac{N_{\text{successful lateral attempts}}}{N_{\text{total lateral attempts}}} \text{----26}$$

A lower LMSR indicates stronger containment of east–west attacks. Attack containment rate quantifies the framework's ability to confine compromises within a limited micro-segment:

$$\mathrm{ACR} = 1 - \frac{N_{\text{compromised workloads}}}{N_{\text{reachable workloads}}} \text{----27}$$

Higher ACR values indicate effective micro-perimeter enforcement. This metric captures the frequency of detected policy violations during operation:

$$\mathrm{PVR} = \frac{N_{\text{policy violations}}}{N_{\text{total access requests}}} \text{---28}$$

It reflects the effectiveness of Zero Trust policy enforcement and anomaly detection. Enforcement latency measures the time required to evaluate and enforce a policy decision:

$$L_{\text{enf}} = t_{\text{enforce}} - t_{\text{request}} \text{----29}$$

This metric evaluates whether adaptive security introduces unacceptable delays in cloud communications. Network overhead quantifies the additional control traffic introduced by policy updates and telemetry exchange:

$$O_{\text{net}} = \frac{B_{\text{control}}}{B_{\text{total}}} \text{---30}$$

Lower overhead indicates better scalability and cloud suitability. Policy adaptation time measures how quickly the framework responds to detected threats:

$$T_{\text{adapt}} = t_{\text{policy update}} - t_{\text{anomaly detection}} \text{----31}$$

This metric reflects the responsiveness of adaptive micro segmentation.

## 4. Results and Discussion

This section outlines the results of the experiment carried out using the described cloud testbed in Section V and explains the usefulness of the suggested framework of Zero Trust-supported adaptive micro segmentation. This assessment is based on the aspect of the lateral movement containment, the accuracy of policy enforcement, and system performance overhead against representative baseline security models outlined in table 1. Proposed framework has the smallest LMSR, which minimizes the successful lateral movement attempts by about 58.9 percent as compared to the stationary micro segmentation and 81.4 percent as compared to the conventional perimeter-based security. This has been improved by dynamic tightening of micro-perimeter that is brought about by persistent risk assessment.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

**Table 1 Lateral Movement Success Rate (LMSR)**

| Security Model | Lateral Attempts | Successful Attempts | LMSR |
|---|---|---|---|
| Perimeter-Based Cloud Security | 500 | 312 | 0.624 |
| Static Micro segmentation | 500 | 167 | 0.334 |
| Zero Trust (Access-Only) | 500 | 141 | 0.282 |
| Proposed ZT + Adaptive Micro segmentation | 500 | 58 | 0.116 |

**Table 2 Attack Containment Rate (ACR)**

| Security Model | Compromised Workloads | Reachable Workloads | ACR |
|---|---|---|---|
| Perimeter-Based | 14 | 20 | 0.30 |
| Static Micro segmentation | 7 | 20 | 0.65 |
| Zero Trust (Access-Only) | 6 | 20 | 0.70 |
| Proposed Framework | 2 | 20 | 0.90 |

**Table 3 Policy Violation Rate (PVR)**

| Security Model | Total Requests | Policy Violations | PVR |
|---|---|---|---|
| Perimeter-Based | 10,000 | 982 | 0.098 |
| Static Micro segmentation | 10,000 | 524 | 0.052 |
| Zero Trust (Access-Only) | 10,000 | 471 | 0.047 |
| Proposed Framework | 10,000 | 213 | 0.021 |

**Table 4 Enforcement Latency and Network Overhead**

| Metric | Static Microsegmentation | Proposed Framework |
|---|---|---|
| Avg. Enforcement Latency (ms) | 3.1 | 3.9 |
| Network Control Overhead (%) | 4.2 | 5.1 |
| Policy Adaptation Time (ms) | N/A | 180 |

