Mapping the Cloud: A Mixed-Methods Study of Cloud Security and Privacy Configuration Challenges

Supplementary Material

I. Findings

A. Mapping Cloud Security & Privacy Challenges (RQ 1)

The main paper focuses on prominent combinations (use cases with more than 30,000 posts); this supplementary material provides descriptive mappings for the remaining challenge–use case combinations for completeness.

1) Secure Communication and Encryption:

Use Case 3: Network, Connectivity, and Routing.

In network and connectivity settings, operators struggle to apply encryption when traffic must pass through load balancers, VPN tunnels, and private links. They report issues such as failed TLS handshakes, untrusted certificates, and confusion about which endpoint should terminate SSL in multi-hop paths. These misconfigurations can leave internal traffic unencrypted or break connectivity when security controls are tightened.

Use Case 6: Cloud Automation and CI/CD Pipelines.

In automation and CI/CD pipelines, encryption challenges arise when build agents and deployment scripts need to connect securely to cloud services. Operators must manage certificates, API keys, and secret stores while keeping pipelines reproducible and non-interactive. Small mistakes in how certificates are mounted, how HTTPS is enforced, or how keys are rotated often lead to failing jobs or insecure shortcuts in deployment workflows.

2) Network Configuration and Management:

Use Case 1: Cloud Web/App Development.

For web and app development, network configuration issues often surface when front-end applications cannot reach back-end services. Developers struggle with setting correct ports, security group rules, and load balancer targets so that web traffic can flow while still limiting exposure to the public internet. Misplaced rules or subnet choices often appear as timeouts in the browser or intermittent access to APIs.

Use Case 4: Data and Database Operations.

For data and database operations, posts describe difficulty in placing databases in the right networks and exposing them only to trusted clients. Operators must balance private subnets, VPN links, and IP allowlists so that applications can reach the database without opening it to the wider internet. Common problems include blocked connections from application servers, confusion around which IPs to whitelist, and accidental exposure of management ports.

Use Case 5: Application and Service Deployment and Management.

During application deployment, small mistakes in network setup can prevent services from starting or being reachable. Operators report trouble configuring load balancer listeners, health check paths, and target groups so that new versions receive traffic correctly. They also face challenges when moving services between environments, where different subnets or security groups cause previously working deployments to fail.

Use Case 6: Cloud Automation and CI/CD Pipelines.

In automation and CI/CD pipelines, network issues emerge when build agents and deployment runners cannot reach the resources they need. This includes private container registries, internal APIs, or configuration services that sit inside VPCs or behind firewalls. Misconfigured routing or missing VPC endpoints often result in failing jobs that cannot pull images, fetch configuration, or apply infrastructure updates.

