www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 06, Issue 01, January 2026, pp : 69-74

e-ISSN : 2583-1062
Impact Factor : 7.001

A MODULAR AND ADAPTIVE CLOUD INFRASTRUCTURE FOR IDENTITY AND ACCESS GOVERNANCE

Bharti Dubey[1], Anamika Singh[2]

[1]Electronics And Communication Engineering, LNCT University, Bhopal, Madhya Pradesh, India.

[2]Computer Science Engineering, LNCT University, Bhopal, Madhya Pradesh, India.

ABSTRACT

Access control mechanisms form the foundational layer of cloud ecosystems, ensuring secure and efficient resource utilization. Over the years, organizational practices have largely centered on role-based paradigms to allocate user entitlements, fostering a sense of familiarity and ease. However, contemporary identity and access management (IAM) solutions in cloud settings continue to grapple with the proliferation of roles, often resulting in unwarranted expansions of user permissions that undermine overall system integrity. Such proliferation not only complicates governance but also exposes infrastructures to heightened vulnerabilities, potentially compromising expansive, globally distributed deployments.

To mitigate these persistent challenges, this study introduces the TRAC framework, an innovative architectural model grounded in principles of modularity and adaptive role orchestration. Departing from conventional static assignments, TRAC evaluates and provisions access predicated on the specific operational imperatives of users—focusing on discrete tasks rather than enduring role classifications. This task-centric orientation, coupled with contextual attribute evaluation, promotes precision in privilege allocation, thereby curtailing excess entitlements and enhancing resilience in dynamic cloud landscapes.

Keywords: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), Temporary Access Provisioning, Adaptive Frameworks.

1. INTRODUCTION

The evolution of cloud computing over recent decades has spurred the development of diverse protocols aimed at safeguarding identity and access within distributed environments. Despite these advancements, the phenomenon of role proliferation—commonly termed "role explosion"—persists as a formidable obstacle, particularly in role-centric systems. This issue arises when ad hoc role creation, driven by transient project needs or personnel shifts, generates a labyrinth of near-duplicate designations. Consequently, delineating precise access mappings becomes elusive, inadvertently bestowing superfluous privileges upon users and eroding the clarity essential for robust governance.

In expansive cloud deployments that underpin mission-critical, large-scale applications across the globe, the ramifications of such disarray are profound. Roles, often tailored to ephemeral initiatives, languish post-completion or upon staff attrition, devoid of systematic oversight regarding their lifecycle. Administrators, under pressure to expedite resolutions, habitually resort to instantiating novel roles or duplicating extant ones with incremental enhancements. While this yields immediate relief, it accrues substantial technical liabilities over time, manifesting as an unwieldy tangle of entitlements that hampers scalability and elevates breach risks.

The TRAC framework, as delineated herein, charts a forward-looking pathway to redress this entrenched dilemma. Eschewing immutable roles, it orchestrates ephemeral assemblies of permissions at execution time, tethered exclusively to the exigencies of the immediate undertaking. Herein, access adjudication pivots upon task execution rather than role affiliation, positioning roles merely as versatile repositories for task aggregations. Augmented by attribute annotations on both users and assets, this schema infuses real-time contextual acuity, enabling judicious, time-delimited access grants that align precisely with operational necessities.

2. LITERATURE REVIEW

This inquiry foregrounds the enduring vulnerability inherent to RBAC-dominant cloud architectures: the unchecked expansion of roles, which imperils the foundational security of IT ecosystems. By synthesizing a constellation of computational paradigms and governance strategies, the proposed framework proffers a sophisticated antidote to this proliferation, modulating cloud behaviors toward greater adaptability and restraint.

A. Research Inquiries

The ensuing queries orient the investigation:

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 06, Issue 01, January 2026, pp : 69-74
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

RQ1: To what extent can RBAC integrate seamlessly within hybrid configurations to bolster its efficacy?

RQ2: Is it feasible to eradicate role proliferation within RBAC architectures through targeted interventions?

