Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 01 | Jan-2026
ISSN (O) 3107-6696

Fortifying Cloud Ecosystems: A Comparative Evaluation of Access Control Models through the Principle of Least Privilege

[1]Vikas Dubey, [2]Divyarth Rai

Computer Science Engineering, LNCT Univeristy Bhopal, Madhya Pradesh

[1]vikasdubey.it@gmail.com, [2]divyarthrai@gmail.com

Abstract - The proliferation of cloud computing infrastructures has compelled organizations to adopt distributed architectures for the storage, processing, and dissemination of sensitive information. Although these platforms deliver unparalleled scalability and adaptability, they concurrently engender intricate security vulnerabilities, most notably in the domains of authorization and access governance. Central to mitigating these risks is the Principle of Least Privilege (PoLP), a cornerstone security doctrine that prescribes granting entities solely the essential permissions requisite for their designated functions, thereby curtailing the expanse of potential breaches stemming from credential compromise.

This investigation undertakes a rigorous examination of prevailing cloud authorization paradigms, appraised through the prism of parsimonious security imperatives. It scrutinizes the efficacy with which extant models uphold PoLP stipulations within multifaceted, multi-tenant cloud ecosystems. Conventional methodologies—encompassing Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC)—undergo methodical appraisal, juxtaposed against nascent frameworks such as relational, risk-responsive, credence-oriented, and situational authorization constructs.

Employing a systematic synthesis of contemporaneous scholarship augmented by analytical juxtappositions and substantiated via pragmatic access governance corpora, this inquiry elucidates the intrinsic merits, pragmatic constraints, and latent vectors for privilege amplification inherent to each paradigm. The emergent insights reveal that, notwithstanding the contextual acuity afforded by sophisticated models, RBAC manifests superior fidelity in delineating circumscribed privilege allocations, contingent upon meticulously articulated role delineations. In summation, the discourse endorses an integrative or stratified authorization schema, amalgamating RBAC's prognostic reliability with the plasticity of attribute- and context-infused modalities, thereby charting a judicious trajectory for fortifying resilient cloud security paradigms.

Keywords: Principle of Least Privilege, Cloud Security, Access Control Paradigms, RBAC, ABAC, PBAC

I. Introduction

The advent of cloud computing has profoundly reconfigured the architecture of contemporary information ecosystems, facilitating instantaneous procurement of communal computational assets irrespective of geospatial constraints. Enterprises have enthusiastically embraced these services to underpin expansive applications, facilitate dispersed collaborative endeavors, and accommodate mutable computational burdens. Nonetheless, this paradigm shift has exacerbated apprehensions pertaining to surreptitious ingress, aberrant privilege utilization, and inadvertent data divulgation, particularly within milieus characterized by heterogeneous stakeholder interactions over communal reservoirs.

Fundamentally, the exigency of secure cloud assimilation pivots upon the judicious modulation of resource accessibility: delineating permissible interactions between actors and assets under circumscribed predicates. A solitary errant configuration in access stipulations may precipitate the exposition of proprietary repositories, rendering authorization lapses a predominant etiology of cloud-centric security infractions. To obviate such perils, practitioners invariably invoke the Principle of Least Privilege, positing that entitlements—whether for personnel or subsystems—ought to be calibrated precisely to operational imperatives, eschewing superfluous latitude.

Not with standing its doctrinal perspicuity, operationalizing PoLP amid the vicissitudes of cloud terrains proves arduous. These environments contend with disparate task profiles, protean occupational designations, and instantaneous solicitation imperatives, collectively impugning the robustness of inflexible authorization architectures. In response, a panoply of access control apparatuses has proliferated, each endeavoring to harmonize imperatives of fortification, malleability, and administrative parsimony.

The present inquiry interrogates the congruence of emergent cloud access control architectures with PoLP tenets. Through a

contrapuntal assay of archetypal and avant-garde authorization schemas, it endeavors to discern actionable methodologies for excising supererogatory entitlements sans impeding efficacious operations. Furthermore, it probes the prospective saliency of syncretic stratagems in ameliorating the deficiencies of unitary models, thereby augmenting congruence with the protean exigencies of cloud ontologies.

