CloudWalk – Monitoring Alerts (PoC)

2025-09-25 15:25

Objective

Detect minutes where **failed**, **denied**, or **reversed** transactions exceed normal levels and raise an alert.

Data

● transactions.csv: *timestamp*, *status*, *count* (per minute).

● Status normalization: *reversed*, *backend_reversed*, *refunded* → **reversed**.

Method

• Aggregate to one row per minute (columns: **failed**, **denied**, **reversed**).

• Compute global baseline per status: mean (μ) and standard deviation (σ).

• Raise alert if minute value > $\mu + $ **3.0**$\cdot\sigma$ (K is tunable).

Summary of Alerts

• failed: **70** minutes

• denied: **113** minutes

• reversed: **35** minutes

Time Series & Thresholds

Reversed – Per-minute with Threshold
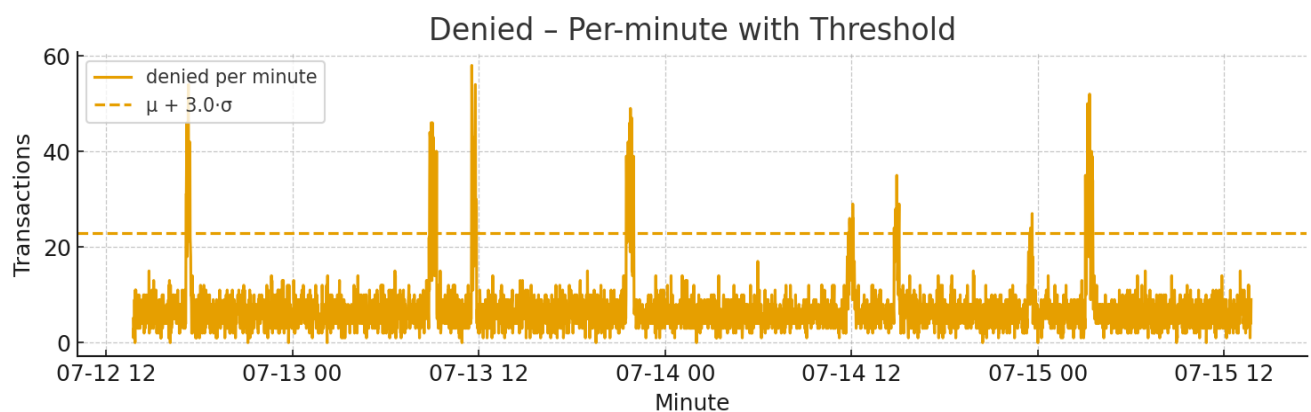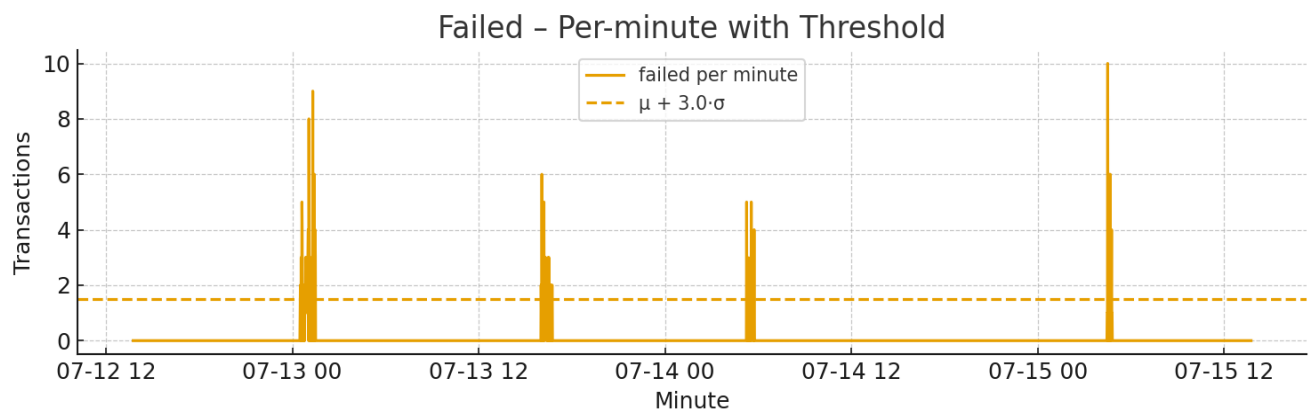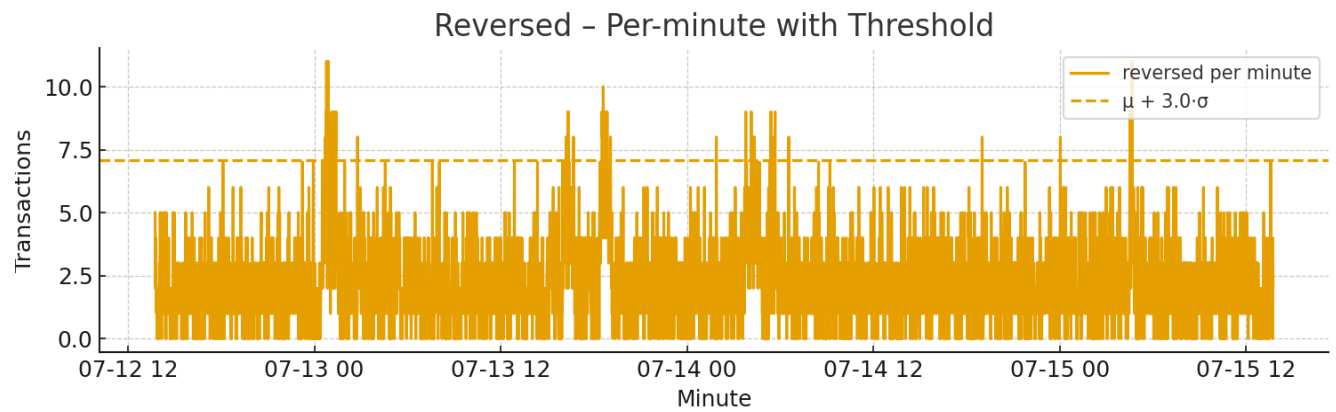
Top minutes – FAILED (by z-score)