RQ3: Might an emergent framework supplant conventional models in addressing these deficiencies?

B. Paper Organization

The inaugural segment interrogates the frailties afflicting RBAC implementations. Succeeding it, the subsequent division elucidates the mechanics of role proliferation and delineates remedial pathways. The tertiary portion surveys an array of methodologies and conceptual tools—encompassing modularity, ephemeral access, adaptive schemas, attribute annotation, and astute policy formulation—illustrating their synergistic potential in ameliorating IAM quandaries. Culminating this discourse, the quaternary section unveils the avant-garde TRAC framework as a comprehensive rejoinder to role surfeit.

Scholarly discourse underscores RBAC's ubiquity, attributable to its inherent simplicity, yet recurrently laments the attendant risks of role engorgement. Proponents advocate for architectural refinements to harness RBAC's virtues more judiciously. Complementary analyses probe role discovery processes, advocating methodical reassessments and reallocations of entitlements vis-à-vis evolving permissions.

Empirical forays reveal the persistent hurdles in deploying multifaceted models, underscoring the imperative for fluid access adjudication to invigorate legacy paradigms. In sector-specific contexts, such as healthcare, where individuals navigate manifold responsibilities, RBAC's granularity proves insufficient, prompting calls for context-infused variants attuned to contemporary cloud intricacies.

Further critiques spotlight RBAC's rigidity amid flux, positing zero-trust infusions and hybrid amalgamations as panaceas for scalability in mutable terrains. These syntheses affirm RBAC's latent prowess when interwoven with nascent technologies.

Dynamic augmentations to RBAC, incorporating trust heuristics and ledger-enabled scalability, evince enhanced authentication and operational throughput, reaffirming RBAC's preeminence in fortified paradigms. Analogously, containerized orchestration and event-responsive policies mitigate latency in permission flux, while decoupled strata foster fault-tolerant elasticity, severing the rigid interlinks plaguing orthodox designs.

Eventual paradigms transcend static edicts, engendering policy genesis responsive to emergent stimuli, thereby optimizing global routing and computational agility. Just-in-time mechanisms, refined for hardware abstraction and runtime optimization, underscore their salience in accommodating cloud's vicissitudes, particularly within under-explored stacks demanding architectural tailoring.

3. METHODOLOGY

Role surfeit constitutes the paramount affliction in RBAC ecosystems, amenable to amelioration via infusions of cloud-native tenets such as intelligent policies, ephemeral entitlements, task-oriented adjudication, modularity, and adaptive dynamism. These infusions transmute RBAC's static essence into a pliant archetype, primed for flux and expansive scaling.

Intelligent policies impose hierarchical gradients, cascading diminished authorities downward to curtail nascent role genesis.

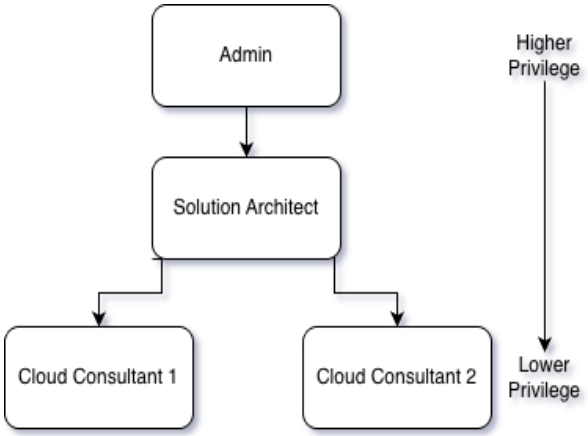

Fig 1: Intelligent Policies

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 06, Issue 01, January 2026, pp : 69-74
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Such policies obviate the proliferation of bespoke designations by externalizing intricate logics into evaluative heuristics that interrogate runtime variables—encompassing temporal constraints, apparatus provenance, identity markers, initiative labels, and vocational mandates. Thus, a singular archetype morphs contextually, obviating myriad niche variants.