The suggested solution isolates attack in a highly confined micro-segment with an ACR of 0.90, showing a big decrease in the breach radius. Adaptive segmentation ensures that propagation to other services which are outlined in table 2 is avoided even when workloads are compromised. The decrease in the number of policy violations indicates the efficiency of the ongoing authorization and telemetry-based enforcement. The proposed framework is dynamic and revokes permissions as the risk increases unlike static methods where the permission is repeatedly abused as explained in table 3. Although the suggested framework leads to the fact that the enforcement latency is slightly increased (approximately, 0.8 ms), the overhead is still within reasonable bounds of cloud applications. The extra cost is explained by the high security benefits, especially real time threats containment and adaptive

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

enforcement in the table 4. Figure 2 depicts the success rate of the lateral movement at varying cloud security architectures. The perimeter-based security model has the highest success rate implying that after an attacker has obtained initial access to a system, internal east west traffic is not highly limited. Numerically, even with the lateral movement being very minimized due to work load level isolation through static micro segmentation, this is limited because lateral risk changes are not covered by the policies that are strictly set and therefore do not change. The Zero Trust access-only model also reduces the success rate to the identity-based authentication but does not provide internal traffic isolation. Conversely, the resulting success rate of lateral movement is the lowest in the proposed Zero Trust with adaptive micro segmentation, which proves to be efficient in the dynamically limited inter-workload communication, as well as blocking the propagation of attackers.

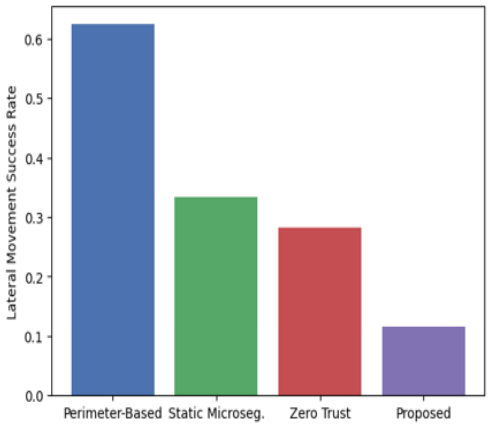


**Figure 1 Lateral Movement Success Rate**

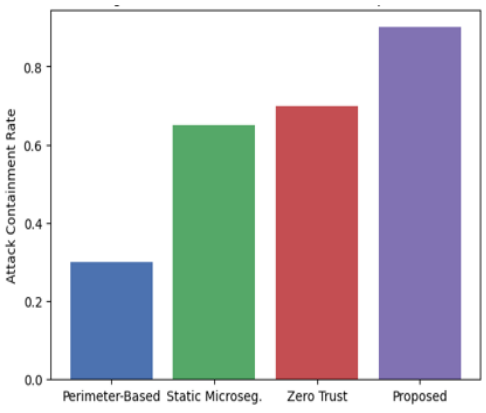


**Figure 2 Attack Containment Rate**

Figure 3 indicates the rate of attack containment, which is the capacity of the framework to restrict the amount of the breach radius following a workload compromise. Perimeter-based security presents low containment and will spread the attack across a variety of workloads. The benefits of Static micro segmentation are that it enhances containment by adding segmentation boundaries to it and is still prone to policy drift [16]. The Zero trust access-only model offers a middle way level of improvements by restricting access privileges but fails to completely stop further propagation. The suggested framework is the most effective one in terms of the highest containment rate, which means that the adaptive micro-perimeters and constant risk-sensitive policy updates contain the attacks to a limited number of workloads.