A. Research Questions

This inquiry is steered by the ensuing interrogatives:

RQ1: In what manner may cloud fortifications be sustained amid profoundly peripatetic and decentralized computational matrices?

RQ2: Which apparatuses guarantee the perennial conferral of circumscribed entitlements commensurate with occupational designations?

RQ3: Among antecedent access control schemas, which evinces the most steadfast adherence to the Principle of Least Privilege within cloud substrates?

B. Paper Structure

Succeeding sections proceed thusly: Section II surveys antecedent erudition on cloud access governance and its consonance with least-privilege axioms. Section III delineates the investigative praxis and evidentiary substrates. Section IV proffers contrapuntal outcomes across salient authorization schemas. Section V expounds interpretive ramifications, whilst Section VI consummates with prescriptive insights and prospective scholarly vectors.

II. Literature Review

Scholarship has copiously underscored access governance as the linchpin of cloud fortifications, attributing a preponderance of data effusions to authorization anomalies. Primordial frameworks predominantly orbited role-centric axioms, emulating ossified institutional stratifications. Whilst efficacious in sedentary corporate precincts, these constructs faltered amid the ebullience and contextual density of cloud ontologies.

Role-Based Access Control (RBAC) has endured as a predilect modality, lauded for its administrative lucidity and supervisory coherence. By yoking entitlements to occupational archetypes rather than nominative identifiers, RBAC attenuates policy intricacy and buttresses centralized stewardship. Yet, empirical exegeses recurrently bespeak its lacunae in exigencies demanding granular, temporally attuned adjudications, engendering role engorgement or inadvertent surfeit of entitlements.

To redress these inadequacies, Attribute-Based Access Control (ABAC) emerged, predicated upon evaluative syntheses of actorial, artifactual, operational, and ambient predicates. ABAC proffers augmented pliancy and propels instantaneous authorization, albeit at the exaction of policy labyrinths and augmented calculatory impositions. Orchestrating voluminous predicate ensembles and reconciling normative dissonances persist as recalcitrant conundrums.

Extending these precepts, savants have propounded relational, credence-centric, and peril-adaptive schemas that interweave interpersonal ligatures, historicity of comportment, or stochastic hazard appraisals into adjudicative calculus. Such augmentations enrich situational perspicacity, yet hinge upon nebulous credence quanta or perpetual surveillance, precipitating erosions in systemic alacrity and enforcement opacity.

Contemporaneous evolutions incorporate distributed ledgers, inductive inference apparatuses, and hermeneutic intent elucidation to enhance traceability, verifiability, and adaptiveness. Whilst auspicious, these infusions beget architectural prolixity and remain peripheral to operational cloud deployments. Cumulatively, the corpus intimates that no singular schema consummately fulfills PoLP mandates across cloud variegations, thereby impelling syncretic and discriminative appraisals.

III. Methodology

A. Evidentiary Corpus

The empirical exegesis herein deploys a publicly accessible cloud authorization compendium curated by Mainik Choudhary, encompassing circa 100,000 instantiations across 50 descriptors. This corpus encapsulates veridical authorization vignettes within networked cloud architectures, furnishing a credible substratum for assaying entitlement apportionments across actor typologies—encompassing transients, nominal operatives, supervisory cadres, and paramount overseers.

Salient descriptors encompass authorization archetypes, occupational alignments, ingress gradations, informational criticality, and circumstantial determinants modulating affirmative/negative adjudications.