Ephemeral access curtails role accrual by provisioning transient entitlements aligned to sporadic imperatives, obviating perpetual allocations for infrequent duties. Upon cessation, these dissipate autonomously, forestalling vestigial designations.

Adaptive models recalibrate entitlements in situ, leveraging metadata strata to refashion core archetypes sans bespoke derivations, insulating against environmental idiosyncrasies.

Modularity in cloud paradigms disentangles identity, entitlements, heuristics, and assets into autonomous echelons, facilitating archetype reuse and asset-specific modulation via discrete directives, thereby insulating against service-specific sprawl.

The proffered schema amalgamates these sinews into a tripartite edifice: a definitional nucleus delineating archetypes, entitlements, and assets; a heuristic nucleus orchestrating granular runtime impositions and task delimitation; and an adjudicative nucleus scrutinizing policies, annotations, and asset compatibilities to authorize or rebuff ingress.

This stratified construct yields performant, efficacious, and extensible cloud governance, mitigating surfeit, excess, and misalignment through runtime heuristics.

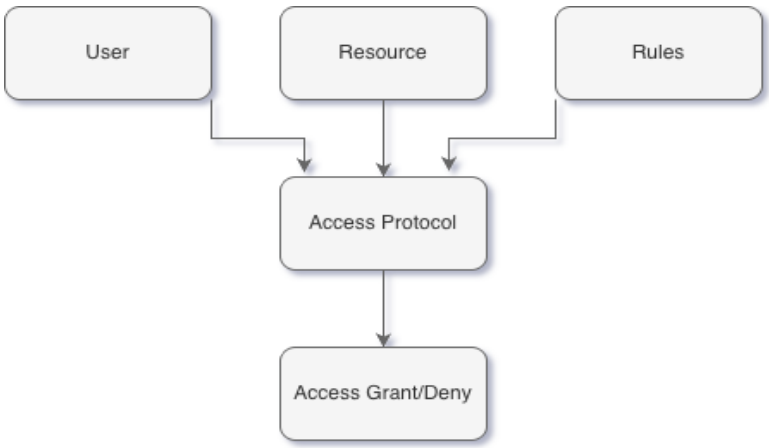

Fig 2: Ephemeral Compilation Mechanism

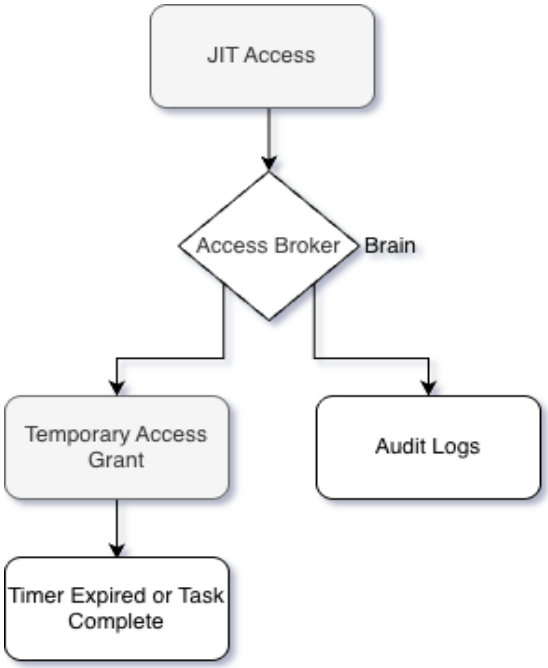

Fig 3: Modular Architecture

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 06, Issue 01, January 2026, pp : 69-74
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

TRAC redresses surfeit by sequentially discerning actor, asset, operation, and milieu; instantiating runtime heuristics; and ratifying ingress per contextual fidelity.

Validation ensues via software engineering canons: architectural congruence, narrative feasibility assays, and antithetical benchmarking.

4. ARCHITECTURAL VERIFICATION

1. Narrative Feasibility: Exemplifying operational viability, consider a reliability engineering operative seeking provisional asset ingress.

Phase 1: Operative (Cohort=Reliability) petitions task-specific ingress.