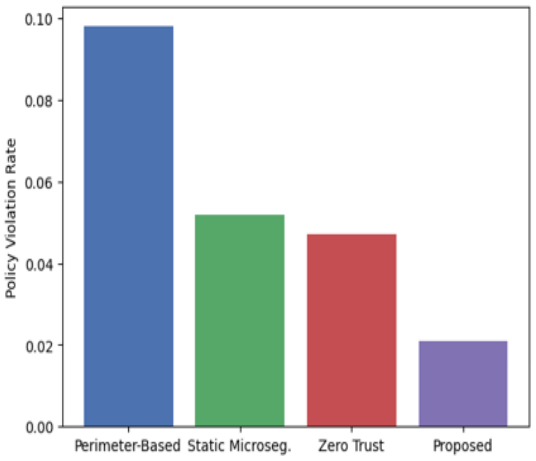


**Figure 4 Policy Violation Rate**

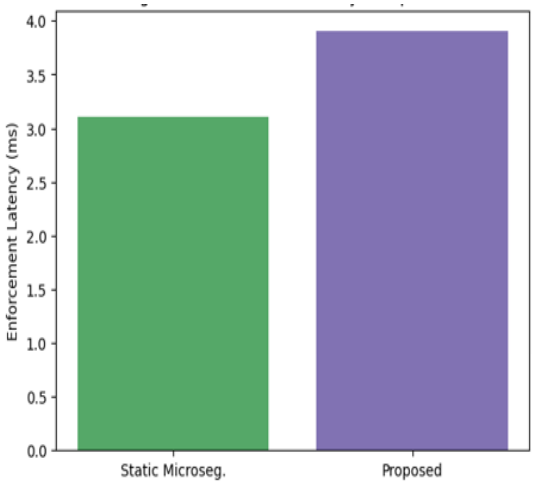


**Figure 5 Enforcement Latency**

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3765-4774
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0495

The levels of policy violation of various security mechanisms are compared in Figure 4. The impossibility of using perimeter-based security to implement fine-grained access control is emphasized by high rates of violation. One of these is the application of Static micro segmentation where violation is mitigated through predefined rules, and access-only through zero trust further enhances compliance with identity verification. The suggested framework has the lowest policy violation rate as it is verified constantly, and real-time analytical of telemetry and dynamic policy enforcement. This finding proves the fact that adaptive Zero Trust implementation is more efficient to prevent repetitive abuses and unauthorized access attempts

Figure 5 compares the enforcement latency that the proposed framework provides with the enforcement latency that is provided by the static micro segmentation. Although the adaptive Zero Trust micro segmentation model has a small increase in the latency because of continuous evaluation of the policy and risk assessment, the improvement is not significant and is within the acceptable limits of cloud computing applications. The benefits in terms of significant improvement in security, especially the prevention of lateral movement and containing breach warrant the marginal overhead, proving the feasibility of the offered solution on the real-life cloud deployment.

## Conclusion

The current paper introduced a flexible Zero Trust-based micro segmentation model to protect the cloud network against the latest attack patterns, especially lateral movement and insider attacks. The proposed solution is based on the combination of identity-based access control and the fine-grained, workload-based micro segmentation to eliminate implicit trust and enforce least-privilege communication within the cloud infrastructure. In contrast to the standard perimeter-based security and fixed segmentation frameworks, the proposed framework is built on the continuous assessment of trust based on real-time telemetry, contextual features and behavioral cues. This allows tightening of the micro-perimeters dynamically and re-enforcement of the policy in real time in the case of an increase in the levels of risks. Adaptive security enforcement can be rigorously and scalable based on the mathematical formulation of policy choices, risk calculation and segmentation control. The experimental outcomes can prove the fact that the suggested framework can significantly decrease the lateral movement success rates, decrease the breach radius, and decrease the rate of the policy violation and introduce only a small penalty of the enforcement latency. These findings support the fact that high security assurances are possible without affecting cloud performance or scalability. The steady positive change in all metrics of evaluation confirms the efficiency of the combination of the principles of Zero Trust and adaptive micro segmentation.

## References

[1]. S. Nalluri, M. M. Malyala, H. Kandagiri, P. C. Jakku and K. K. Kandagiri, "AI-Enhanced Zero Trust Architecture for Cloud Security with Quantum Resilience," 2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2025, pp. 1085-1092, doi: 10.1109/ICICV64824.2025.11085906.