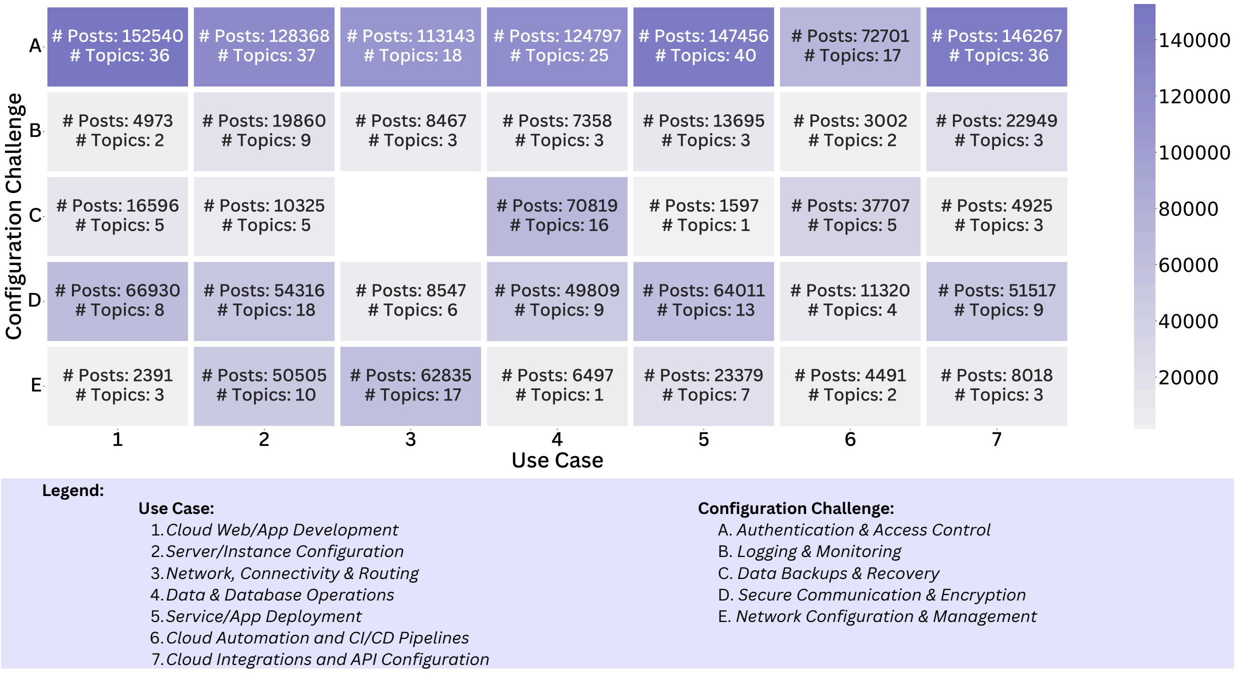
Use Case 7: Cloud Integrations and API Configuration.

For cloud integrations and API configuration, operators must route traffic across services, regions, and sometimes providers. Posts describe difficulties with DNS records, IP-based allowlists, and reverse proxy rules that need to line up on both sides of an integration. When these pieces are misaligned, API calls fail with timeouts or connection errors, even when authentication and application logic are correct.

3) Logging and Monitoring:

Use Case 1: Cloud Web/App Development.

In web and app development, logging problems often appear as missing or incomplete error reports from front-end and back-end services. Developers struggle to capture relevant fields, correlate client-side and server-side events, and surface security-relevant information without overwhelming dashboards. When logs are misconfigured, issues such as failed



Configuration Challenge	1	2	3	4	5	6	7
A	# Posts: 152540 # Topics: 36	# Posts: 128368 # Topics: 37	# Posts: 113143 # Topics: 18	# Posts: 124797 # Topics: 25	# Posts: 147456 # Topics: 40	# Posts: 72701 # Topics: 17	# Posts: 146267 # Topics: 36
B	# Posts: 4973 # Topics: 2	# Posts: 19860 # Topics: 9	# Posts: 8467 # Topics: 3	# Posts: 7358 # Topics: 3	# Posts: 13695 # Topics: 3	# Posts: 3002 # Topics: 2	# Posts: 22949 # Topics: 3
C	# Posts: 16596 # Topics: 5	# Posts: 10325 # Topics: 5		# Posts: 70819 # Topics: 16	# Posts: 1597 # Topics: 1	# Posts: 37707 # Topics: 5	# Posts: 4925 # Topics: 3
D	# Posts: 66930 # Topics: 8	# Posts: 54316 # Topics: 18	# Posts: 8547 # Topics: 6	# Posts: 49809 # Topics: 9	# Posts: 64011 # Topics: 13	# Posts: 11320 # Topics: 4	# Posts: 51517 # Topics: 9
E	# Posts: 2391 # Topics: 3	# Posts: 50505 # Topics: 10	# Posts: 62835 # Topics: 17	# Posts: 6497 # Topics: 1	# Posts: 23379 # Topics: 7	# Posts: 4491 # Topics: 2	# Posts: 8018 # Topics: 3

Legend:

Use Case:

1. *Cloud Web/App Development*
2. *Server/Instance Configuration*
3. *Network, Connectivity & Routing*
4. *Data & Database Operations*
5. *Service/App Deployment*
6. *Cloud Automation and CI/CD Pipelines*
7. *Cloud Integrations and API Configuration*

Configuration Challenge:

A. *Authentication & Access Control*
B. *Logging & Monitoring*
C. *Data Backups & Recovery*
D. *Secure Communication & Encryption*
E. *Network Configuration & Management*

Fig. 1: Mapping use cases to configuration challenges uncovered in the qualitative sample. This figure was obtained by mapping each post's assigned use case and configuration challenge. The count of posts in each cell is an upper bound value obtained via the methodology defined in the main paper. Each cell also contains the total number of assigned topics of the respective posts in that cell.

logins or access errors show up only as vague HTTP errors with no clear trace.