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 01 | Jan-2026
ISSN (O) 3107-6696

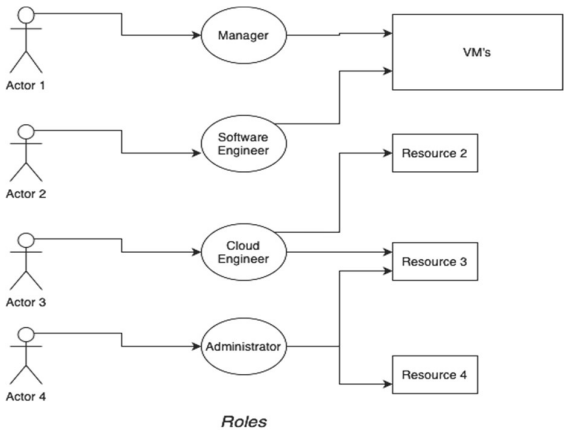

Fig 1. Role-Based Access Control

RBAC predominates in ubiquity, apportioning entitlements to predefined occupational matrices rather than individuated actors. Operatives accede to competencies via associative linkages to role taxonomies reflective of vocational mandates—exemplars including supervisory, directorial, or provisional designations. This modality attenuates administrative onus, consolidates oversight, and resonates with hierarchical institutional morphologies, excelling in equilibrated enterprise contexts.

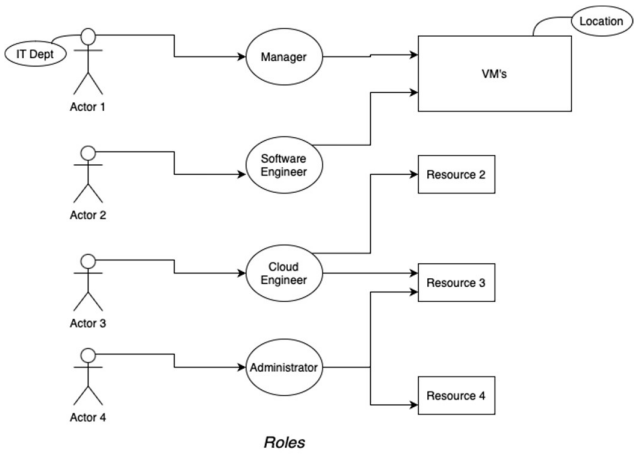

Fig 2. Attribute-Based Access Control

RBAC intrinsically buttresses PoLP by confining entitlements to vocational requisites; however, its inelasticity constrains applicability in volatile cloud matrices wherein imperatives transmute expeditiously. Conversely, ABAC adjudicates ingress via predicate scrutiny encompassing actorial, resourcial, actional, and contextual attributes. Descriptors such as affiliation, locus, apparatus typology, or temporal incidence facilitate discriminatory and temporally attuned authorizations, rendering ABAC propitious for labile, dispersed apparatuses. Reciprocally, this sophistication exacts exigencies in formulation, husbandry, and execution, potentially inflating latency and configurative susceptibilities at expanse.

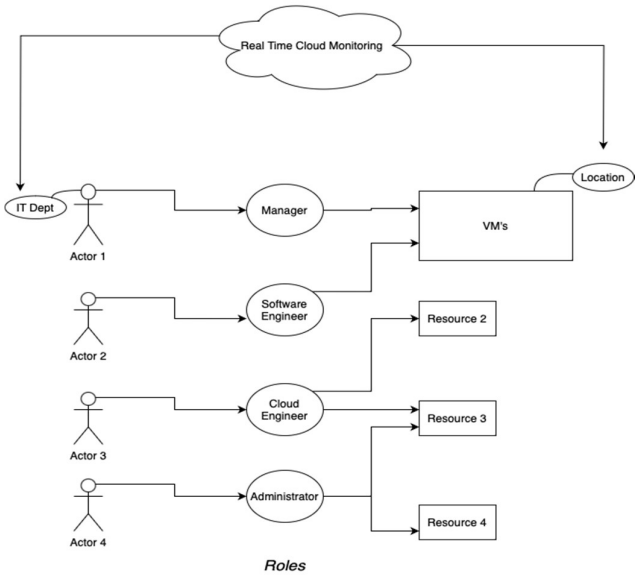

Fig 3. Policy-Based Access Control

PBAC extrapolates predicate-oriented tenets by operationalizing adjudications through codified normative edicts delineating concessional/repudiative predicates. Integrating circumstantial, behavioral, and ambient facets, PBAC accommodates instantaneous and adaptive governance. Congruent with indigenous cloud security ontologies, its potency pivots upon normative precision and iteration; expansive implementations hazard normative antagonisms, administrative encumbrance, and deliberative retardations.