[2]. L. Sharma, A. Dokania, A. Verma, D. P. Shah, P. M. Parekh and S. S. Shinde, "AI-Augmented Security Protocols for Scalable Cloud Infrastructure Management," 2025 International Conference on Engineering, Technology & Management (ICETM), Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051957.

[3]. Joshi, “Emerging Technologies Driving Zero Trust Maturity Across Industries,” in IEEE Open Journal of the Computer Society, vol. 6, pp. 25 - 36, 2025, doi: 10.1109/OJCS.2024.3505056.

[4]. A. Kurulkar, A. S. Gurjar, R. R. Alva and T. B. Jamdar, "Cloud-Based Network Threat Detection Using Deep Learning Models," 2025 2nd International Conference on Computing and Data Science (ICCDS), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICCDS64403.2025.11209603.

[5]. L. P.M, J. J. B and A. J. H. Catherine, "Adaptive Deep Learning Framework for Privilege Escalation Attack Detection and

Mitigation in Cloud Environments," 2025 International Conference on Frontier Technologies and Solutions (ICFTS), Chennai, India, 2025, pp. 1-9, doi: 10.1109/ICFTS62006.2025.11031905.

[6]. L. Zhao, B. Li and H. Yuan, "Cloud Edge Integrated Security Architecture of New Cloud Manufacturing System," in Journal of Systems Engineering and Electronics, vol. 35, no. 5, pp. 1177 - 1189, October 2024, doi: 10.23919/JSEE.2024.000112.

[7]. Y. Liu et al., "Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain," in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 2603 - 2618, July-Aug. 2024, doi: 10.1109/TDSC.2023.3313799.

[8]. M Ehsan, F Masood, G Morteza, et al., "A framework for throughput bottleneck analysis using cloud-based cyber-physical systems in Industry 4. 0 and smart manufacturing ", Procedia Computer Science, vol. 232, pp. 3121 - 3130, 2024.

[9]. P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," in IEEE Access, vol. 11, pp. 19487 - 19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[10]. T. Sasada, M. Kawai, Y. Masuda, Y. Taenaka and Y. Kadobayashi, "Factor Analysis of Learning Motivation Difference on Cybersecurity Training With Zero Trust Architecture," in IEEE Access, vol. 11, pp. 141358 - 141374, 2023, doi: 10.1109/ACCESS.2023.3341093.

[11]. Q. Yu et al., "Cybertwin Based Cloud Native Networks," in Journal of Communications and Information Networks, vol. 8, no. 3, pp. 187 - 202, Sept. 2023, doi: 10.23919/JCIN.2023.10272347.

[12]. X. Zhang, J. Zhao, C. Xu, H. Wang and Y. Zhang, "DOPIV: Post-Quantum Secure Identity-Based Data Outsourcing with Public Integrity Verification in Cloud Storage," in IEEE Transactions on Services Computing, vol. 15, no. 1, pp. 334 - 345, 1 Jan.-Feb. 2022, doi: 10.1109/TSC.2019.2942297.

[13]. J. Jiang, D. Wang and G. Zhang, "QPause: Quantum-Resistant Password-Protected Data Outsourcing for Cloud Storage," in IEEE Transactions on Services Computing, vol. 17, no. 3, pp. 1140 - 1153, May-June 2024, doi: 10.1109/TSC.2023.3331000.

[14]. I. Pedone, A. Atzeni, D. Canavese and A. Lioy, "Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment," in IEEE Access, vol. 9, pp. 115270 - 115291, 2021, doi: 10.1109/ACCESS.2021.3102313.

[15]. B H Li, X D Chai, B C Hou, et al., "Cloud manufacturing system 3.0—a new intelligent manufacturing system in the "Intelligent+" era.", Computer Integrated Manufacturing System, vol. 25, no. 12, pp. 2997 - 3012, 2019.

[16]. B H Li, X D Chai, L Zhang, et al., "Accelerate the development of intelligent manufacturing technologies industries and application under the guidance of a new generation of artistic intelligence technology ", Engineering Sciences, vol. 20, no. 4, pp. 81 - 86, 2018.