Phase 2: Intermediary elicits operative annotations, task corpus, and asset descriptors (Initiative=Phoenix).

Phase 3: Heuristic engine assays directives via scaffold-embedded logics.

Phase 4: Affirmation yields delimited credentials.

Phase 5: Ingress lapses upon task fulfillment or temporal exhaustion.

Corollaries: Absence of persistent archetypes; no enduring entitlements; autonomous closure.

2. Antithetical Benchmarking:

Paradigm	Persistent Archetypes	Contextual Acuity	Ephemeral Ingress	Surfeit Hazard
RBAC	Affirmative	Absent	Absent	Elevated
ABAC	Absent	Affirmative	Absent	Moderate
PBAC	Partial	Circumscribed	Affirmative	Moderate
TRAC	Absent	Affirmative	Affirmative	Diminished

Fig 4: Antithetical Scrutiny: TRAC, RBAC, ABAC, PBAC

3. Fortification Rationale:

The adjudicative nexus singularizes heuristic resolution, insulating direct asset ingress. Credentials embody transience, task confinement, and annotation ratification. Stratification sequesters heuristic genesis from resolution, antecedent to contextual harmonization and provisional conferral, engendering authenticity, durability, and dependability.

4. Verification Constraints: Scrutiny encompasses structural congruence, narrative deduction, and benchmarking. Empirical assay lies beyond this purview; forthcoming endeavors shall instantiate TRAC in cloud milieus to quantify throughput, extensibility, and fortification.

5. DISCUSSION

Verification unequivocally attests to TRAC's robustness, integrity, dependability, and extensibility. This avant-garde construct deftly harnesses computational tenets—modularity, ephemeral ingress, intelligent directives, annotations, adaptive schemas, and task primacy—to transcend RBAC's stasis. Unlike RBAC's runtime immutability, TRAC assays dynamically, enforcing graduated minimalism to avert surfeit.

Harmonious with workflow paradigms, TRAC deploys directives as containerized artifacts, with task corpora under repository governance for traceability. The adjudicative nexus privileges integrity over dispatch, infusing pliancy and vigilance.

6. CONCLUSION

This exposition elucidates the TRAC framework, engineered for throughput, extensibility, and fortification within cloud ontologies. It proffers a cogent counter to RBAC's surfeit via modular disentanglement, task-centric ratification, ephemeral provisioning, adaptive flux, and astute directives.

Corroborated through structural, narrative, and antithetical lenses, TRAC evinces seamless assimilation into contemporary cloud and workflow arenas. Stratified constituents revolutionize pliancy, traceability, and runtime vigilance, obviating recalibration and suiting multi-occupant paradigms.

Prospective pursuits shall prototype TRAC amid multi-occupant clouds to appraise throughput, extensibility, and fortification metrics.

7. REFERENCES

[1] Z. Asaf, M. Asad, S. Ahmed, W. Rasheed, and T. Bashir, "Role based access control architectural design issues in large organizations," in 2014 International Conference on Open Source Systems & Technologies, Lahore, Pakistan: IEEE, Dec. 2014, pp. 197–205. doi: 10.1109/ICOSST.2014.7029344.

[2] S. R. Selamat, "117 PUBLICATIONS 1,823 CITATIONS SEE PROFILE," 2017.

[3] M. Uddin, S. Islam, and A. Al-Nemrat, "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control," IEEE Access, vol. 7, pp. 166676–166689, 2019, doi: 10.1109/ACCESS.2019.2947377.

[4] M. A. De Carvalho and P. Bandiera-Paiva, "Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling," in 2017 International Carnahan Conference on Security Technology (ICCST), Madrid: IEEE, Oct. 2017, pp. 1–8. doi: 10.1109/CCST.2017.8167833.

[5] P. Hlushchenko and V. Dudykevych, "Exploratory survey of access control paradigms and policy management engines".

[6] O. Emma and P. Peace, "ROLE-BASED ACCESS CONTROL (RBAC) ENHANCEMENTS FOR BIG DATA".

