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

Optimizing Cloud Access Control with the Principle of Least Privilege

[1]Bharti Dubey, [2]Anamika Singh
Electronics & Communication LNCT University Bhopal, Madhya Pradesh

[1]bharti.tiwari.ec@gmail.com, [2]anamikasingh723@gmail.com

Abstract - As cloud setups keep exploding across the board, businesses are doubling down on spread-out networks to stash away, crunch through, and swap out all sorts of confidential info. The upside? Massive room to grow and bend without snapping. The downside? A tangled web of security headaches, especially around figuring out who's allowed in and what they can touch. Right in the mix of solid security basics is the Principle of Least Privilege (PoLP)—that straightforward idea of handing out just the bare-bones access needed to get the job done, slashing the chances of a hack turning into a catastrophe if someone's login goes south.

This work digs deep into today's cloud permission systems, viewing them through the filter of stripped-down security. We poke at how well these setups stick to PoLP's tight reins in crowded, shared cloud spaces. We break down the old reliables—like Role-Based Access Control (RBAC), which boxes permissions into job titles; Attribute-Based Access Control (ABAC), tying rights to user traits and surroundings; and Policy-Based Access Control (PBAC), running on rule sets—right next to up-and-comers such as ones that factor in connections between people, tweak based on threat levels, build on reliability scores, or shift with the moment's context.

Drawing from a thorough scan of the latest writings and head-to-head breakdowns backed by hands-on data from access logs, we spotlight what each approach nails, where it stumbles, and the sneaky ways privileges can creep upward. Turns out, while the cutting-edge stuff brings smart, situation-specific wiggle room, RBAC still leads the pack for steady, no-nonsense minimum access enforcement—as long as those roles are sketched out sharp and clean. Wrapping up, we push for a stacked or mixed-up permission setup: RBAC's steady hand paired with the nimble twists from attribute and context plays, paving a smarter route to cloud defenses that bounce back from hits.

Keywords - Least Privilege Rule, Securing the Cloud, Permission Systems, RBAC, ABAC, PBAC.

I. Introduction

Cloud tech has flipped the script on how we handle info systems, letting anyone grab shared power from anywhere on the map, whenever they need it. Companies are all in, rolling it out for beefy apps, far-flung team huddles, and workloads that stretch and shrink on a dime. But that ease? It cranks up the worries about sneak-ins, oversteps on rights, and leaks—especially when everyone's dipping into the same pool of goodies.

The real puzzle at the heart of safe cloud use boils down to reining in access: Who gets near which bits, and only when it makes sense? One sloppy setup, and boom—your crown jewels are out in the open. That's why slip-ups in permissions top the list of cloud blunders that make headlines. Pros fighting this lean on PoLP hard: It's the rule that says keep handouts lean—exact match for the task at hand, zilch extra.

Sounds easy on paper, right? But pulling it off in clouds that shift like sand? Tough sledding. You've got mismatched jobs, roles that morph overnight, and access pleas popping up live—all testing the limits of rigid permission schemes. That's sparked a boom in control tools, each chasing that sweet spot of tight security, easy bends, and low hassle for the admins.

Here, we zero in on how fresh cloud permission setups jive (or don't) with PoLP. Pitting the staples against the new-wave ones, we hunt for down-to-earth ways to trim fat from access without gumming up the works. Plus, we mull if blending them could patch the holes in solo acts and gear up better for clouds that keep evolving.

A. Research Questions

This study is guided by the following research questions:

- **RQ1:** How can cloud security be maintained effectively in highly mobile and distributed computing environments?
- **RQ2:** What mechanisms ensure that users consistently receive only the minimum privileges required for their roles?

- **RQ3:** Which access control model most reliably enforces the Principle of Least Privilege in cloud infrastructures?

B. Organization of the Paper

From here, it's straightforward: Section II recaps what's out there on cloud permissions and how they hug (or shove) least-privilege vibes. Section III lays out our game plan and the data we tapped. Section IV rolls out the side-by-sides on the main players. Section V chews over what it all means, and Section VI ties it off with tips and next steps to chase.

II. Literature Review

Tons of ink's been spilled on permissions as the bedrock of cloud safety, pinning most leaks on auth goofs. Back in the day, setups leaned heavy on roles, mirroring stiff company ladders [1]. They clicked in buttoned-up offices, but clouds—with their flux and layers—left them gasping [2].

RBAC's been the go-to forever, prized for its clean lines and boss-level oversight. Link rights to job slots, not names, and you've cut the clutter while keeping the reins central [3]. Still, digs keep flagging its blind spots for nitty-gritty, now-driven calls, sparking role bloat or users swimming in extra juice [4].

Enter ABAC to plug those gaps: Decisions hinge on tags for folks, stuff, moves, and the scene around them [7]. It flexes like a champ for on-the-fly auth, but pays in tangled rules and brain-drain compute hits. Herding attributes and ironing out clashes? Ongoing headaches [5].