Minute	Value	z-score
2025-07-15 04:30	10	20.871
2025-07-13 01:19	9	18.771
2025-07-13 01:04	8	16.671
2025-07-15 04:40	6	12.47
2025-07-15 04:36	6	12.47
2025-07-15 04:35	6	12.47
2025-07-13 16:04	6	12.47
2025-07-13 01:25	6	12.47
2025-07-13 16:12	5	10.37
2025-07-13 00:37	5	10.37

Top minutes – DENIED (by z-score)

Minute	Value	z-score
2025-07-13 11:33	58	9.561
2025-07-12 17:18	54	8.812
2025-07-13 11:47	54	8.812
2025-07-15 03:20	52	8.438
2025-07-15 03:12	50	8.063
2025-07-13 21:46	49	7.876
2025-07-13 21:51	47	7.501
2025-07-13 11:46	47	7.501
2025-07-13 21:43	46	7.314
2025-07-12 17:17	46	7.314

Top minutes – REVERSED (by z-score)

Minute	Value	z-score
2025-07-15 04:39	11	5.398
2025-07-13 00:47	11	5.398

2025-07-13 00:54	11	5.398
2025-07-13 18:36	10	4.785
2025-07-13 00:45	9	4.172
2025-07-13 18:31	9	4.172
2025-07-15 04:31	9	4.172
2025-07-14 05:40	9	4.172
2025-07-14 05:24	9	4.172
2025-07-14 04:08	9	4.172

Limitations & Next Steps

- Global baseline ignores time-of-day patterns.
- Consider rolling-window baselines (e.g., last 30–60 minutes).
- Use robust z (median/MAD) to reduce outlier sensitivity.
- Add sustained-alert logic (e.g., N of last M minutes).
- Wire alerts to Slack/Email and expose a simple /alert endpoint.