B. Framework

The scrutiny accentuates the fidelity of PoLP conformance across variegated ingress scenarios, with particular heed to entitlement dispersions by occupational stratum, expositions to critical repositories, and invocations of ancillary safeguards such as bifurcated authentication and archival instrumentation.

IV. Outcomes

Contrapuntal assays evince discrete performative idiosyncrasies among RBAC, ABAC, and PBAC instantiations. RBAC manifests unwavering confinement of entitlements, preeminently for subaltern strata such as transients and basal operatives. Entitlements cohere indissolubly to archetypal delineations, attenuating probabilistic escalations.

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 01 | Jan-2026
ISSN (O) 3107-6696

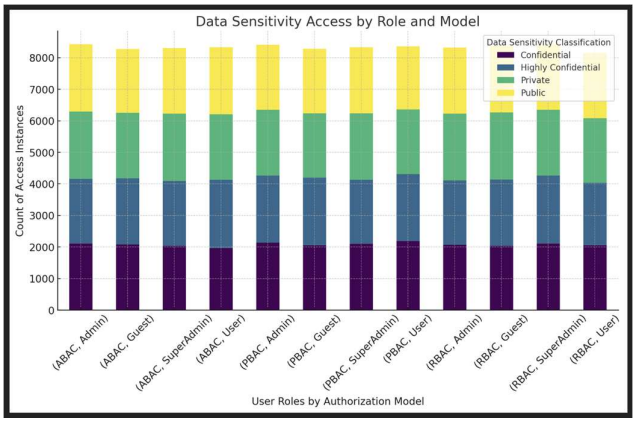

Fig 4. PoLP Conformance Across RBAC, ABAC, PBAC

ABAC, albeit prodigiously malleable, manifests oscillations in entitlement allocations attributable to predicate convolutions. Sundry configurations precipitate unintended expansiveness, particularly amid predicate superpositions. PBAC infuses normative pliancy and archival augmentation, notably via ledger-infused integrations; nonetheless, its predicate-intensive deliberations exacerbate stewardship impositions and executory retardations. ABAC's pliancy, whilst pronounced, engenders lability in allocations consequent to attribute interlacings; miscalibrations recurrently yield profligate ingress, acutely for actors with predicate convergences. PBAC's normative propulsion augments auditability, inter alia through blockchain adjuncts, yet predicates exhaustive normative scrutiny, inflating administrative and chronometric burdens.

Graphical renditions—encompassing columnar depictions and thermal cartographies—attest RBAC's perspicuous demarcation of public and sequestered data ingress. Subaltern archetypes under RBAC evince circumscribed vulnerabilites to confidential assets, consonant with PoLP expectancies. Reciprocally, ABAC and PBAC sporadically confer augmented entitlements to non-supervisory actors, intimating latent security exposures.

V. Result

The adduced outcomes corroborate RBAC's preeminence in aggregate PoLP conformance among scrutinized schemas. Its prognostic constancy and archetypal circumscription streamline entitlement husbandry and attenuate inadvertent ingress trajectories. These corollaries resonate with antecedent erudition extolling RBAC's salience in equilibrated hierarchical milieus.

Comparison	T-Statistic	P-Value	Significance	Conclusion
RBAC vs ABAC	25.43	5.06E-15	Significant	RBAC enforces PoLP much better than ABAC. ABAC tends to over-assign privileges.
RBAC vs PBAC	14.14	3.44E-11	Significant	RBAC is stricter than PBAC, making it more aligned with PoLP. PBAC is more flexible but slightly less restrictive.
ABAC vs PBAC	-13.02	2.66E-10	Significant	PBAC performs better than ABAC but is still less strict than RBAC. ABAC allows more excessive permissions.

Fig 6. T-Test Contraposition

Notwithstanding, RBAC's rigidity circumscribes its aptness for tumultuous cloud onuses. Occupational vicissitudes and emergent imperatives may precipitate stewardship onus or retardant recalibrations. ABAC and PBAC, contrariwise, proffer amplified adaptiveness, albeit necessitating scrupulous normative artisanship to forestall entitlement prodigality.