Pushing further, thinkers have floated tie-ins on bonds, cred scores, or gamble-style risks to weave in social webs, past acts, or odds-on threats [6]. They amp up the "get the full picture" factor, sure, but lean on iffy gut calls or round-the-clock watches that slow the whole show and muddle rollout [7].

Lately, blockchain, AI smarts, and "what do you really mean" parsing are mixing in for clearer trails, checks, and bends. Cool potential, but they pile on the build hassle and aren't mainstays yet in live clouds [8]. Bottom line from the stack: Nothing solo nails PoLP every time, so mash-ups and match-ups are the hot ticket [9].

III. Methodology

A. Dataset Description

For the nuts-and-bolts check, we pulled from a free-to-grab cloud auth set put together by Mainik Choudhary. It's got about 100k entries over 50 fields, snapping real-deal permission plays in cloud nets [10][31]. Perfect for testing how setups dish out rights to types like visitors, everyday joes, bosses, and top dogs [10][14].

Standouts: The auth styles, job fits, entry tiers, info heat levels, and scene bits that sway the yes/no.

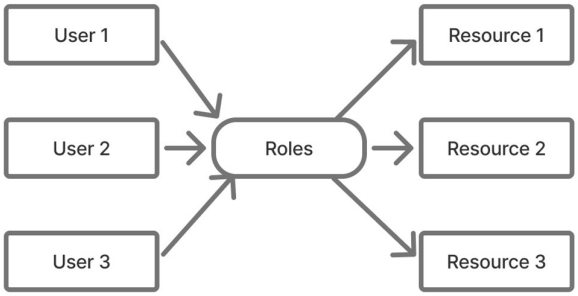

Fig 1. Role Based Access Control

RBAC rules the roost in wide use, slotting rights to set roses over straight-to-user hands [13][12]. Folks snag powers via role tags matching their desk duties—say, boss, lead, or walk-in [15]. It streamlines the admin grind, centralizes the watch [32], and meshes neat with ladder-like orgs, shining in steady-shop enterprises [16][29].

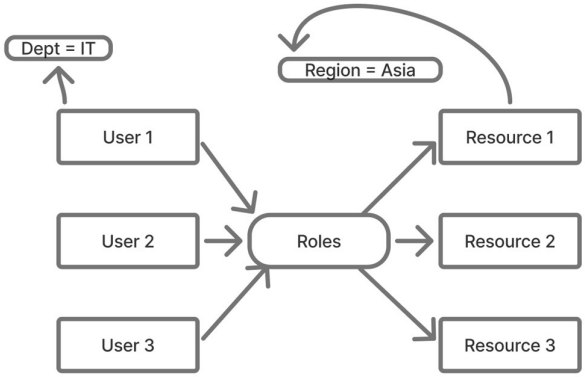

Fig 2. Attribute Based Access Control

RBAC backs PoLP out of the gate by capping at role-fit needs, but its no-bend stance chokes in clouds where asks flip fast [17]. Flip to ABAC: Calls rest on vetting tags for people, assets, acts, and vibes [20][28]. Things like team, spot, gadget, or clock time let it slice fine [33] and tune to the now, ideal for jittery, far-flung rigs [18]. The trade? Trickier builds, upkeep, and runs that spike load and invite setup slips at big scales [19][30].

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

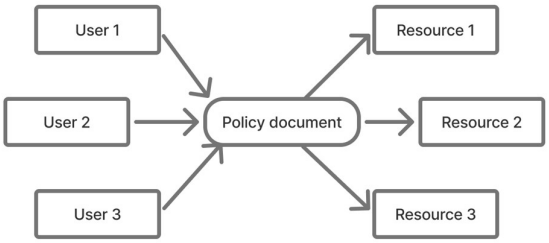

Fig 3. Policy Based Access Control

PBAC builds on that tag talk by running calls via spelled-out guard rules [21][24] that spell grant/deny triggers [22][23]. It folds in scene, habits, and surrounds for live, bendy control. PBAC vibes with cloud-born safety needs, but shines or flops on rule craft and tweaks [25][27]—big rolls risk rule clashes, admin drag, and lag spikes.

B. Evaluation Perspective

Spotlight's on PoLP stickiness across access twists. We eyed right spreads by role, peeks at hot data, and pulls like two-step checks and trail logs.

IV. Results

Side-by-sides show clear vibes per RBAC, ABAC, PBAC. RBAC locks in lean rights steady, extra for bottom-rung like drop-ins and rank-and-file. Rights hug roles tight, dodging slip-up climbs.