Use Case 2: Server/Instance Configuration.

For server and instance configuration, operators must ensure that system logs, audit trails, and agent-based metrics are correctly shipped to central logging services. Posts describe difficulty installing and configuring log agents, choosing the right log groups, and keeping track of rotating instance identifiers. Missteps here result in gaps in audit trails or servers that silently fail without emitting useful alerts.

Use Case 3: Network, Connectivity, and Routing.

In networking scenarios, logging and monitoring are needed to understand why traffic does not flow as expected across VPCs, VPNs, or gateways. Operators attempt to combine flow logs, firewall logs, and load balancer access logs, but encounter problems with incomplete data, inconsistent formats, or missing context such as client IPs. Without clear network-level logs, they struggle to distinguish between routing errors, blocked connections, and failing upstream services.

Use Case 4: Data and Database Operations.

For data and database operations, posts describe challenges in configuring query logs, access logs, and audit trails for managed database services. Operators want to track who accessed which records, from where, and under which credentials, but face unclear configuration options or cost trade-offs when enabling detailed logging. Errors in these setups can hide suspicious access patterns or make it hard to debug failed transactions.

Use Case 5: Application and Service Deployment and Management.

During application and service deployment, logging and monitoring issues often appear when new versions go live but emit incomplete or misrouted logs. Operators report trouble wiring application logs, health checks, and runtime metrics into existing dashboards after changes in containers, functions, or platforms. If these links are not updated correctly, alerts fail to trigger or show misleading signals, which makes it harder to catch security problems or performance regressions after a deployment.

Use Case 6: Cloud Automation and CI/CD Pipelines.

Within automation and CI/CD pipelines, logging issues arise when build logs, deployment events, and infrastructure changes are spread across many tools. Operators struggle to pipe logs from build agents, template engines, and cloud APIs into a single view where they can trace a failed deployment from commit to runtime error. Missing or truncated logs often force them to rerun jobs just to capture enough detail for debugging.

Use Case 7: Cloud Integrations and API Configuration.

For cloud integrations and API configuration, logging and monitoring are essential to understand how requests move across multiple services and providers. Posts describe difficulty enabling detailed request logs on all hops, correlating request IDs, and separating transient client errors from deeper configuration faults. When logging is incomplete, operators only see generic timeouts or 500 errors at the client, with no clear insight into which link in the integration failed.

4) Data Backups and Recovery:

Use Case 1: Cloud Web/App Development.

In web and app development, backup questions focus on protecting user data stored in cloud-managed services. Developers ask how to schedule exports or snapshots for items such as user profiles or session data and how to restore only selected parts without breaking the application. They also worry about accidentally exposing backups when storing them in shared buckets or other storage locations.

Use Case 2: Server/Instance Configuration.

For server and instance configuration, operators ask how to back up virtual machines, configuration files, and attached storage so they can recover quickly from failures. Posts describe uncertainty about choosing between image-based backups, filesystem-level backups, and copying disks to cheaper storage tiers. They also seek guidance on how to test restores without disrupting running services.

Use Case 5: Application and Service Deployment and Management.

During application and service deployment, backup and recovery issues arise when new versions may corrupt data or change schemas. Operators want strategies for taking safe pre-deployment snapshots, rolling back both code and data, and keeping configuration secrets safe across versions. Misconfigured workflows can leave them with backups that are out of date or hard to restore when a deployment goes wrong.

Use Case 7: Cloud Integrations and API Configuration.

In cloud integrations and API configuration, backup concerns shift to data that flows between services and providers. Operators ask how to preserve messages, events, or API payloads so they can replay them after an outage or integration bug. They also worry that backups spanning multiple systems may leak sensitive information if not encrypted or access controlled consistently.