The corollaries intimate the prospective efficacy of syncretic authorization ontologies—fusing RBAC's architectonic perspicuity with ABAC's contextual acuity—in equilibrating imperatives. Such integrations perpetuate PoLP assurances whilst accommodating instantaneous onuses.

VI. Conclusion

This treatise furnishes an exhaustive appraisal of cloud access governance apparatuses through the lens of PoLP-centric parsimony. Via contrapuntal scrutiny of RBAC, ABAC, and PBAC schemas, it substantiates RBAC's perspicuous enforcement of constricted entitlement perimeters, saliently for subaltern actors.

Whilst progressive schemas infuse contextual perspicacity and normative adaptiveness, they concomitantly amplify intricacy and configurative perils. RBAC endures as a steadfast substratum for PoLP instantiation, preeminently in enterprise contexts with delineated occupational taxonomies.

Prospective inquiries ought to interrogate automated and inferential occupational husbandry, alongside syncretic frameworks interweaving contextual acuity sans forfeiting architectonic simplicity. Such advancements are indispensable for perpetuating robust governance amid the inexorable dynamism of cloud ecologies.

References:

1. M. Ghafoorian, D. Abbasinezhad-Mood, and H. Shakeri, “A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud,” IEEE Transac-

tions on Parallel and Distributed Systems, vol. 30, no. 4, pp. 778–788, Apr2019.

2. A. Bozorgi, M. Jadidi, and J. Anderson, "UPSS: A Global, Least- Privileged Storage System with Stronger Security and Better Performance:," in Proceedings of the 10th International Conference on Information Systems-Security and Privacy. Rome, Italy: SCITEPRESS - Science and Technology Publications, 2024, pp. 660–671.

3. A. U. R. Butt, T. Mahmood, T. Saba, S. A. O. Bahaj, F. S. Alamri,M. W. Iqbal, and A. R. Khan, "An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment,"IEEEAccess, vol. 11, pp. 138 813–138 826, 2023.

4. "An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment," IEEE Access, vol. 11, pp. 138 813–138 826,2023.

5. P. Gill, W. Dietl, and M. V. Tripunitara, "Least-Privilege Calls to Amazon Web-Services," IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2022.

6. S. Long and L. Yan, "RACAC: An Approach toward RBAC and ABAC Combining Access Control," in 2019 IEEE 5th International Conference on Computer and Communications (ICCC). Chengdu, China: IEEE, Dec. 2019, pp.1609–1616.

7. S. Alayda, Najad.A. Almowaysher, M. Humayun, and N. Jhanjhi, "A Novel Hybrid Approach for Access Control in Cloud Computing," International Journal of Engineering Research and Technology, vol.13,no.11,p. 3404, Nov. 2020.

8. L. Cao, L. Meng, D. Stefan, and E. Fernandes,"Stateful Least Privilege Authorization for the Cloud."

9. R. El Sibai, N. Gemayel, J.Bou Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 2, p.e3720, Feb. 2020.

10. W. Wu and W.-c. Feng, "Game to Dethrone: A Least Privilege CTF," in 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud). Newark, NJ, USA: IEEE, Nov. 2021, pp.132–137.

11. C. Perducat, D. C. Mazur, W. Mukai, S. N. Sandler, M. J. Anthony, and J. A. Mills, "Evolution and Trends of Cloud on Industrial OT Networks," IEEE Open Journal of Industry Applications, vol. 4, pp. 291–303, 2023.

12. I. Dhanapala, S. Bharti, A. McGibney, and S. Rea, "Toward a Performance-Based Trustworthy Edge-Cloud Continuum," IEEE Access, vol. 12, pp. 99 201–99212, 2024.

13. M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles," IEEE Transactions on Industrial Informatics, vol.17, no.6, pp. 4288–4297, Jun. 2021.

14. K. A. Torkura, M. I. H. Sukmana, F.Cheng, and Meinel, "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure," IEEE Access,vol. 8, pp. 123 044–123 060,2020.