[7] A. Elliott and S. Knight, "Towards Managed Role Explosion," in Proceedings of the 2015 New Security Paradigms Workshop, Twente Netherlands: ACM, Sept. 2015, pp. 100–111. doi: 10.1145/2841113.2841121.

[8] United States and A. Adeyinka, "Zero Trust Architectures in Multi-Tenant Cloud Platforms: A Role-Based Access Control Reinforcement Framework," Int. J. Innov. Res. Comput. Commun. Eng., vol. 12, no. 05, May 2024, doi: 10.15680/IJIRCCE.2024.1205372.

[9] M. Asim, N. Tariq, A. Ismail Awad, F. Waheed, U. Ullah, and G. Murtaza, "SecT: A Zero-Trust Framework for Secure Remote Access in Next-Generation Industrial Networks," IEEE J. Sel. Areas Commun., vol. 43, no. 6, pp. 2293–2311, June 2025, doi: 10.1109/JSAC.2025.3560015.

[10] P. Habibi and A. Leon-Garcia, "SliceSphere: Agile Service Orchestration and Management Framework for Cloud-Native Application Slices," IEEE Access, vol. 12, pp. 169024–169049, 2024, doi: 10.1109/ACCESS.2024.3492138.

[11] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-Based Secure Multi-Cloud Collaboration Framework in Cloud-Fog-Assisted IoT," IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1546–1561, Apr. 2023, doi: 10.1109/TCC.2022.3147226.

[12] M. Usman, M. S. Sarfraz, M. U. Aftab, U. Habib, and S. Javed, "A Blockchain Based Scalable Domain Access Control Framework for Industrial Internet of Things," IEEE Access, vol. 12, pp. 56554–56570, 2024, doi: 10.1109/ACCESS.2024.3390842.

[13] H. Wang, P. Liu, X. Zhong, F. Luo, B. Xiao, and Y. Yang, "PAC-MC: An Efficient Password-Based Access Control Framework for Time Sequence Aware Media Cloud," IEEE Trans. Mob. Comput., vol. 24, no. 7, pp. 5632–5648, July 2025, doi: 10.1109/TMC.2025.3534861.

[14] B. C. Şenel, M. Mouchet, J. Cappos, T. Friedman, O. Fourmaux, and R. McGeer, "Multitenant Containers as a Service (CaaS) for Clouds and Edge Clouds," IEEE Access, vol. 11, pp. 144574–144601, 2023, doi: 10.1109/ACCESS.2023.3344486.

[15] Z. Ding, Y. Zhou, S. Wang, and C. Jiang, "SCAFE: A Service-Centered Cloud-Native Workflow Engine Architecture," IEEE Trans. Serv. Comput., vol. 16, no. 5, pp. 3682–3695, Sept. 2023, doi: 10.1109/TSC.2023.3259989.

[16] Q. Yang, L. Duan, W. Song, and S. Zhang, "A Service-Based Cloud-Edge Fusion Approach for Abnormality Detection of Power Generation Equipment," IEEE Access, vol. 12, pp. 51556–51569, 2024, doi: 10.1109/ACCESS.2024.3386189.

[17] C. Yan and S. Sheng, "Sdn+K8s Routing Optimization Strategy in 5G Cloud Edge Collaboration Scenario," IEEE Access, vol. 11, pp. 8397–8406, 2023, doi: 10.1109/ACCESS.2023.3237201.

[18] P. Zhang, Y. Liu, and M. Qiu, "SNC: A Cloud Service Platform for Symbolic-Numeric Computation Using Just-In-Time Compilation," IEEE Trans. Cloud Comput., vol. 7, no. 2, pp. 580–592, Apr. 2019, doi: 10.1109/TCC.2017.2656088.

[19] S. Ma, D. Andrews, S. Gao, and J. Cummins, "Breeze computing: A just in time (JIT) approach for virtualizing FPGAs in the cloud," in 2016 International Conference on ReConFigurable Computing and FPGAs (ReConFig), Cancun, Mexico: IEEE, Nov. 2016, pp. 1–6. doi: 10.1109/ReConFig.2016.7857159.