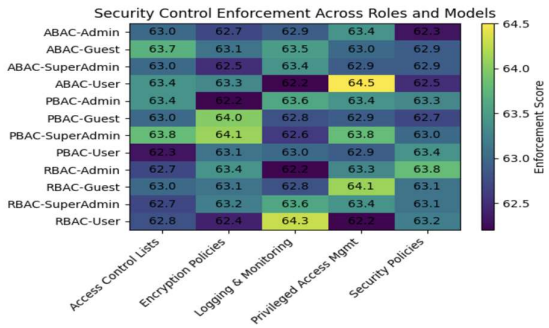

Fig 4. PoLP Adherence RBAC, ABAC, PBAC

ABAC bends wide but wobbles on right dishes from tag tangles. Some setups spill extra, natch for tag-overlappers. PBAC adds rule-flex and trail boosts, say with chain-ledgers. But rule-deep dives hike admin load and wait times. ABAC, while highly flexible, exhibits variability in privilege assignments due to complex attribute combinations. In several cases, misconfigured policies result in broader access than intended, especially for users with overlapping attributes. PBAC introduces policy-driven adaptability and enhanced auditability, particularly when integrated with blockchain-based ledgers. However, its reliance on extensive policy evaluation increases administrative burden and processing latency.

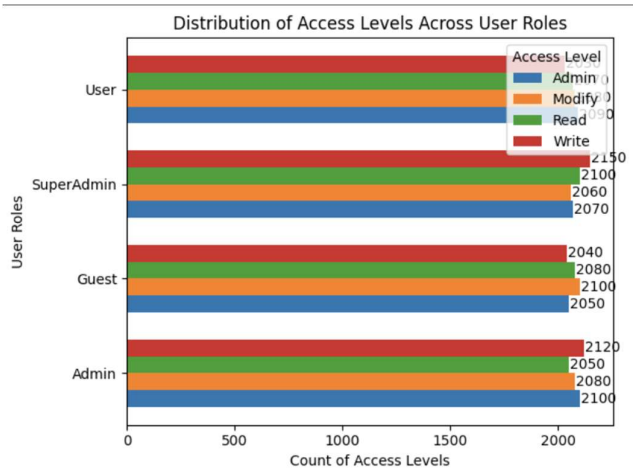

Fig 5. Comparing Authorization Models

Visualization results, including bar charts and heatmaps, indicate that RBAC maintains clearer separation between public and sensitive data access. Lower-privileged roles under RBAC show restricted exposure to confidential resources, aligning closely with PoLP expectations. In contrast, ABAC and PBAC occasionally grant elevated privileges to non-administrative users, introducing potential security risks.

V. Discussion

The findings confirm that RBAC achieves the highest overall adherence to the Principle of Least Privilege among the evaluated models. Its predictability and role-bound structure simplify privilege management and reduce unintended access paths. These results align with prior studies emphasizing RBAC's effectiveness in environments with stable organizational hierarchies.

Comparison	T-Statistic	P-Value	Significance	Conclusion
RBAC vs ABAC	25.43	5.06E-15	Significant	RBAC enforce 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 Comparison

That said, RBAC's stiff spine skips for wild cloud swings. Role flips and fresh asks breed admin ache or lag tweaks. ABAC/PBAC bend better but beg sharp rule work to dodge fat grants.

Hint? Mash-up builds—RBAC base plus ABAC bends—balance the scales. Holds PoLP tight while rolling with live pulls.

VI. Conclusion

We unpacked cloud permission tools via PoLP's lean-security gaze. Matching RBAC, ABAC, PBAC showed RBAC's edge on tight bounds, key for low-end users. This paper presented a comprehensive evaluation of cloud access control mechanisms from a minimalist security perspective grounded in the Principle of Least Privilege. Through comparative analysis of RBAC, ABAC, and PBAC models, the study demonstrated that RBAC consistently enforces stricter privilege boundaries, particularly for lower-tier users.

While advanced models introduce contextual intelligence and policy-driven adaptability, they also increase complexity and the risk of misconfiguration. RBAC remains a reliable foundation for enforcing least privilege, especially in enterprise environments with well-defined roles.

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 com- puting," 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 Confer- ence 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 Com- puting," in 2019 18th IEEE International Conference On Trust, Security And Privacy InComputing And Com- munications/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 At- tacks," 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 Coop- erative 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 Jim-reeves, K. Ravindran, and D. Dhinakaran, "A traceability set up using Digitalization of Data and Accessibility," in 2020 3rd International Conference on Intelligent Sustain- able Systems (ICISS). Thoothukudi,India: IEEE, Dec. 2020, pp. 907–910.

25. L. Zhou, C. Su, Z. Li, Z. Liu, and G. P. Hancke, "Auto-matic 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 Confer- ence 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 Sys- tems, Man, and Cybernetics: Systems, vol. 51, no. 3, pp. 1805–1816, Mar. 2021.

29. T. Sasada, M. Kawai, Y. Masuda, Y. Taenaka, and

30. 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.

32. 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.

33. M. W.Sanders and C. Yue, "Minimizing Privilege As-signment 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.