15. S. An, T. Eom, J. S. Park, J. B.Hong, A. Nhlabatsi, N. Fetais, K. M. Khan, and D. S. Kim, "CloudSafe: A Tool for an Automated Security Analysis for Cloud Computing," in 2019 18th IEEE International Conference On Trust, Security And Privacy InComputing And Communications/13th IEEE International Conference On Big Data Science And Engineering(TrustCom/BigDataSE). Rotorua, New Zealand: IEEE, Aug. 2019, pp. 602–609.

16. S. Challita, F. Korte, J. Erbel, F. Zalila, J. Grabowski, and P. Merle, "Model-based cloud-resource management with TOSCA and OCCI," Software and Systems Modeling, vol. 20, no. 5, pp. 1609–1631, Oct. 2021.

17. K. Albulayhi, A. Abuhussein,F. Alsubaei, and F. T. Sheldon, "Fine-Grained Access Control in the Era of Cloud Computing: An Analytical Review," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas,NV, USA: IEEE, Jan. 2020, pp. 0748–0755.

18. S. T. Alshammari, M. Al-Razgan, T. Alfakih, and K. A. AlGhamdi, "Building a Comprehensive Trust-Evaluation Model to Secure Cloud Services From Reputation Attacks," IEEE Access, vol. 12, pp. 150 754–150 775, 2024.

19. N. Mundbrod and M. Reichert, "Object-Specific Role-Based Access Control,"International Journal of Cooperative Information Systems, vol. 28, no. 01, p. 1950003, Mar. 2019.

20. B. S, N. K. Pathi, S. Abhi, and R. Agarwal, "AccessFlex: Flexible Attribute Based Access Control Scheme for Sharing Access Privileges in Cloud Storage," in 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET. Sydney, Australia:IEEE, Jul. 2024, pp. 1–6.

21. P. Gill, "Least-Privilege Identity-Based Policies for Lambda Functions in Amazon Web Services (AWS)."

22. C. Liu, X. Li, M. Sun, Y. Gao, J. Yuan, and S. Duan, "Bi-TCCS : Trustworthy Cloud Collaboration Service Scheme Based on Bilateral-Social Feedback," IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1021–1037, Apr. 2022.

23. Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A Semi-Centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," IEEE Transactions on Services Computing,vol. 16, no. 2, pp. 858–871, Mar. 2023.

24. J. Aruna Jasmine, V. Nisha Jenipher, J. S. Richard Jimreeves, K. Ravindran, and D. Dhinakaran, "A traceability set up using Digitalization of Data and Accessibility," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). Thoothukudi,India: IEEE, Dec. 2020, pp. 907–910.

25. L. Zhou, C. Su, Z. Li, Z. Liu, and G. P. Hancke, "Automatic fine-grained access control in SCADA by machine learning," Future Generation Computer Systems, vol. 93,

26. pp. 548–559, Apr. 2019.

27. W. Wu and W.-c. Feng, "Game to Dethrone:A Least Privilege CTF," in 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud). Newark, NJ, USA: IEEE, Nov. 2021, pp. 132–137.

28. P. Zhang, M. Zhou, and Y. Kong, "A Double-Blind Anonymous Evaluation-Based Trust Model in Cloud Computing Environments," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 3, pp. 1805–1816, Mar. 2021.

29. T. Sasada, M. Kawai, Y. Masuda, Y. Taenaka, and Y. Kadobayashi, "Factor Analysis of Learning Motiva- tion Difference on Cybersecurity Training With Zero Trust Architecture," IEEE Access, vol.11, pp. 141 358 31. 141 374, 2023.

30. M. I. Sukmana, K. A. Torkura, H.Graupner, F. Cheng, and C. Meinel, "Unified Cloud Access Control Model for Cloud Storage Broker," in 2019 International Conference on Information Networking (ICOIN). KualaLumpur, Malaysia: IEEE, Jan. 2019, pp. 60–65

31. M. W.Sanders and C. Yue, "Minimizing Privilege Assignment Errors in Cloud Services," in Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. Tempe AZ USA:ACM, Mar.2018, pp. 2–12.