[20] S. S. Ponangi, G. W. Dueck, K. B. Kent, D. Maier, and K. Konno, "Java Runtime Optimization for Copying Arrays on AArch64," in 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro: IEEE, June 2023, pp. 1–6. doi: 10.1109/MECO58584.2023.10155064.

[21] A. Deshmukh, R. Li, R. Sen, R. R. Henry, M. Beckwith, and G. Gupta, "Performance Characterization of .NET Benchmarks," in 2021 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Stony Brook, NY, USA: IEEE, Mar. 2021, pp. 107–117. doi: 10.1109/ISPASS51385.2021.00028.

[22] V. Tsakanikas and T. Dagiuklas, "A Generic Framework for Deploying Video Analytic Services on the Edge," IEEE Trans. Cloud Comput., vol. 11, no. 3, pp. 2614–2630, July 2023, doi: 10.1109/TCC.2022.3218813.

[23] G. Fragkos, J. Johnson, and E. E. Tsiropoulou, "Dynamic Role-Based Access Control Policy for Smart Grid Applications: An Offline Deep Reinforcement Learning Approach," IEEE Trans. Hum.-Mach. Syst., vol. 52, no. 4, pp. 761–773, Aug. 2022, doi: 10.1109/THMS.2022.3163185.

[24] J. Gupta, K. Kant, and A. Abouelwafa, "FussyCache: A Caching Mechanism for Emerging Storage Hierarchies," in 2020 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Bangkok, Thailand: IEEE, Dec. 2020, pp. 74–81. doi: 10.1109/CloudCom49646.2020.00010.

[25] H. Deng, S. Chen, X. Zhu, B. Jiang, K. Jing, and L. Wang, "EP-Net: Improving Point Cloud Learning Efficiency Through Feature Decoupling," IEEE Trans. Instrum. Meas., vol. 73, pp. 1–14, 2024, doi: 10.1109/TIM.2024.3451587.

[26] F. Luo, H. Wang, X. Yan, and J. Wu, "Key-Policy Attribute-Based Encryption With Switchable Attributes for Fine-Grained Access Control of Encrypted Data," IEEE Trans. Inf. Forensics Secur., vol. 19, pp. 7245–7258, 2024, doi: 10.1109/TIFS.2024.3432279.

[27] S. T. Alshammari, K. Alsubhi, H. M. A. Aljahdali, and A. M. Alghamdi, "Trust Management Systems in Cloud Services Environment: Taxonomy of Reputation Attacks and Defense Mechanisms," IEEE Access, vol. 9, pp. 161488–161506, 2021, doi: 10.1109/ACCESS.2021.3132580.

[28] Z. Fan, C. Yuan, X. Si, and S. Yuan, "Enhancing Security in Cloud Computing: A Comprehensive Analysis of a Zero-Trust Dynamic Access Control Architecture with Integrated Multifactor Authentication," in 2023 3rd International Conference on Networking Systems of AI (INSAI), Xi'an, China: IEEE, Nov. 2023, pp. 275–285. doi: 10.1109/INSAI60116.2023.00057.

[29] L. Fen and L. Quan, "Digital right management based on cloud computing and dynamic secure permission," in 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), Xianning, China: IEEE, Apr. 2011, pp. 3091–3094. doi: 10.1109/CECNET.2011.5768311.

[30] E. Chen, Y. Zhu, K. Liang, and H. Yin, "Secure Remote Cloud File Sharing With Attribute-Based Access Control and Performance Optimization," IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 579–594, Jan. 2023, doi: 10.1109/TCC.2021.3104323.

[31] R. Andreoli et al., "A Multi-Domain Survey on Time-Criticality in Cloud Computing," IEEE Trans. Serv. Comput., vol. 18, no. 2, pp. 1152–1170, Mar. 2025, doi: 10.1109/TSC.2025.3539197.